Bezpieczeństwo informacji w systemach informatycznych

Paweł Plaskura

IT Security

ISBN 978-83-937245-3-6

Recenzenci:
prof. dr hab. Zygmunt Matuszak
dr inż. Andrzej Góralski

Dokument złożono systemem składu LaTeX
Wykorzystano system operacyjny Linux (Debian) 
Wersja dokumentu: 1.3

Bezpieczeństwo informacji w systemach informatycznych

Paweł Plaskura

http://epub.aiva.pl?isbn=978-83-937245-3-6

AIVA
ul.Przelotowa 15A
97-300 Piotrków Trybunalski
Poland
http://www.aiva.pl
biuro@aiva.pl

ISBN 978-83-937245-3-6

Spis treści

Recenzja I

Opracowanie naukowe dr. Pawła Plaskury jest nowatorskim opracowaniem naukowym na trwale wpisującym się w całokształt problematyki bezpieczeństwa narodowego. Wydawać by się mogło, iż *Bezpieczeństwo informacji w systemach informatycznych* należy tylko do tzw. technicznego obszaru działalności naukowej. Nic bardziej mylnego. W obecnym świecie każda działalność naukowa, dydaktyczna, czy jakakolwiek inna nawet artystyczna, nie może obejść się bez wykorzystania środków i systemów informatycznych. Informatyzacja zdominowała każdy zakres działalności człowieka, a w tym pracownika naukowego.

W związku z szerokim upowszechnieniem informatyki i jej wykorzystywaniem na wszystkich poziomach wszechstronnej działalności człowieka, zaistniała konieczność zapewnienia ochrony przesyłanych danych, ich udostępniania, przetwarzania, wykorzystywania itp. Wiele informacji dotyczących tworzenia i wykorzystywania różnych danych, ma wpływ na nasze życie i działalność, a także na utrzymywanie w stanie stałej gotowości systemów bezpieczeństwa państwa. Dlatego bezpieczeństwo informatyczne, stało się obok bezpieczeństwa narodowego, militarnego, ekonomicznego, jednym z najważniejszych.

O ile wyróżnia się ok. 11 rodzajów bezpieczeństwa, to bezpieczeństwo informatyczne przewija się we wszystkich rodzajach i nie w sposób go bagatelizować. Dziś światem, naszym życiem *rządzi* informacja. Dlatego niezbędnym jest jej zabezpieczenie, aby trafiała do właściwych organów, komórek czy osób. Szczególną rolę ma bezpieczeństwo informacji w systemach bezpieczeństwa narodowego czy militarnego.

Praca dr P. Plaskury dotyczy właśnie tej problematyki bezpieczeństwa informacji w systemach informatycznych. Biorąc pod uwagę znaczenie tej problematyki oraz zakres tematyczny, jaki Autor zawarł w swoim opracowaniu, wysoko oceniam prezentowane dzieło i z pełnym przekonaniem polecam je do szybkiego wydania i skierowania do pracowników naukowych, a głównie studentów kierunku Bezpieczeństwo Narodowe. Na rynku wydawniczym funkcjonuje wiele różnych opracowań dotyczących bezpieczeństwa szeroko pojętego, czasami pod podobnie brzmiącymi tytułami ale z różnymi treściami, jednak opracowanie dr. Pawła Plaskury zaliczam do nielicznych poświęconych bezpieczeństwu informacji w systemach informatycznych. Dlatego z pełnym przekonaniem opiniuję pracę dr. Plaskury do druku i pilnego upowszechnienia.

prof. dr hab. Zygmunt Matuszak
Uniwersytet Jana Kochanowskiego w Kielcach
Filia w Piotrkowie Trybunalskim
Katedra Bezpieczeństwa Narodowego
Piotrków Trybunalski, 25 października 2016

Recenzja II

W pracy przedstawiono kompleksowe podejście do zagadnienia bezpieczeństwa informacji. Spotykane w publikacjach sposoby prezentowania tego typu zagadnień często obejmują je tylko fragmentarycznie. Z racji różnorodności tematyki oraz całego wachlarza rozwiązań i technik, jakie się stosuje potrzebne obecnie jest zawsze podejście interdyscyplinarne. Bez tego taka wiedza zawsze jest niekompletna i prowadzi do powstawania wielu luk bezpieczeństwa.

Mnogość systemów, stopień ich komplikacji, czy to rozważając je na poziomie makro (np. jako system) czy w sakli mikro (np. jako język programowania) stwarza konieczność szerszego spojrzenia na bezpieczeństwo danego rozwiązania aby nie stwarzać bezkrytycznie luk bezpieczeństwa poprzez nieznajomość elementarnych zasad i wiedzy w tym zakresie. Często niweczy to trud włożony w stworzenie danego rozwiązania IT, czego chociażby są dowodem wszelkie systemy WWW tworzone bez uwzględniania we właściwy sposób ich zabezpieczeń.

Zakres wiedzy teoretycznej związany z tą tematyką przedstawiono w sposób umożliwiający nawet nieprzygotowanemu czytelnikowi zrozumienie najistotniejszych dosyć skomplikowanych zagadnień bezpieczeństwa i jego analizy dla systemów komputerowych, systemów operacyjnych oraz w zakresie sieci i kryptografii. Jest to szczególnie cenne, gdyż umożliwia to samodzielne dalsze rozszerzanie wiedzy w tym zakresie.

Zawarta w pracy wiedza została przedstawiona w sposób jasny i czytelny dzięki wieloletniemu interdyscyplinarnemu doświadczeniu autora.

Publikacja powinna ukazać się drukiem lub lepiej w formie elektronicznej, gdyż zawiera cały system odnośników, co bardzo ułatwia nawigację. Publikacja jest dobrze dopracowana od strony edycyjnej.

dr inż. Andrzej Góralski
Wyższa Szkoła Menadżerska w Warszawie
Warszawa, 22 listopada 2016 r.

Rozdział 1

Wstęp

Zagadnienia bezpieczeństwa informacji mają coraz większe znaczenie w dobie rozwoju technik komunikowania się. Łatwość gromadzenia i pozyskiwania informacji (z różnych źródeł) stanowi realne zagrożenie dla wielu aspektów funkcjonowania ludzi i firm we współczesnym świecie. Informacja to nic innego jak dane, które mogą być przesyłane, gromadzone i przetwarzane.

Ochrona informacji jest zagadnieniem wielowymiarowym. Obejmuje szereg zagadnień:

- ochronę przed utratą informacji,
- ochrona przed podsłuchem przesyłanych informacji,
- ochrona przed dostępem do informacji.

Instytucje państwowe zauważają od dawna potrzebę ochrony informacji i w związku z tym powołują szereg instytucji oraz wprowadzają odpowiednie uregulowania prawne.

I tak w obszarze cywilnym powołano do życia np. instytucję GIODO (Głównego Inspektora Ochrony Danych Osobowych) celem ochrony danych osobowych oraz stworzono odpowiednią ustawę. Rozwiązań takich jest więcej zarówno w sferze cywilnej jak i w sektorze wojskowym.

Wraz z rozwojem technik komunikowania się każdy człowiek jest coraz bardziej narażony na konsekwencje wycieku informacji. Szczególnie narażone dane to, np.: informacje o stanie zdrowia, finansach, informacje poufne. Utrata takich danych naraża użytkownika na straty finansowe, moralne, utratę wizerunku lub niesie bezpośrednie zagrożenie życia.

W przypadku firm utrata danych najczęściej powoduje upadek firmy. Ujawnienie danych wrażliwych powoduje szereg problemów jak np. utratę kontraktów, utratę wypracowanych rozwiązań technologicznych i innych. W konsekwencji może to doprowadzić do upadku firmy.

Na przestrzeni wieków powstała dziedzina wiedzy, która zajmuje się zagadnieniami przekazywaniem informacji w bezpieczny sposób. Definicję kryptologii podaje definicja 1.1.

Definicja 1.1. *Kryptologia (z greek. kryptos - ukryty i greek. logos - rozum, słowo) - dziedzina wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem.*

Obecnie kryptologia jest uznawana za gałąź zarówno matematyki i informatyki. Jest blisko związana z teorią informacji, inżynierią oraz bezpieczeństwem komputerowym. Przetwarzana informacja w dziedzinie kryptologii nazywana jest wiadomością. Kryptologię dzieli się na:

- kryptografię (*greek. grafos* - pisać) - gałąź wiedzy o utajnianiu wiadomości;
- kryptoanalizę (*greek. kryptos* oraz *greek. analyein* - rozluźnić) - gałąź wiedzy o przełamywaniu zabezpieczeń oraz o deszyfrowaniu wiadomości przy braku klucza lub innego wymaganego elementu schematu szyfrowania (szyfru).

1.1 Cel pracy

Celem pracy jest zebranie i uporządkowanie najważniejszych informacji z dziedziny ochrony informacji, także dla potrzeb prowadzonego wykładu dla studentów kierunku Bezpieczeństwo Narodowe.

1.2 Zawartość pracy

Praca składa się z 12 rozdziałów. W każdym rozdziale starano się omówić zagadnienie stanowiące pewną całość.

Rozdział 1 stanowi wprowadzenie w tematykę. Omówiono zagrożenia z jakimi spotyka się użytkownik w codziennej pracy i procedury ochrony. Przedstawiono krótką historię rozwoju technik zabezpieczania informacji od czasów antycznych, aż do chwili obecnej.

W rozdziale 2 omówiono najczęściej spotykane oszustwa i podano rzeczywiste przykłady.

W rozdziale 3 omówiono podstawowe zagadnienia prawne związane z przetwarzaniem i zabezpieczaniem informacji. Podano szereg odnośników do obowiązujących ustaw i rozporządzeń. Wprowadzono klasyfikację informacji zgodnie z obowiązującymi przepisami. Omówiono zagadnienia certyfikacji urządzeń. Zajęto się polityką bezpieczeństwa i przetwarzaniem danych osobowych. Omówiono zadania ABI i GIODO.

W rozdziale 4 przedstawiono popularne systemy operacyjne. Omówiono ich budowę i podstawy zabezpieczania. Szczególnie dużo miejsca poświęcono systemom klienckim firmy Microsoft. Przedstawiono kwestie związane z bezpieczeństwem przeglądarek internetowych. Przedstawiono także wybrane narzędzia do administracji ww. systemów.

W rozdziale 5 omówiono oprogramowanie złośliwe. Podano klasyfikację i omówiono w skrócie sposoby działania poszczególnych grup.

W rozdziale 6 omówiono podstawowe rodzaje ataków na systemy komputerowe, w szczególności te działające w sieci. Omówiono sposoby obrony przed wybranymi atakami. Omówiono technikę czarnych list.

W rozdziale 7 zajęto się zagadnieniami ochrony i zabezpieczania systemów informatycznych. Zajęto się backupem jako jedną z metod ochrony. Podano także sposób konfiguracji najpopularniejszych przeglądarek WWW. Przedstawiono wybrane pakiety oprogramowania antywirusowego i antimalware.

W rozdziale 8 przedstawiono szereg zagadnień z dziedziny kryptografii. Omówiono kryptografię symetryczną i asymetryczną. Podano metody realizacji podstawowych usług ochrony informacji. Omówiono funkcję skrótu i jej zastosowanie. Przedstawiono najpopularniejsze algorytmy szyfrujące.

W rozdziale 9 przedstawiono podstawowe zagadnienia kryptoanalizy, tj. dziedziny która zajmuje się metodami łamania szyfrów.

W rozdziale 10 omówiono system PKI, który umożliwia realizacje podstawowych usług ochrony informacji, także w sieciach komputerowych. Omówiono historię funkcję i zastosowanie PKI. Przedstawiono zagadnienia ataków na system PKI.

Rozdział 11 poświęcony jest sprzętowi kryptograficznemu. Przedstawiono szereg urządzeń, które produkowane są w kraju, w tym: karty i czytniki kryptograficzne, sprzęt kryptograficzny, systemy bezpiecznej telefonii.

W rozdziale 12 omówiono zagadnienia związane z sieciami komputerowymi. Omówiono zagadnienia związane z przesyłaniem informacji w sieciach. Omówiono podstawowe programy, które stanowią największe zagrożenia. Omówiono szereg programów, które umożliwiają analizę pracy sieci i komputerów w niej pracujących.

W pracy zamieszczono także literaturę problemu, słownik oraz dodatki.

1.3 Zagrożenia

W praktyce istnieje wiele źródeł zagrożeń związanych z możliwością utratą informacji. Jednak najsłabszym ogniwem jest prawie zawsze człowiek. Źródła zagrożeń można klasyfikować na różne sposoby.

Dotyczy to samego fizycznego zabezpieczenia i przechowywania danych, fizycznego dostępu do danych, ale także lokalizacji sprzętu, jego zasilania. Są to uwarunkowania środowiskowe. Osobną kwestią jest przechowywanie dokumentów w odpowiednich warunkach środowiskowych. Przy przechowywaniu danych bardzo ważną rolę grają formaty danych, które umożliwiają odczytanie danych w dłuższej perspektywie czasowej. To samo dotyczy weryfikowalności i odczytywalności kopii zapasowych. Kwestie te będą omawiane w kolejnych rozdziałach. Podstawowym podziałem zagrożeń może być podział ze względu na lokalizację źródła niebezpieczeństwa:

- Zagrożenia wewnętrzne występujące wewnątrz organizacji, które są związane z:
  - utratą danych,
  - uszkodzeniem danych,
  - brakiem możliwości obsługi z powodu błędów bądź przypadku,
  - utratą lub celowe uszkodzenie danych (poprzez nieautoryzowany dostęp do informacji lub danych),
  - celowym zniszczeniem danych w oprogramowaniu systemowym (instalacja złośliwego oprogramowania).
- zagrożenia zewnętrzne (powstające na zewnątrz organizacji) związane z:

  - uszkodzeniem danych lub pozbawieniem możliwości obsługi poprzez celowe bądź przypadkowe działanie ze strony osób trzecich w stosunku do systemu lub sieci,
  - unieruchomieniem usług systemów komputerowych,
  - uzyskaniem nieautoryzowanego dostępu do systemów komputerowych/danych,
  - przechwytywaniem danych (podsłuch).

Obecnie większość informacji przetwarzana jest przez systemy komputerowe. Dodatkowo sytuację komplikuje fakt, że komputery podłączone są do sieci i przez sieć przesyłają pomiędzy sobą dane. Można wymienić wiele rodzajów zagrożeń dla systemów komputerowych:

- Kradzież nośników informacji lub ich zamiana.
- Celowe niszczenie zawartości zbiorów lub ich uszkodzenie uniemożliwiające wykorzystanie.
- Uzyskanie niedozwolonego dostępu do zastrzeżonych baz danych lub usiłowanie uzyskania takiego dostępu.
- Przechwytywanie informacji w trakcie pracy systemu.
- Unieruchamianie lub paraliżowanie usług systemu komputerowego.
- Zagrożenia naturalne, takie jak:
  - pożar,
  - powódź,
  - trzęsienie ziemi,
  - awaria,
  - wypadek lub inne nieprzewidziane zdarzenia wpływające na system informacyjny bądź urządzenia sieciowe.

Należy zwrócić uwagę, że nielegalne przechwycenie danych z systemu komputerowego jest możliwe w bardzo prosty sposób, np. przez:

- Wejście osoby nieuprawnionej do pomieszczenia i dokonanie kradzieży.
- Skopiowanie nośnika z danymi wybranych zbiorów przez osobę posiadającą dostęp do informacji z tytułu zajmowanego stanowiska bądź wykonywanego zadania.
- Skopiowanie informacji przez obsługę z serwisu.
- Pomyłkowe wydanie nośnika z danymi osobie nieuprawnionej np. osobie która przyniosła do pomieszczenia nośnik danych ze swoimi programami lub grami.
- Udostępnianie komputera osobom nieuprawnionym do dokonywania na nim operacji bezpośrednio po zakończeniu pracy z wykorzystaniem programów zawierających informacje charakteru niejawnego bez uprzedniego jego zabezpieczenia (część informacji może pozostać w pamięci komputera i jest do odzyskania przez osobę znającą system).

Przeciwdziałanie przechwyceniu danych jest możliwe, jeżeli użytkownik będzie stosował podstawowe zasady bezpieczeństwa, które można sformułować w postaci pytań.

- Czy na komputerze pracownika instalowane i wykonywane są programy prywatne?
- Czy do pomieszczeń, gdzie usytuowany jest komputer, wchodzą osoby do tego nieuprawnione za zgodą obsługi?
- Czy osoby nieuprawnione pozostają w pomieszczeniu bez nadzoru?
- Czy osoby nieuprawnione wykonują operacje na komputerze?
- W jaki sposób zabezpieczone są nośniki danych?

  Czy prowadzona jest właściwa ewidencja nośników danych?

  Czy i jak odbywa się niszczenie wykorzystywanych zbiorów informacji?
- W jaki sposób konserwuje się systemy informatyczne?

  Kto zajmuje się konserwacją systemu?

  Czy istnieją możliwości dostępu do programów niejawnych?

  Czy pracownicy serwisu pozostają bez nadzoru?
- W jaki sposób zabezpieczone jest archiwum?
- W jaki sposób zorganizowane jest zabezpieczenie fizyczne systemu informatycznego?

Należy zaznaczyć, że zamierzone lub przypadkowe uszkodzenie (zniszczenie) systemów informatycznych możliwe jest w kilku często spotykane w praktyce przypadkach:

- Jeżeli z systemu korzysta niewyszkolona obsługa lub z systemu korzysta wiele osób. Dotyczy to głównie systemów klienckich firmy Microsoft, gdzie poziom zabezpieczeń niektórych z nich pozostawia dużo do życzenia.
- Osoby działające z motywów osobistych:
  - wrogi stosunek do przełożonych,
  - dla osiągnięcia założonego celu osobistego,
  - wykonanie zadania na korzyść innej organizacji.
- Modyfikowanie danych lub programów komputerowych, np. poprzez udoskonalenia dla własnej wygody.
- Zainfekowanie systemów komputerowych złośliwym oprogramowaniem.

W związku z powyższym należy wdrożyć odpowiednie procedury ochrony systemów informatycznych. Można je zgrupować w punktach.

- Systemy informatyczne, z których korzysta więcej niż jeden użytkownik, a które udostępniają tym użytkownikom informacje wycinkowe z chronionej bazy danych, powinny posiadać wbudowane procedury uwierzytelnienia użytkowników i systemów.
- System musi być tak zaprojektowany, aby użytkownik wiedział, że korzysta z danego systemu. System musi sprawdzać czy użytkownik ma prawo do uzyskania określonych informacji.
- Użytkownicy powinni posiadać identyfikatory (np. nazwa bądź numer identyfikacyjny inny dla każdego), które podlegają uwierzytelnieniu w systemie komputerowym. Jeżeli wynik procedury uwierzytelnienia jest właściwy, wówczas użytkownik powinien mieć pewność że pracuje z odpowiednim systemem komputerowym, a system zrealizuje jego polecenia.
- W systemach powinny być prowadzone dzienniki ewidencji pracy systemu. Powinny one zawierać m.in.:
  - informacje o realizacji zadań przez system,
  - informacje o realizacji zadań przez osoby, które uzyskały dostęp,
  - informacje o próbach (nieudanych) uzyskania dostępu do systemu.

System informatyczny powinien być tak zaprojektowany, aby była możliwość ustalenia przez osobę kontrolującą:

- Informacji dotyczących upoważnień (praw dostępu) związanych z każdym chronionym zbiorem.
- Odpowiedzialności za zmiany dokonane w zbiorach informacji.
- Zmian dokonanych w zbiorach informacji.
- Wszelkich przypadków dostępu do chronionych zasobów. Ze względu na dużą ilość danych musi istnieć możliwość sortowania zdarzeń po odpowiednim kluczu, np po użytkowniku, programie, terminalu z którego uzyskano dostęp, zadaniu, danych ....
- Informacji o odmowie udzielenia dostępu do systemu lub danych.
- Wszystkich tymczasowych upoważnień udzielonych wówczas, gdy konieczny był dostęp do chronionych danych, a upoważniony użytkownik lub terminal był niedostępny.
- Wszystkich przestawień zegara.
- Zmian w konfiguracji sprzętu i oprogramowanie dokonane przez operatora lub administratora systemu.

Rozdział 2

Oszustwa komputerowe

Internet jest nieocenionym źródłem informacji niosących za sobą wiele korzyści. Niestety jest to także miejsce pracy wielu bardzo kreatywnych oszustów internetowych. Ich perfekcja działania sprawia, że wielu użytkowników sieci padło już ich ofiarą. Jedyną metodą na ustrzeżenie się przed tego typu zagrożeniami jest zwiększenie świadomości zagrożeń w sieci. Kluczem do uniknięcia niekorzystnych sytuacji jest przede wszystkim poznanie zagrożeń i sposobów ich unikania. Historia oszustw jest dosyć długa. Oszustwa można sklasyfikować na kilka grup:

2.1 Scam

Scam (wym. [skaem]) to oszustwo polegające na wzbudzeniu u kogoś zaufania, a następnie wykorzystanie tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm.

Scam przybiera różne formy - począwszy od bezpośredniego wzbudzania zaufania poprzez kontakty osobiste, przez wysyłanie maili i tradycyjnych listów, po skomplikowane technicznie zabiegi z użyciem usług internetowych.

Scam listowy Współcześnie najczęstszą formą scamu jest masowa korespondencja w formie tradycyjnej lub elektronicznej - odmiana spamu.

Typowy mechanizm polega na proponowaniu ofierze udziału w ogromnych zyskach w zamian za rzekome pośrednictwo wymagające zainwestowania proporcjonalnie niewielkich własnych środków w różnego rodzaju koszty operacyjne. Opłaty ponoszone przez ofiarę są w rzeczywistości przechwytywane przez oszusta, który następnie znika, nie dokonując ostatecznie żadnej wpłaty na rzecz ofiary. Oszust wciela się zwykle w postać spadkobiercy, wcześniej oszukanego przedsiębiorcy, potomka ofiary zamachu stanu itp.

Ten rodzaj oszustwa znany jest pod nazwą nigeryjski szwindel lub oszustwa nigeryjskie.

Do tej grupy należą także:

- oszustwa loteryjne. Oszust wysyła maila z informacją, że odbiorca został on zwycięzcą danej loterii i zyskał nagrodę pieniężną. W celu odebrania nagrody należy wpłacić proporcjonalnie niewielką sumę pieniędzy.

- Oszustwa matrymonialne - najczęściej dotyczą wysyłania na przypadkowo pozyskany adres e-mail określonego mężczyzny propozycji matrymonialnych (np. z Rosji czy Ukrainy). Problemem jest brak środków na finansowanie podróży.

Scam na stronach WWW Inną formą scamu są strony WWW oferujące wysokie zyski lub bardzo wartościowe informacje najczęściej w zamian za niewielki wkład inwestycyjny (np. HYIP). Może to być również wypełnianie ankiet, wprowadzanie danych on-line, jak i odbieranie reklam w poczcie elektronicznej (GPT). Istnieje również dużo agencji matrymonialnych (głównie na terenie Rosji), których celem jest zwerbowanie jak największej ilości osób (SCAM VICTIM) w celu wyłudzania od nich pieniędzy na rzekome wizy oraz podróże dla przepięknych kobiet poznanych za pomocą internetu. Przy rejestracji na tego rodzaju stronach jest wymagany adres poczty elektronicznej, więc jest ona często przyczyną dużej ilości spamu w skrzynce.

W niektórych przypadkach strona początkowo płaci, żeby później, przekształcając się w scam, przynieść większe zyski. Po krótkim czasie scam znika z sieci lub ogłasza zmianę właściciela, która w rzeczywistości niekoniecznie nastąpiła.

Scam w grach online Scam w grach online ma miejsce podczas wymiany przedmiotów. Sprzedawca i kupujący otwierają okno wymiany, sprzedawca wystawia wartościowy przedmiot, kupujący wystawia odpowiednią ilość gotówki, w tym momencie sprzedawca zmienia ten wartościowy przedmiot na przedmiot o znacznie mniejszej wartości, ale nie różniący się wyglądem. Gracze zatwierdzają wymianę, a kupujący zamiast wymarzonego przedmiotu ma w ekwipunku bezwartościowy przedmiot oraz stracił pokaźną sumę pieniędzy. Sprzedający zachowuje przedmiot oraz pieniądze.

Scam na eBayu Przykładem scamu na ebayu są osoby oferujące tajemnicze sposoby, pozwalające rzekomo, na zarobienie kilku tysięcy dolarów w jeden dzień, bez wychodzenia z domu i wydawania dodatkowych pieniędzy. Dodatkowo, do opisu aukcji dołączane są zdjęcia sprzedawcy, przy bardzo eleganckim samochodzie lub domu.

Przykładowe sposoby, po cenie 30$:

1. Kup e-booka za 10$, od kogoś
2. Obrób go programem za 300$
3. Zakup serwer za 500$
4. Utwórz stronę promującą e-booka.

Inne formy to np. propozycje zarabiania na Forexie, czy wytwarzania i sprzedawania biżuterii własnej produkcji.

Scam w fałszywych instalatorach oprogramowania Przykładem scamu w popularnym oprogramowaniu, podobnym do powyższego są fałszywe instalatory bezpłatnego opensource'owego pakietu OpenOffice, które żądają od zaskoczonego użytkownika podania kodu aktywacyjnego rzekomo koniecznego do aktywacji

premium, który ma być przesłany po wysłaniu płatnego *premium SMS*, a nawet kilku do: *Libela Gestion SMS Limitada* z siedzibą w *Calle Estado 42 Of. 405 Santiago Centro, Chile*. Z tego względu pakiet biurowy OpenOffice należy pobierać zawsze ze strony projektu: OpenOffice.org. Pakiet jest zawsze bezpłatny.

2.2 Pishing

Phishing - w branży komputerowej metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

Termin został ukuty w połowie lat 90. przez crackerów próbujących wykraść konta w serwisie AOL. Atakujący udawał członka zespołu AOL i wysyłał wiadomość do potencjalnej ofiary. Wiadomość zawierała prośbę o ujawnienie hasła, np. dla *zweryfikowania konta* lub *potwierdzenia informacji w rachunku*. Gdy ofiara podawała hasło, napastnik uzyskiwał dostęp do konta i wykorzystywał je w przestępczym celu, np. do wysyłania spamu.

Termin phishing jest niekiedy tłumaczony jako password harvesting fishing (łowienie haseł). Inni utrzymują, że termin pochodzi od nazwiska Briana Phisha, który miał być pierwszą osobą stosującą techniki psychologiczne do wykradania numerów kart kredytowych, jeszcze w latach 80. Jeszcze inni uważają, że Brian Phish był jedynie fikcyjną postacią, za pomocą której spamerzy wzajemnie się rozpoznawali.

Dzisiaj przestępcy sieciowi wykorzystują techniki phishingu w celach zarobkowych. Popularnym celem są banki czy aukcje internetowe. Phisher wysyła zazwyczaj spam do wielkiej liczby potencjalnych ofiar, kierując je na stronę w Internecie, która udaje rzeczywisty bank internetowy, a w rzeczywistości przechwytuje wpisywane tam przez ofiary ataku informacje. Typowym sposobem jest informacja o rzekomym zdezaktywowaniu konta i konieczności ponownego reaktywowania, z podaniem wszelkich poufnych informacji. Strona przechwytująca informacje - adres do niej był podawany jako klikalny odsyłacz w poczcie phishera - jest łudząco podobna do prawdziwej, a zamieszanie było często potęgowane przez błąd w Internet Explorerze (w 2004 r. ponad 90% rynku przeglądarek), który pozwalał zamaskować także rzeczywisty adres fałszywej strony. Innym sposobem było tworzenie fałszywych stron pod adresami bardzo przypominającymi oryginalny, a więc łatwymi do przeoczenia dla niedoświadczonych osób - na przykład www.paypai.com zamiast www.paypal.com.

Przykład omawianej techniki podano poniżej. Jest to zawartość mail'a otrzymanego w imieniu mBanku z prośbą o dokonanie dodatkowej autoryzacji w związku z zablokowaniem konta.

```
Date: Sat, 28 Feb 2015 11:10:54 -0800
From: MBank <waynes@highgrove.net>
To: xxxxx@xxxx.pl
Subject: Twoje konto zostalo zablokowane !
X-Mailer: Microsoft Outlook Express 6.00.2800.1106

Szanowny kliencie mBanku !
Dostęp do Twojego konta został zablokowany, powodem blokady jest
    ↪ nieautoryzowany
dostęp do rachunku oszczędnościowego.
Ze względu na dużą ilość ataków do kont naszych klientów przeprowadzamy
dodatkową weryfikację.
```

```
W~celu weryfikacji prosimy o~zalogowanie się na konto mBank.
Kliknij Tutaj aby się zalogować.
http://autoryzacja-mbank.com/

Zespół mBank.
```

W treści mail'a pojawia się adres strony http://autoryzacja-mbank.com/, na który należy kliknąć celem dokonania autoryzacji przez zalogowanie na własne konto. Strona ta jest łudząco podobna do strony banku. Wpisanie loginu i hasła przenosi natychmiast na oryginalną stronę logowania banku. Wygląda to tak jakby coś się nie udało podczas logowania. Należy zwrócić uwagę, że połączenie z fałszywą stroną nie jest szyfrowane (protokół HTTP).

Obrona przed phishingiem Zdecydowana większość wiadomości phishingowych jest dostarczana za pośrednictwem poczty elektronicznej lub portali społecznościowych.

- Zazwyczaj serwisy nie wysyłają e-maili z prośbą o odwiedzenie i zalogowanie się na stronie. Taka prośba powinna wzbudzić czujność, zawsze warto w takim wypadku potwierdzić autentyczność listu poprzez kontakt z administratorami strony. Banki i instytucje finansowe nigdy nie wysyłają listów z prośbą o ujawnienie (wpisanie w formularzu) jakichkolwiek danych (loginu, hasła, numeru karty), próby podszycia się pod nie powinny być zgłaszane do osób odpowiedzialnych za bezpieczeństwo.

- Nie należy otwierać hiperłączy bezpośrednio z otrzymanego e-maila. Stosunkowo prosto jest zmodyfikować ich treść tak, by pozornie wskazujące na autentyczną witrynę kierowały do nieautoryzowanej, podszywającej się strony.

- Należy regularnie uaktualniać system i oprogramowanie, w szczególności klienta poczty e-mail i przeglądarkę WWW. Nie wolno przesyłać mailem żadnych danych osobistych typu hasła, numery kart kredytowych itp. Prośby o podanie hasła i loginu w mailu należy zignorować i zgłosić odpowiednim osobom.

- Banki i instytucje finansowe stosują protokół HTTPS tam, gdzie konieczne jest zalogowanie do systemu. Jeśli strona z logowaniem nie zawiera w adresie nazwy protokołu HTTPS, powinno się zgłosić to osobom z banku i nie podawać na niej żadnych danych.

- Nie zaleca się używania starszych przeglądarek internetowych (np. Internet Explorer 6), które bywają często podatne na różne błędy. Alternatywnie można korzystać z innych programów, jak Mozilla Firefox czy Opera lub Internet Explorer 9 i 10 (których najnowsze wersje wyposażone są w filtry antyphishingowe) albo też z oprogramowania firm trzecich chroniącego przed phishingiem.

- Używanie OpenDNS celem ochrony przed przekierowaniem przez serwer DNS na strony i serwery intruzów.

Oszustwa domenowe Oszustwa domenowe (*ang. domain name selling scam*) polegają na tym, iż określona osoba dzwoni do właściciela konkretnej domeny i proponuje wykupienie domeny z inną końcówką (przedstawia się jako przedstawiciel jakiejś firmy internetowej i *rzetelnie* uprzedza, że nieuczciwa konkurencja chce wykupić domenę o tej samej nazwie co nasza, ale z inną końcówką). Osoby, które dają się na to nabrać szybko przelewają pieniądze na podane mailem konto. Po jakimś czasie okazuje się jednak, że wcale domeny z inną końcówką nie wykupiliśmy, a tylko ją dzierżawimy.

Oszustwa wybranych firm reklamowych Oszustwa wybranych firm reklamowych i agencji interaktywnych dotyczą najczęściej aspektu tworzenia stron www. Zlecając firmie stworzenie witryny powinniśmy zatem rozważnie wybierać agencje, z usług której zamierzamy korzystać i zapoznać się z pozyskanymi przez nią referencjami.

Oszustwa w portalach społecznościowych Oszustwa w portalach społecznościowych polegają najczęściej na włamaniu się na konto użytkownika np. Facebooka czy Naszej Klasy i rozsyłają w imieniu właściciela profilu maile do jego znajomych. Oszuści o przesłanie kwoty na podane konto (uzasadniają to chociażby tym, iż zostali oszukani za granicą i nie mają pieniędzy na powrót do kraju). Wiele osób przesyła środki finansowe sądząc że prawdziwy przyjaciel jest w potrzebie.

Fałszywe oferty pracy z zagranicy Fałszywe oferty pracy z zagranicy skierowane są do określonej osoby poszukującej pracy. Zagraniczna firma proponuje bardzo atrakcyjne zarobki przy wykonywaniu określonej czynności, głównie na zasadzie zdalnej. Nieuczciwi *pracodawcy* proszą o dane konta bankowego, aby można było dokonać przelewu za wykonaną pracę. Niestety po jakimś czasie okazuje się, że dane te zostały wykorzystane do zrabowania pieniędzy z kont innych osób, których dane zostały przechwycone. Można powiedzieć, że dana osoba myśląc, że pracuje dla określonej firmy, staje się pośrednikiem w kradzieży pieniędzy z innych kont. Dana osoba nieświadomie bierze udział w dokonaniu czynu niedozwolonego - udostępniając przestępcom swoje konto i pośrednicząc w przelewaniu środków.

Oszustwa związane z telemarketingiem Zdarza się, że do firmy czy osoby prywatnej dzwoni osoba, która proponuje wykupienie domeny, reklamę na jakimś portalu czy inną usługę. Bardzo szybko przesyła fakturę z podaną do zapłaty kwotą. Zdarza się, że zgodę na przesłania oferty na e-maila traktuje jak zdecydowanie się na określoną usługę. W przypadku nie uiszczenia należności firma ta straszy podaniem do sądu lub wpisaniem do Krajowego Rejestru Długów. Oszuści posuwają się w manipulacji bardzo daleko, np. nagrywają rozmowy i próbują je wykorzystać tak, aby dana osoba przelała należność. Często osoby dzwoniące podszywają się pod daną firmę.

Oszustwa SMS-owe w Internecie Celem oszustów jest wyłudzenie pieniędzy za pośrednictwem SMS-ów. Nierzadko można wejść na strony internetowe, gdzie proponowane są takie usługi jak wysłanie e-kartki do znajomych czy skorzystanie z porady wróżki. Oczywiście nie wszystkie tego typu serwisy są nieuczciwe.

Deklarowany koszt jest niższy niż w rzeczywistości. Najczęściej firmy, które w ten sposób oszukują klientów, działają wbrew pozorom legalnie. Rzeczywiste koszty są podane np. w regulaminie. Jedyną metodą obrony jest dokładne przeczytanie regulaminu serwisu.

Rozdział 3

Aspekty prawne

Zagadnienia związane z ochroną informacji można znaleźć w wielu aktach prawnych. Akty prawne dotyczą zarówno ochrony przetwarzanych informacji jak i ich klasyfikacji oraz archiwizowania. Ustawodawca w formie ustaw i rozporządzeń uregulował kwestie budowy systemów informatycznych służących do przetwarzania informacji oraz certyfikacji urządzeń kryptograficznych. Akty prawne dotyczą zarówno sfery cywilnej jak i wojskowej. Zmiany wprowadzane są o ile zajdzie taka potrzeba, np. na skutek rozwoju i postępu w omawianej dziedzinie. Na początek zostanie omówiona klasyfikacji informacji.

3.1 Klasyfikacja informacji

Zgodnie z Ustawą z dnia 5 sierpnia 2010 roku o ochronie tajemnicy niejawnych (Dz.U. 2010 nr 182 poz. 1228) zostały wyeliminowane pojęcia tajemnicy służbowej i państwowej. W państwach NATO i UE podział taki nie był stosowany.

Nowe definicje klauzul tajności zostały określone w art. 5:

ściśle tajne - jeżeli nieuprawnione ujawnienie informacji spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
- zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
- zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- osłabi gotowość obronną Rzeczypospolitej Polskiej;
- doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub
- kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;

- zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
- zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka (Dz. U. z 2015 r. poz. 21), albo świadków ....

tajne - jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

- uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
- utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

poufne - jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

- utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

zastrzeżone - jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony

narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Na podkreślenie zasługuje fakt, iż w nowej ustawie zrezygnowano z *Wykazu informacji niejawnych, które mogą stanowić tajemnicę państwową*. Z powyższego jasno wynika, iż przy przyznawaniu danej klauzuli musimy kierować się wyłącznie nowymi definicjami klauzul oraz przede wszystkim świadomością nieuprawnionego ujawnienia danej informacji oraz jego ewentualnymi jego skutkami.

Oznacza to, że w każdej jednostce organizacyjnej należy stworzyć samodzielnie *Wykazu podstawowych rodzajów dokumentów zawierających informacje niejawne*. Takie rozwiązanie pozwoli na uniknięcie naruszeń w zakresie zawyżania lub zaniżania klauzul.

W ustawie przewidziano także sposób postępowania w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności (Art.9).

Zrezygnowano także z narzuconych odgórnie czasów ochrony dla informacji niejawnych. Obecnie ochronę informacji można stosować tak długo, jak jest to niezbędne (art. 6 ust. 2).

Ustawa w przyjętej formie dostosowuje przepisy do rozwiązań prawnych obowiązujących w NATO i UE.

3.2 Przetwarzanie informacji niejawnych

W ustawodawstwie istnieje szereg ustaw regulujących różne aspekty przetwarzania informacji. Ustawodawstwo cały czas zmienia się i jest dostosowywane do nowych warunków i technologii.

3.2.1 Ustawy

- USTAWA z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Dz.U. 2010 nr 182 poz. 1228
- USTAWA z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach Dz.U.2011.123.698
- USTAWA z dnia 6 czerwca 1997 roku Kodeks Karny (Przestępstwa przeciwko ochronie informacji) Dz.U.1977.88.553
  - rozdział XXXIII Przestępstwa przeciwko ochronie informacji (art. 267 § 1 i 2, art. 268 § 2 oraz art. 296 § 1 i 2 kk);
  - rozdział XXXV Przestępstwa przeciwko mieniu (art. 278 § 2 i 5, art. 285 § 1, art. 287 § 1 oraz art. 293 § 1 kk);
  - rozdział XX Przestępstwa przeciwko bezpieczeństwu powszechnemu (art. 165 § 1 ust. 4, art. 165 § 2 i art. 167 § 2 kk);
  - rozdział XVII Przestępstwa przeciwko Rzeczypospolitej Polskiej (art. 130 § 2 i 3 oraz art. 138 § 2 kk);
  - rozdział XXXIV Przestępstwa przeciwko wiarygodności dokumentów (art. 270 § 1 kk).

- USTAWA z dnia 18 kwietnia 2002 roku o stanie klęski żywiołowej Dz.U.2002.62.558
- USTAWA z dnia 29 sierpnia 2002 roku o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej Dz.U. 2002 nr 156 poz. 1301
- USTAWA z dnia 21 czerwca 2002 roku o stanie wyjątkowym Dz.U.2002.113.985

3.2.2 Rozporządzenia

Szereg aspektów regulowanych jest w drodze rozporządzeń. Poniżej zamieszczono zebraną listę rozporządzeń:

- ROZPORZĄDZENIE Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych Dz.U.2012.683
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności Dz.U.2011.288.1692
- ROZPORZĄDZENIE Rady Ministrów z dnia z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych Dz.U.2011.276.1631
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne Dz.U.2011.271.1603
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 4 października 2011 roku w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa Dz.U.2011.220.1302
- ROZPORZĄDZENIE Rady Ministrów z dnia 22 czerwca 2011 roku w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych Dz.U.2011.196.1161
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 27 kwietnia 2011 roku w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych Dz.U.2011.93.541
- ROZPORZĄDZENIE Rady Ministrów z dnia z dnia 5 kwietnia 2011 roku w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego Dz.U.2011.86.470
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 22 marca 2011 roku w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych

przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających Dz.U.2011.67.356

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych Dz.U.2011.14.67

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa Dz.U.2010.258.1754

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa Dz.U.2010.258.1753

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów poświadczeń bezpieczeństwa Dz.U.2010.258.1752

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego Dz.U.2010.258.1751

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego Dz.U.2010.258.1750

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 26 lutego 2010 roku w sprawie postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa Dz.U.2010.34.181

- ROZPORZĄDZENIE Rady Ministrów z dnia 3 czerwca 2008 roku w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych Dz.U.2008.107.679

- ROZPORZĄDZENIE Ministra Kultury i Dziedzictwa Narodowego z dnia 22 maja 2006 roku w sprawie szczegółowych zasad i trybu gromadzenia, ewidencjonowania, kwalifikowania, klasyfikacji oraz udostępniania materiałów archiwalnych tworzących zasób jednostek publicznej radiofonii i telewizji Dz.U.2006.98.680

- ROZPORZĄDZENIE Rady Ministrów z dnia 25 Października 2005 roku w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych, podporządkowanych Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw zagranicznych, ministrowi właściwemu do

spraw finansów publicznych, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Kancelarii Sejmu, Szefowi Kancelarii Senatu i Szefowi Kancelarii Prezydenta Dz.U.2005.219.1847

- ROZPORZĄDZENIE Rady Ministrów z dnia 13 kwietnia 2006 roku w sprawie rodzaju informacji, które mogą naruszyć słuszny interes emitenta, oraz sposobu postępowania emitenta w związku z opóźnianiem przekazania do publicznej wiadomości informacji poufnych Dz.U.2004.95.947

- ROZPORZĄDZENIE Rady Ministrów z dnia 3 kwietnia 2003 roku w sprawie zakresu, warunków i trybu przekazywania Agencji Bezpieczeństwa Wewnętrznego informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez organy, służby i instytucje państwowe. Dz.U.2003.70.643

- ROZPORZĄDZENIE Ministra Kultury z dnia 16 września 2002 roku w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych. Dz.U.2002.167.1375

- ROZPORZĄDZENIE Ministra Kultury i Dziedzictwa Narodowego z dnia 13.12.2000 roku w sprawie określenia szczególnych wypadków i trybu wcześniejszego udostępniania materiałów archiwalnych Dz.U.2001.13.116

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 25.02.1999 roku w sprawie szczegółowego zakresu warunków i trybu szczegółowego współdziałania organów, służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających. Dz.U.1999.18.159

- Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych Dz.U. 2011 nr 276 poz. 1631, Dz.U. 2013 poz. 11

- Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych Dz.U. 2011 nr 14 poz. 67

- DECYZJA KOMISJI EUROPEJSKIEJ z dnia 29 listopada 2001 roku zmieniająca jej regulamin wewnętrzny - Przepisy Komisji w sprawie bezpieczeństwa 2001/844/WE, EWWiS, Euratom)

- ROZPORZĄDZENIE Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych Dz.U.2012.683

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 22 grudnia 2011 roku w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności Dz.U.2011.288.1692

- ROZPORZĄDZENIE Rady Ministrów z dnia z dnia 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych Dz.U.2011.276.1631
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 7 grudnia 2011 roku w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne Dz.U.2011.271.1603
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 4 października 2011 roku w sprawie współdziałania Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego w zakresie wykonywania funkcji krajowej władzy bezpieczeństwa Dz.U.2011.220.1302
- ROZPORZĄDZENIE Rady Ministrów z dnia 22 czerwca 2011 roku w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych Dz.U.2011.196.1161
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 27 kwietnia 2011 roku w sprawie przygotowania i przeprowadzania kontroli stanu zabezpieczenia informacji niejawnych Dz.U.2011.93.541
- ROZPORZĄDZENIE Rady Ministrów z dnia z dnia 5 kwietnia 2011 roku w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego Dz.U.2011.86.470
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 22 marca 2011 roku w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających Dz.U.2011.67.356
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 18 stycznia 2011 roku w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych Dz.U.2011.14.67
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa Dz.U.2010.258.1754
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa Dz.U.2010.258.1753
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów poświadczeń bezpieczeństwa Dz.U.2010.258.1752
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego Dz.U.2010.258.1751

- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 28 grudnia 2010 roku w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego Dz.U.2010.258.1750
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 26 lutego 2010 roku w sprawie postępowania z dokumentacją w komórkach organizacyjnych wykonujących zadania w zakresie obronności i bezpieczeństwa państwa Dz.U.2010.34.181
- ROZPORZĄDZENIE Rady Ministrów z dnia 3 czerwca 2008 roku w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych Dz.U.2008.107.679
- ROZPORZĄDZENIE Ministra Kultury i Dziedzictwa Narodowego z dnia 22 maja 2006 roku w sprawie szczegółowych zasad i trybu gromadzenia, ewidencjonowania, kwalifikowania, klasyfikacji oraz udostępniania materiałów archiwalnych tworzących zasób jednostek publicznej radiofonii i telewizji Dz.U.2006.98.680
- ROZPORZĄDZENIE Rady Ministrów z dnia 25 Października 2005 roku w sprawie sposobu i trybu udostępniania materiałów archiwalnych znajdujących się w archiwach wyodrębnionych, podporządkowanych Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw zagranicznych, ministrowi właściwemu do spraw finansów publicznych, Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu, Szefowi Kancelarii Sejmu, Szefowi Kancelarii Senatu i Szefowi Kancelarii Prezydenta Dz.U.2005.219.1847
- ROZPORZĄDZENIE Rady Ministrów z dnia 13 kwietnia 2006 roku w sprawie rodzaju informacji, które mogą naruszyć słuszny interes emitenta, oraz sposobu postępowania emitenta w związku z opóźnianiem przekazania do publicznej wiadomości informacji poufnych Dz.U.2004.95.947
- ROZPORZĄDZENIE Rady Ministrów z dnia 3 kwietnia 2003 roku w sprawie zakresu, warunków i trybu przekazywania Agencji Bezpieczeństwa Wewnętrznego informacji uzyskanych w wyniku wykonywania czynności operacyjno-rozpoznawczych przez organy, służby i instytucje państwowe. Dz.U.2003.70.643
- ROZPORZĄDZENIE Ministra Kultury z dnia 16 września 2002 roku w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych. Dz.U.2002.167.1375
- ROZPORZĄDZENIE Ministra Kultury i Dziedzictwa Narodowego z dnia 13.12.2000 roku w sprawie określenia szczególnych wypadków i trybu wcześniejszego udostępniania materiałów archiwalnych Dz.U.2001.13.116
- ROZPORZĄDZENIE Prezesa Rady Ministrów z dnia 25.02.1999 roku w sprawie szczegółowego zakresu warunków i trybu szczegółowego współdziałania organów, służb i innych państwowych jednostek organizacyjnych

ze służbami ochrony państwa w toku prowadzonych postępowań sprawdzających. Dz.U.1999.18.159

3.2.3 Zarządzenia

- ZARZĄDZENIE NR 3 MINISTRA SPRAW WEWNĘTRZNYCH z dnia 9 grudnia 2011 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego El.Dz.Urz.MSW.Zarz.nr 3

3.3 Przestępstwa komputerowe

Kwestie dotyczące postępowania w przypadku przestępstw komputerowych reguluje przede wszystkim Kodeks Karny w ustawie z 6 czerwca 1997 r. (Dz.U. 1997 nr 88 poz. 553), w kilku osobnych rozdziałach:

- rozdział XXXIII - Przestępstwa przeciwko ochronie informacji (art. 267 § 1 i 2, art. 268 § 2 oraz art. 296 § 1 i 2 kk);
- rozdział XXXV - Przestępstwa przeciwko mieniu (art. 278 § 2 i 5, art. 285 § 1, art. 287 § 1 oraz art. 293 § 1 kk);
- rozdział XX - Przestępstwa przeciwko bezpieczeństwu powszechnemu (art. 165 § 1 ust. 4, art. 165 § 2 i art. 167 § 2 kk);
- rozdział XVII - Przestępstwa przeciwko Rzeczypospolitej Polskiej (art. 130 § 2 i 3 oraz art. 138 § 2 kk);
- rozdział XXXIV - Przestępstwa przeciwko wiarygodności dokumentów (art. 270 § 1 kk).

Odpowiednie przepisy wykonawcze i wprowadzające można znaleźć w: Dz.U. 1997 nr 88 poz. 554, Dz.U. 1997 nr 90 poz. 557)

Niektóre rozwiązania można znaleźć także w Kodeksie Cywilnym Dz.U. 2014 poz. 121) w art.23 (ochrona korespondencji).

3.4 Podpis elektroniczny

Podpis elektroniczny jest zbiorem środków technicznych, organizacyjnych oraz prawnych, które zapewniają autentyczność oraz skutki prawne dokumentów elektronicznych. Podpis elektroniczny jest realizowany za tzw. podpisu cyfrowego. Podpis elektroniczny może być równoważny pod względem skutków prawnych podpisowi własnoręcznemu jeżeli można go uznać za tzw. podpis elektroniczny bezpieczny, który (zgodnie z ustawą):

- jest przyporządkowany wyłącznie do osoby składającej ten podpis,
- jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,

- jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Skutki prawne zapisane w art. 781 § 2 Kodeksu Cywilnego. Traktuje on o tzw. oświadczenie woli: *Oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej, chyba że ustawa lub czynność prawna zastrzega inaczej.*

Najważniejsze ustawy dotyczące podpisu elektronicznego to:

- Ustawa z dnia 21 lipca 2006 r. o zmianie ustawy o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych oraz ustawy o podpisie elektronicznym Dz.U. 2006 nr 145 poz. 1050

- Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym Dz.U. 2001 nr 130 poz. 1450

3.5 Informatyzacja podmiotów publicznych

W związku z obowiązującym ustawodawstwem unijnym oraz koniecznością wymuszenia odpowiedniego postępowania w projektowany oraz użytkowaniu systemów informatycznych została stworzona odpowiednia ustawa, która nakłada na jednostki publiczne określone wymagania. Do ustawy zostało wydanych szereg rozporządzeń specjalnie do tego powołanego Ministra Administracji i Cyfryzacji. Akty prawne regulują m.in. zasady przetwarzania dokumentów elektronicznych w związku z powstałymi na przestrzeni lat systemami do elektronicznego przetwarzania dokumentów, w tym systemu ePUAP - elektronicznej Platformy Usług Administracji Publicznej (https://epuap.gov.pl/wps/portal).

3.5.1 Ustawy

- Ustawa z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw Dz.U. 2014 poz. 183

- USTAWA z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne Dz.U. 2005 nr 64 poz. 565

3.5.2 Rozporządzenia

- Dz.U. 2014 nr 0 poz. 1671 Rozporządzenie Rady Ministrów z dnia 27 listopada 2014 r. zmieniające rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

- Dz.U. 2014 nr 0 poz. 778 Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 5 czerwca 2014 r. w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej

- Dz.U. 2014 nr 0 poz. 590 Rozporządzenie Prezesa Rady Ministrów z dnia 8 maja 2014 r. zmieniające rozporządzenie w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych

- Dz.U. 2014 nr 0 poz. 584 Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej

- Dz.U. 2012 nr 0 poz. 526 Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

- Dz.U. 2011 nr 206 poz. 1216 Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych

- Dz.U. 2011 nr 93 poz. 545 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników

- Dz.U. 2010 nr 177 poz. 1195 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych

- Dz.U. 2010 nr 113 poz. 757 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 czerwca 2010 r. w sprawie wysokości wynagrodzenia członków Rady Informatyzacji

- Dz.U. 2005 nr 217 poz. 1836 Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania

3.6 Polityka bezpieczeństwa

Polityka bezpieczeństwa organizacji (rozważana w odniesieniu do bezpieczeństwa systemu informatycznego) definiuje sposoby wykorzystywania kont użytkowników i danych przechowywanych w systemie. Polityka bezpieczeństwa informacji to dokument opisujący założenia dotyczące zabezpieczenia informacji. Polityka bezpieczeństwa nie jest pojęciem jednoznacznym, gdyż może chodzić o:

- Politykę bezpieczeństwa jako dokument całościowy,

- Politykę bezpieczeństwa w rozumieniu Ustawy o Ochronie Danych Osobowych,

- Politykę bezpieczeństwa opisującą założenia tylko dla wybranego systemu IT.

Całościowa polityka bezpieczeństwa, rzadko zawiera bardzo szczegółowe i kompletne informacje dotyczące przyjętych założeń dla danego obszaru. Szczegółowe rozwiązania opisane są w innych dokumentach.

Określaniem polityki bezpieczeństwa zajmują się zarząd organizacji, a także osoby odpowiedzialne za bezpieczeństwo w ścisłej współpracy z administratorami systemu informatycznego. Określanie strategii realizacji polityki bezpieczeństwa należy administratorów, natomiast zadania opracowywania i realizacji taktyk współdzielą administratorzy i użytkownicy.

Należy dbać, aby polityka bezpieczeństwa była dokumentem spisanym i była przeczytana i zrozumiana przez wszystkich pracowników organizacji użytkujących systemy komputerowe.

Nowi pracownicy powinni podlegać obowiązkowi zaznajamiania się z dokumentem opisującym politykę bezpieczeństwa. W związku z tym dokument ten nie powinien mieć charakteru zbyt abstrakcyjnego. Dokument ten musi być zrozumiały dla użytkowników, w związku z tym musi być pisany zrozumiałym językiem bez niezrozumiałych ogólników i legislacyjnych sformułowań. Może zaistnieć potrzeba stworzenia dokumentu sformalizowanego na skutek np. wymogów odgórnych czy wymogami prawnymi. Dokument taki jest najczęściej nieczytelny dla większości użytkowników. Należy stworzyć drugą, bardziej praktyczną wersję dokumentu, przeznaczoną ogółu pracowników.

Nie należy również na siłę starać się upodobnić polityki bezpieczeństwa organizacji do funkcjonujących w tej dziedzinie standardów. Każda organizacja jest inna, posiada swoją specyfikę i z tego względu powinna mieć odrębną, własną politykę bezpieczeństwa.

Należy wziąć pod uwagę koszty realizacji projektując politykę bezpieczeństwa, czy organizacja będzie w stanie je ponieść. Niestety bezpieczeństwo zapewniane jest zwykle kosztem wygody i efektywności. Czy ograniczenie funkcjonalności systemu nie przełoży się na ograniczenie dynamiki funkcjonowania organizacji.

Niedociągnięcia w systemie bezpieczeństwa a bezpieczeństwo Trzeba zwrócić uwagę, że małe niedociągnięcia w systemie bezpieczeństwa mogą pozytywnie wpłynąć pozytywnie na jego poziom. Spowodowane jest to tym, że świadomość niebezpieczeństwa połączona z obawą przed jego wystąpieniem. Powoduje to zaostrzenie czujności administratorów i użytkowników systemu dając w efekcie poprawę poziomu zabezpieczeń.

Zawartość polityki bezpieczeństwa Każda polityka bezpieczeństwa powinna zawierać szereg danych oraz powinna mieć pewne cechy przedstawione poniżej:

- Wyjaśnienia. Polityka bezpieczeństwa powinna być czytelna i zrozumiała. Oprócz zasad postępowania powinna zawierać uzasadnienia dlaczego zasady są takie a nie inne. W dokumencie powinny znajdować się wyjaśnienia zalecanych metod ochrony. Większość ludzi jest gotowa zastosować się do określonych wymogów w sytuacji gdy jest jasne dlaczego takie właśnie są i dlaczego są ważne.

- Podział odpowiedzialności. W polityce bezpieczeństwa powinien znaleźć się podział kompetencji i odpowiedzialności. Informacje takie czynią sytuacje jasnymi i pozytywnie wpływają na organizację działań.

- Jasne sformułowania. Język, którym jest napisany dokument polityki bezpieczeństwa powinien być prosty i zrozumiały. Piszący ten dokument powinni pamiętać, że nie jest on dowodem ich elokwencji lecz ma efektywnie definiować zasady bezpieczeństwa.

- Opis mechanizmów realizacji polityki bezpieczeństwa Nawet najlepiej opracowana polityka bezpieczeństwa na nic się nie zda jeśli nie będzie realizowana w praktyce. Aby była realizowana muszą istnieć mechanizmy wymuszające realizację. Mechanizmem takim może być np. uczynienie odpowiednich osób odpowiedzialnymi za realizację polityki bezpieczeństwa.

Można wymienić także zagadnienia, które nie powinny zostać umieszczone w polityce bezpieczeństwa. Należą do nich:

- Szczegóły techniczne. Polityka bezpieczeństwa definiuje metody zapewniania odpowiednio wysokiego poziomu bezpieczeństwa organizacji. Szczegóły techniczne powinny znaleźć się w opisie strategii i taktyk zapewniania bezpieczeństwa organizacji.

- Bezkrytycznie wziętych zapożyczeń z innych polityk. Każda organizacja ma pewną specyfikę, więc bezkrytyczne kopiowanie elementów z polityk innych organizacji jest więc silnie odradzane. Można natomiast wykorzystać elementy, które mają swoje uzasadnienie w danej organizacji.

Bezpieczeństwo informacji w systemach IT rozumiane jest jako zapewnienie:

- Poufności informacji - ochrona danych przed dostępem osób trzecich.

- Integralności informacji - uniknięcie nieautoryzowanych zmian w danych.

- Dostępności informacji - zapewnienie dostępu do danych, w każdym momencie żądanym przez użytkownika.

- Rozliczalności operacji wykonywanych na informacjach - przechowywania pełnej historii dostępu do danych, wraz z informacją kto taki dostęp uzyskał i ewentualnie jakich zmian dokonał.

Typy zagadnień zawieranych w opracowywanych politykach bezpieczeństwa

- Zdefiniowanie wymagań dot. haseł; na ile powinny być zawikłane (nietrywialne), czy można je ujawniać współpracownikom lub przełożonym; określenie okresów ważności haseł itp.

- Określenie zasad przyłączania się i korzystania z globalnej sieci komputerowej; określenie osób, której mają do tego prawo. Określenie zakresu i zasad udostępniania informacji instytucji użytkownikom globalnej sieci komputerowej (np. przez www czy ftp).

- Zobligowanie pracowników do wyrażenia zgody na wykonywanie przez administratorów czynności związanych z bezpieczeństwem instytucji.

- Określenie zasad korzystania ze zdalnych połączeń z instytucją; opisanie zasad korzystania z systemu przez osoby znajdujące się w oddaleniu od niego (czy przez sieć globalną czy przez łącza telefoniczne).
- Określenie metod ochrony informacji o finansach i pracownikach firmy.
- Określenie zasad sporządzania i przechowywania wydruków informacji zw. z instytucją.
- Określenie metod ochrony przed wirusami.

Powody zmian polityki bezpieczeństwa Raz opracowana polityka bezpieczeństwa instytucji będzie funkcjonować w niej zawsze ze względu na:

- Zmiany struktury.
- Zmiany wielkości.
- Zmiany struktury zatrudnienia (nowi pracownicy).
- Zmieniające się system informatyczne.
- Zmiany otaczającego świata (np. rozwój globalnej sieci komputerowej i wzrost liczby związanych z nim zagrożeń).

Polityka bezpieczeństwa powinna być ciągle dostosowywana do pojawiających się nowych sytuacji i potrzeb.

Opracowywanie i realizacja polityki bezpieczeństwa ma ścisły związek z ogólnym zarządzaniem organizacją. Bezpieczeństwo wymaga pracy i środków finansowych. Bez przychylności zarządu instytucji nie ma mowy o prawidłowym zarządzaniu bezpieczeństwem. Do kadry inżynierskiej organizacji należy więc uświadamianie zagrożeń i potencjalnych strat związanych z nie zapewnieniem instytucji należytego bezpieczeństwa.

Strategie realizacji polityki bezpieczeństwa Spisane strategie bezpieczeństwa tworzą dokument zwany planem ochrony. Plan ochrony opracowywany jest głównie przez osoby opiekujące się systemem informatycznym. Jego realizacja ciąży zarówno na administratorach, jak i na pozostałych użytkownikach systemu.

Plan bezpieczeństwa

- Opis realizacji metod kontroli dostępu do systemu.
- Opis realizacji metod kontroli dostępu do zasobów systemu.
- Opis metod okresowego lub stałego monitorowania systemu.
- Dokładny (na poziomie technicznym) opis metod reagowania na wykrycie zagrożenia.
- Opis metod likwidacji skutków zagrożeń (np. tworzenia kopii zapasowych).
- Zapewnianie bezpieczeństwa dzięki wielowarstwowemu mechanizmowi ochrony ograniczanie fizycznego dostępu do systemu komputerowego.

- Zamykanie komputerów w pomieszczeniach, do których dostęp odbywa się przy uwierzytelnieniu np. za pomocą karty magnetycznej lub wprowadzeniu kodu dostępu na klawiaturze przy drzwiach. Dodatkowo dostęp do drzwi takiego pomieszczenia może być chroniony przez kolejne punkty wartownicze z pracownikami ochrony. W powyższy sposób chronione są systemy wymagające największego poziomu bezpieczeństwa, np. w organizacjach rządowych lub w wojsku. Zwykle systemy takie nie są podłączone do globalnej sieci komputerowej, lecz korzystają z własnych sieci telekomunikacyjnych. Zaistnienie zagrożenia w takim systemie automatycznie kieruje podejrzenia na wąskie grono osób mających do nich dostęp.
- Zapewnianie bezpieczeństwa dzięki wielowarstwowemu mechanizmowi ochrony. Kolejną warstwą ochrony może być procedura uwierzytelniania użytkownika rozpoczynającego pracę w systemie. Procedura ta ma na celu ochronę przed nielegalnym dostępem do systemu. Najczęściej procedura taka wykonywana jest z wykorzystaniem haseł. Aby procedura ta zapewniała odpowiednio wysoki poziom bezpieczeństwa, hasło powinno być kontrolowane na etapie tworzenia. Hasło powinno wykazywać odpowiedni stopień zawiłości (nie powinno być oczywiste), np. powinno się nie dopuszczać haseł, które wywodzą się z nazwy lub opisu użytkownika, są zbyt krótkie, zawierają zbyt ubogi wachlarz znaków, były już stosowane, wynikają z kodu klawiatury itp. Istnieje szereg narzędzi, zarówno dostarczanych z systemami operacyjnymi, jak i dodatkowych, służących do kontroli zawiłości haseł (np. npasswd, passwd+, goodpw, crack). Niektóre z tych narzędzi tworzą słowniki najpopularniejszych wyrażeń (wśród których są nazwy użytkowników systemu) i stosując pewien zbiór reguł próbują wygenerować niebezpieczne hasła, które później nie są dopuszczane do użytkowania.

Kontrola jakości haseł Użytkownicy niechętnie zmieniają hasła (jest to niewygodne) i w związku z tym starają się posługiwać małą liczbą haseł (np. dwoma) na zmianę. Aby utrudnić takie działanie, w systemie tworzona jest lista historii haseł. Oczywiście rozwiązanie takie sprawdzi się, jeżeli jest dostatecznie silne ograniczenie na czas używania haseł.

Dodatkowe metody uwierzytelniania Do uwierzytelniania użytkowników można stosować różne rodzaje kart:

- Karty inteligentne.
- Karty telefoniczne.
- Karty procesorowe.

Do uruchomienia karty, konieczne jest podanie przez użytkownika osobistego numeru identyfikacyjnego PIN (*ang. Personal Identification Number*). Karty mogą działać na różnorakie sposoby. Jeden z najpopularniejszych to protokół typu wezwanie-odpowiedź. System generuje pewną losową liczbę i podaje ją użytkownikowi. Ten wprowadza ją do karty, która szyfruje liczbę i rezultat szyfrowania zwracany jest do systemu. System sprawdza, czy liczba została zaszyfrowana poprawnie (metoda ta oparta jest na tzw. kryptograficznym protokole uwierzytelniania ze współdzielonym kluczem).

Inna metoda wykorzystania karty polega na tym, że liczba, którą należy podać systemowi, generowana jest przez kartę po wprowadzeniu numeru identyfikacyjnego (ta metoda z kolei wykorzystuje protokół Lamporta - S/KEY - hasła jednorazowe). Karta musi być uprzednio zainicjowana w systemie, z którym będzie współdziałać.

Dodatkowe metody uwierzytelniania Do dodatkowych metod uwierzytelniania należą:

- Procedura hasła telefonicznego, które musi być podawane przy rozpoczynaniu pracy w systemie z wykorzystaniem połączeń telefonicznych.
- Dodatkowe pytanie zadawane po zaakceptowaniu hasła dostępu. Zadawane pytanie może dotyczyć preferencji użytkownika. Wymaga to wcześniejszego zadeklarowania poprawnych odpowiedzi. Metoda ta zakłada, że jeśli intruz złamie hasło użytkownika, to nie będzie znał odpowiedzi na ustalone pytanie.

Różnicowanie typów mechanizmów ochrony Różnicowanie mechanizmów ochrony jest bardzo ważne z punktu widzenia systemu. W przypadku zastosowania tylko jednego rodzaju zabezpieczeń, przełamanie ich powoduje problemy z bezpieczeństwem. Różne mechanizmy ochrony mogą obejmować:

- Stosowanie produktów zabezpieczających np. pochodzących od różnych dostawców znacznie zmniejsza prawdopodobieństwo utraty bezpieczeństwa całego systemu, gdy zawiedzie jego jedno ogniwo, zwłaszcza w sytuacji, gdy metoda ta połączona jest z wielowarstwowym mechanizmem ochrony. Należy mieć na uwadze, że administrowanie takim zróżnicowanym systemem bezpieczeństwa może być znacznie bardziej złożone niż administrowanie systemem jednolitym; jak zwykle, wyższy poziom bezpieczeństwa okupiony jest większymi niedogodnościami użytkowania systemu.
- Wydzielanie i monitorowanie punktów wymiany informacji systemu z otoczeniem
- Świadome kreowanie i eksponowanie słabych punktów

  Strategia ta polega na zastosowaniu pewnego triku polegającego na świadomym wyborze i eksponowaniu fragmentów systemu, które w opinii włamywacza mają uchodzić za słabe punkty. Odwraca to wówczas uwagę intruza od pozostałych części systemu. Należy oczywiście zadbać o to, aby poziom ochrony w tych słabych punktach był dostatecznie wysoki dla uniemożliwienia przeprowadzenia udanego ataku.
- Automatyczne blokowanie się systemu w przypadku wykrycia włamania

  W strategii tej w przypadku wykrycia zagrożenia system sam blokuje w mniejszym lub większym stopniu swoje działanie uniemożliwiając intruzowi wyrządzanie szkód. Oczywiście ogranicza to (bądź blokuje) możliwości pracy legalnych użytkowników. Jednocześnie system zapewnia zapis swojego stanu w momencie wykrycia zagrożenia, co później ułatwia likwidację ewentualnych szkód lub lokalizację wyłomu w systemie bezpieczeństwa.

- Hierarchizacja uprawnień użytkowników systemu

  Użytkownicy pełniący funkcje administracyjne mają większe prawa niż użytkownicy tych funkcji nie pełniący. Administratorzy poszczególnych podsystemów (np. podsystemu drukowania czy podsystemu poczty elektronicznej) posiadają mniejsze prawa niż administratorzy główni itd. Obowiązuje zasada przyznawania minimum uprawnień. Dzięki temu w przypadku zagrożenia na niebezpieczeństwo narażony jest tylko fragment systemu.

3.6.1 Reakcje na próby ataku na system

Bardzo ważną sprawą jest prawidłowa reakcja na wykrycie faktu udanego bądź nieudanego ataku na bezpieczeństwo systemu. W razie wykrycia na przykład działania dziwnych procesów w systemie, wielokrotnych prób zalogowania się na pewne konto czy modyfikacji pliku lub katalogu, należy natychmiast podjąć zaplanowane uprzednio środki bezpieczeństwa. Obejmują one następujące działania:

- Szczegółowa analiza zaistniałej sytuacji.
- Zatrzymanie pracy całego lub części systemu w celu zapobieżenia powstaniu nowych szkód.
- Poinformowanie użytkowników o zaistniałym zagrożeniu.
- Zapis stanu systemu w celu późniejszej dokładnej analizy.
- Odtworzenie ostatnio zachowanego stanu systemu z archiwów.
- Konieczność wcześniejszego opracowania planu działania w przypadku awarii.

W celu wyeliminowania efektów działań intruza należy odtworzyć poprzedni stan systemu. Należy przy tym pamiętać, że poprzedni stan systemu może również zawierać modyfikacje wprowadzone przez napastnika, o ile zagrożenie nastąpiło po jego zapisie. Prawdopodobnie zostaną utracone modyfikacje systemu, jakie wykonano przed sporządzeniem ostatniej kopii zapasowej.

Plan wstrzymywania pracy systemu zawierający opis sposobu sprawnego informowania użytkowników. Działanie zgodnie z opracowanym wcześniej planem znacząco ułatwia likwidację skutków zagrożenia.

3.7 Administrator Bezpieczństwa Informacji

Funkcja Administratora Bezpieczeństwa Informacji (ABI)została wprowadzona na mocy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji (03.06.98) obok Administratora Danych Osobowych (ADO). Obowiązkiem ABI ma być przeciwdziałanie dostępowi osób niepowołanych do systemu oraz podejmowanie odpowiednich działań w przypadku naruszeń w systemie zabezpieczeń. Bardzo często zdarza się, że powołana funkcja koliduje z dotychczasowym zakresem obowiązków administratora systemu informatycznego, który może utrudniać realizację zadań uważając ją za niepotrzebną.

Przykładowe zadania administratora bezpieczeństwa informacji można zapisać w punktach:

Do zadań administratora bezpieczeństwa informacji zgodnie z (Art. 36a ust 2) ustawy należy:

1. Zapewnianie przestrzegania przepisów o ochronie danych osobowych (Art. 36a ust 2 pkt 1).

2. Prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 (Art. 36a ust 2 pkt 2).

3. Wykonywanie innych zleconych przez ADO obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań wymienionych w pkt. 1 i 2 (Art. 36a ust 4).

3.8 Generalny Inspektor Ochrony Danych Osobowych

Generalny Inspektor Ochrony Danych Osobowych (w skrócie http://www.giodo.gov.pl/) - organ do spraw ochrony danych osobowych działający na podstawie http://pl.wikipedia.org/wiki/Ustawa_o_ochronie_danych_osobowych.
W 2010 roku nastąpiła nowelizacja ustawy, której tekst ujednolicony został opublikowany w Dz.U. 2014 poz. 1182. Definicja 3.1 opisuje (dane osobowe rozumiane wg powyższej ustawy.

Definicja 3.1. *Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osoba zidentyfikowana znana z imienia i nazwiska np. Jan Kowalski, ul. Kryształowa 1, Piotrków Tryb. Osoba możliwa do zidentyfikowania to np.: autor książki, właściciel firmy XXX w Piotrkowie Tryb., posiadacz polisy ubezpieczeniowej nr XXX-10.*

W ustawie mówi się o osobie możliwej do zidentyfikowania, której definicja 3.2 jest zgodna z ustawą.

Definicja 3.2. *Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.*

Zgodnie z ustawą informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu i działań. Danymi osobowymi będą zatem zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia.

Daną osobową będzie taka informacja, która pozwala na ustalenie tożsamości danej osoby, bez nadzwyczajnego wysiłku i nakładów, zwłaszcza przy wykorzystaniu łatwo osiągalnych i powszechnie dostępnych źródeł. Poza zakresem przedmiotowej definicji znajdzie się zatem taka informacja, na podstawie

której identyfikacja osoby wymagać będzie nieracjonalnych, nieproporcjonalnie dużych nakładów kosztów, czasu lub działań.

Ustawodawca formułując art. 6 ustawy o ochronie danych osobowych posłużył się klauzulą generalną. Tym samym nie określił zamkniętego katalogu informacji stanowiących dane osobowe. Dlatego też przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, w większości przypadków, nieuniknione jest dokonanie zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.

W ustawie mówi się także o danych wrażliwych, które podlegają szczególnej ochronie (dane ujawniające): pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, informację o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, dotyczące skazań, orzeczeń o ukaraniu, mandatów karnych, innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Dane wrażliwe można przetwarzać wyłącznie wtedy, gdy:

- pozwala na to przepis prawa (ustawa),
- osoba wyraziła na to zgodę na piśmie,
- dane wrażliwe jej dotyczące zostały przez nią upublicznione.

3.8.1 Zadania

GIODO kontroluje zgodność przetwarzania danych z przepisami ustawy, wydaje decyzje administracyjne i rozpatruje skargi w sprawach wykonania przepisów o ochronie danych osobowych, prowadzi rejestr zbiorów danych, opiniuje akty prawne dotyczące ochrony danych osobowych, inicjuje i podejmuje przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych, uczestniczy w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych (np. Grupy roboczej art. 29).

Jest powoływany na 4-letnią kadencję (liczoną od dnia złożenia przysięgi) przez Sejm RP za zgodą Senatu. W zakresie wykonywania swoich zadań podlega tylko ustawie. Przysługuje mu immunitet.

W celu wykonania swoich zadań ma do pomocy Biuro Generalnego Inspektora Ochrony Danych Osobowych, którego siedziba znajduje się w Warszawie.

Zgodnie z art. 20 ustawy, raz w roku Generalny Inspektor składa Sejmowi sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych. Sprawozdanie jest dostępne w formie druku sejmowego.

3.8.2 Kontrola

Kontrola ze strony GIODO obejmuje szerokie spektrum zagadnień. Zadaniem kontroli jest uzyskanie odpowiedzi na następujące pytania:

- Czy podmiot ma prawo przetwarzać dane (spełnia przesłanki legalności)?
- Czy te dane są odpowiednie do celu przetwarzania?
- Czy zarejestrowano zbiory danych osobowych?

- Czy powołany został ABI?
- Czy dane osobowe są odpowiednio zabezpieczone?

Przebieg kontroli wyjaśnienia składa administrator danych (ADO) i osoby przez niego wskazane kontrolerzy przygotowują protokół kontroli (można do niego wnieść uwagi) w protokole nie ma informacji, czy dane są przetwarzane prawidłowo czy nie. Protokół opisem stanu rzeczywistego. W przypadku nieprawidłowości GIODO wszczyna postępowanie administracyjne w celu *przywrócenia zgodności z prawem.*

Postępowanie administracyjne Jeśli w trakcie kontroli zostaną wykryte nieprawidłowości i administrator danych ich nie usunie GIODO może podjąć działania egzekucyjne takie jak: grzywna, wykonanie zastępcze, przymus bezpośredni. Zgodnie z przepisami grzywnę można nałożyć na:

- osobę fizyczną - maksymalnie 10 tys. zł,
- osobę prawnę (np. spółkę posiadającą osobowość prawną) - maksymalnie 50 tys. zł.

W przypadku konieczności wielokrotnego nałożenia grzywny odpowiednie stawki kar ulegają zwielokrotnieniu i wynoszą:

- 50 tys. zł dla osób fizycznych,
- 200 tys. zł dla osób prawnych.

Rozdział 4

Bezpieczeństwo systemów operacyjnych

Na świecie funkcjonuje wiele organizacji, które zajmują się standaryzacją. W dziedzinie bezpieczeństwa komputerowego do najbardziej znanych organizacji standaryzujących należą:

- NCSC - National Computer Security Center, Department of Defence,
- NBS - National Bureau of Standards, Department of Commerce,
- ANSI - American National Standards Institute,
- ISO - International Organization for Standarization.

Organizacje te wypracowują standardy i zalecenia publikowane w formie norm i standardów. Do najbardziej znanych dokumentów i standardów należą:

- Trusted Computer Systems Evaluation Criteria, DoD, USA, *The Orange Book*, 1985, [1].
- Department of Trade and Industry Commercial Computer Security Centre, *The Green Books*, Wlk. Brytania, 1989.
- Zerntralstelle fuer Sicherheit in der Informationstechnik *The Green Book*, Niemcy, 1989, [**?**, STD:TheGreenBooks]
- Information Technology Security Evaluation Criteria (*Harmonised Criteria of France*, Germany, the Netherlands, the UK), 1991, [7].

Standard The Orange Book jest najpowszechniej stosowanym z w/w standardów. Nazwa Orange Book (Pomarańczową Księgą) pochodzi od koloru okładki dokumentu. W dokumencie zawarto wymagania, co do systemów przetwarzających poufne informacje oraz dane, informację na temat sposobu wykonywania analiz bezpieczeństwa, a także zalecenia dotyczące zapewniania bezpieczeństwa systemu informatycznego. Różne poziomy określają różne sposoby zabezpieczenia sprzętu, oprogramowania i danych. Klasyfikacja ta jest tak sformułowana, że wyższe poziomy klas zabezpieczeń posiadają wszystkie cechy poziomów niższych.

W standardzie tym wykorzystywany jest formalny model polityki bezpieczeństwa podany przez Bella i La Padulę (https://en.wikipedia.org/wiki/Bell-LaPadula_model) w 1976r. Model ten, z wykorzystaniem matematyki (teorii zbiorów), definiuje pojęcia stanu bezpieczeństwa i elementarnych trybów dostępu do obiektu oraz określa zasady przyznawania podmiotom określonych trybów dostępu do obiektów. The Orange Book zawiera także dowód twierdzenia zwanego Podstawowym Twierdzeniem Bezpieczeństwa (*ang. Basic Security Theorem*) mówiącego, iż zastosowanie dowolnej sekwencji reguł do systemu, który jest w stanie bezpiecznym spowoduje przejście systemu do innego stanu, który jest również bezpieczny. Standard zawiera również opis wymogów dotyczących zapewniania bezpieczeństwa systemu informatycznego, do których należą:

- Polityka bezpieczeństwa - musi istnieć jasna i dobrze zdefiniowana polityka bezpieczeństwa systemu. Mało tego - muszą istnieć mechanizmy wymuszające jej realizację i praktyczne stosowanie.
- Opis obiektów - każdy obiekt systemu musi być opisany za pomocą następujących informacji:
  - poziom ochrony, do którego obiekt należy (tzn. klasyfikacja obiektów wg kryterium bezpieczeństwa);
  - dostępu podmiotów, które potencjalnie mogą starać się o dostęp do obiektu.
- Identyfikacja - podmioty muszą być nazwane, aby możliwa była ich identyfikacja.
- Audyt - informacje z audytu muszą być gromadzone, rejestrowane i przechowywane w bezpieczny sposób w celu umożliwienia wykonania dokładnej analizy ewentualnych zagrożeń.
- Pewność - system komputerowy musi zawierać sprzętowe i/lub programowe mechanizmy zabezpieczeń, które można w sposób niezależny ocenić pod względem stopnia spełniania w/w wymogów.
- Ciągła ochrona - mechanizmy ochrony muszą być stale chronione przed nieautoryzowanym dostępem. W przeciwnym wypadku niemożliwe jest utrzymanie odpowiedniego poziomu ochrony.

4.0.3 Klasy bezpieczeństwa

Ocena poziomu bezpieczeństwa danego systemu na bazie The Orange Book polega na zakwalifikowaniu go do którejś z poniższych klas. Jeżeli system spełnia wymogi klasy wyższej to spełnia także wymogi klasy niższej. Klasy uszeregowane są w kolejności od mniej do bardziej restrykcyjnych):

klasa D klasa minimalnej ochrony.

D1 - minimalna ochrona (*ang. minimal protection*). Klasa ta jest określona jako najniższy poziom bezpieczeństwa oznaczający całkowity

brak wiarygodności systemu. Poziom ten nie wymaga certyfikacji, ponieważ cechuje go brak jakichkolwiek zabezpieczeń. Jedyne co można zrobić to ograniczyć fizyczny dostęp do systemu. Każdy użytkownik, który ma dostęp do systemu może w tym systemie dokonać dowolnych zmian. Do klasy tej włączane są systemy, które były oceniane ale nie zostały zakwalifikowane do żadnej z pozostałych klas. Do tej klasy należą także systemy pozornie bezpieczne, czego przykładem może być procedura autoryzacji dostępu w sieciowych komputerach zaopatrzonych w system operacyjny Microsoft Windows. Użytkownik pytany jest tylko o identyfikator i hasło (wystarczy podać wymyślone dane), by uzyskać dostęp do lokalnych zasobów komputera. Trochę lepiej wygląda to w przypadku zabezpieczenia zasobów przed dostępem z innych komputerów w sieci, jednak i w tym przypadku Microsoft Windows nie należy jednak do klasy D1.

klasa C - ochrona uznaniowa.

C1 - dobrowolna kontrola dostępu (*ang. discretionary security protection*) - klasa ta zapewnia separację użytkowników i danych. Każdy użytkownik kontroluje dostęp do obiektów, których jest właścicielem i zezwala na dostęp według własnego uznania. Dostęp może być inny dla właściciela, grupy czy pozostałych użytkowników (np. prawa dostępu w systemie Unix/Linux). Przed rozpoczęciem pracy w systemie użytkownik musi zalogować się do systemu podając swoje hasło. System operacyjny kontroluje uprawnienia użytkowników do odczytu i zapisu plików i kartotek oraz dysponuje mechanizmem autoryzacji i dostępu. System taki nie ma na ogół zdefiniowanego tzw. superużytkownika (administratora) lub użytkownik taki nie jest bardziej zabezpieczony niż pozostali członkowie systemu. Klasa C1 jest także pozbawiona mechanizmów rejestrowania zdarzeń (*ang. auditing logging*). Informacja o nazwach kont użytkowników oraz zakodowane hasła są dostępne dla wszystkich użytkowników. Istnieje duże niebezpieczeństwo rozkodowania hasła na podstawie zakodowanego ciągu (starsze systemy Linuksowe nie posiadały maskowania haseł - *ang. shadowing* przez, co zakodowane hasła były dostępne dla wszystkich w pliku /etc/passwd).

C2 - dostęp kontrolowany (*ang. controlled access protection*) - systemy tej klasy wymuszają silniejszy poziom ochrony niż dla klasy C1 poprzez wprowadzenia procedur logowania, mechanizmów audytu i izolacji zasobów systemowych. Dodatkowo poziom ten gwarantuje automatyczne rejestrowanie wszystkich istotnych z punktu widzenia bezpieczeństwa zdarzeń i zapewnia silniejszą ochronę kluczowych danych systemowych takich jak np. baza danych haseł użytkowych. Zakodowane hasła użytkowników dostępne są tylko dla systemu operacyjnego. Istnieje także możliwość zablokowania niektórych instrukcji poszczególnym użytkownikom.

klasa B - ochrona z etykietowaniem.

B1 - etykiety poziomu bezpieczeństwa (*ang. labeled security protection*) - systemy te posiadają wszystkie właściwości systemów klasy C2. Dodatkowo wprowadzony jest element etykietowania podmiotów i obiektów (opisywania ich właściwości w systemie bezpieczeństwa). Etykiety pozwalają na stopniowanie poziomu poufności obiektów i poziomu zaufania do poszczególnych użytkowników. Klasa ta obsługuje bezpieczeństwo na kilku poziomach takich jak *tajne* oraz *ściśle tajne*. Ma wdrożone mechanizmy uznaniowej kontroli dostępu do zasobów systemu, co może np. sprowadzić się do braku możliwości zmiany charakterystyki dostępu do plików i kartotek przez określonego użytkownika. Klasa ta blokuje możliwość praw dostępu do obiektu przez jego właściciela.

B2 - zabezpieczenie strukturalne (*ang. structure protection*) - klasa ta posiada jasno zdefiniowaną i udokumentowaną politykę bezpieczeństwa. Ponadto musi być przyjęty podział na część krytyczną pod względem ochrony (*ang. protection-critical*) i resztę. Poziom ten wymaga przypisania każdemu obiektowi systemu komputerowego etykiety bezpieczeństwa określającej status tego obiektu w odniesieniu do przyjętej polityki bezpieczeństwa, np. gdy użytkownik żąda dostępu do obiektu typu plik - system ochrony akceptuje lub odrzuca to żądanie na podstawie zawartości etykiet bezpieczeństwa tego obiegu względem użytkownika. Etykiety te mogą zmieniać się dynamicznie w zależności od tego, co jest aktualnie użytkowane. W dodatku muszą być wzmocnione mechanizmy uwierzytelniania oraz narzędzia administrowania bezpieczeństwem systemu. System musi być względnie odporny na penetrację.

B3 - obszary poufne (*ang. security domains*) - w klasie tej system posiada silne wsparcie dla administracji bezpieczeństwem, mechanizm audytu rozszerzony do reagowania na sygnały związane z bezpieczeństwem. Wymagana jest procedura odtwarzania stanu systemu. Obowiązkowym jest chronienie zarówno przechowywanej jak i przesyłanej informacji, czyli ochrona przed możliwością podsłuchu elektronicznego prowadzącego do przechwycenia przesyłanych danych. System jest wysoce odporny na penetrację.

klasa A realizacja zweryfikowana.

A1 - zweryfikowana realizacja systemu (*ang. verified design*) - systemy tej klasy są funkcjonalnie równoważne systemom klasy B3. Dodatkowo posiadają możliwość weryfikacji czy cała konfiguracja sprzętowo - programowa jest poprawnie zaimplementowana. Zarówno sprzęt jak i oprogramowanie musi podlegać specjalnej ochronie w trakcie transportu oraz użytkowania zapewniającej jego nienaruszalność (by nie zostały dokonane podmiany). Wymaga formalnego dowodu, że system jest zgodny z wymaganiami. W tym miejscu należy zwrócić uwagę na problem wzrostu obciążenia systemu operacyjnego związanego z uaktywnieniem opcji bezpieczeństwa. W szczególności może okazać się, że mało wydajne serwery nie będą w stanie obsłużyć wszystkich użytkowników po uruchomieniu wszystkich programów

zabezpieczających, ze względu na duże zużycie zasobów procesora oraz powierzchni dyskowej. Penetracja systemu teoretycznie jest nie możliwa do przeprowadzenia.

Wskaźnik A1 otrzymało już kilka komponentów sieciowych, ale jeszcze żaden system operacyjny. Wiele systemów operacyjnych, np. HP/UX firmy Hewlett-Packard, Ultrix firmy Digital i IRIX firmy Silicon Graphics, uzyskało wskaźniki B1, B2 i B3. Wiele systemów operacyjnych ogólnego przeznaczenia uzyskało wskaźnik C2.

4.0.4 Analiza ryzyka

The Orange Book zawiera rozdział zawierający zalecenia dotyczące sposobów wykonywania analizy systemu. Wśród zaleceń tych są informacje o składzie personelu wykonującego analizę, o czasie wykonywania analizy i inne. Analiza ryzyka przedstawia systematyczny podział na kategorie zagrożeń danych i środków im przeciwdziałających oraz określa plan działania, który większość zasobów (technicznych i pozatechnicznych) skieruje przeciw najbardziej prawdopodobnemu ryzyku. Aby zapewnić stopień bezpieczeństwa proporcjonalny do wagi chronionej informacji, należy uwzględnić priorytet zagrożeń. Analiza ryzyka nie ma na celu stworzenie planu całkowitej ochrony. Do elementów analizy ryzyka należą:

- zagrożenia, częstość zagrożeń,
- cele,
- odporność na zagrożenia,
- konsekwencje ataków,
- stosunek ryzyka do potencjalnych strat,
- ochrona, koszt ochrony,
- koszt analizy,
- implementacja mechanizmów ochrony.

Niestety trzeba też pamiętać, że osiągnięcie całkowitego bezpieczeństwa w dzisiejszych systemach komputerowych jest w praktyce nie możliwe do osiągnięcia. Związane jest to z faktami, iż systemy komputerowe często są systemami *otwartymi*. Zaimplementowanie w nich 100% bezpieczeństwa mogłoby spowodować, że straciłyby swój charakter. Z drugiej strony również koszt wprowadzenia absolutnego bezpieczeństwa mógłby być tak wysoki, iż przerósłby wartość samego systemu. Ocena bezpieczeństwa systemu komputerowego może jednak uświadomić, jakie istnieją w nim luki i niedociągnięcia, i znacząco przyczynić się do podniesienia poziomu ochrony informacji przechowywanych i przetwarzanych w tym systemie komputerowym.

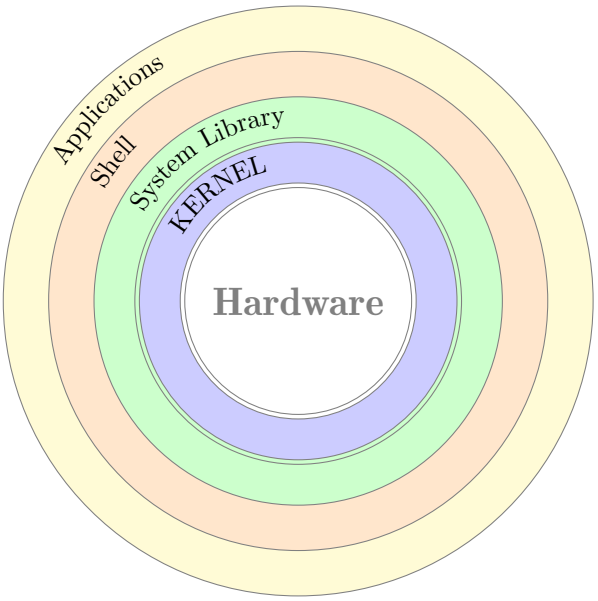
4.1 Budowa popularnych systemów operacyjnych

Obecnie najpopularniejszymi systemami operacyjnymi są trzy rodziny systemów:

- systemy Unix/Linux;
- systemy Windows firmy Microsoft - zarówno systemy end user jak i serwerowe;
- systemy MAC OS firmy Apple, wykorzystujący jądro systemu UNIX;
- AIX (*ang. Advanced Interactive Executive*) firmy IBM, - odmiana systemu Unix tworzona przez firmę IBM na podstawie systemów SysV i BSD;
- Android dla systemów przenośnych, np. telefony komórkowe.

4.1.1 Linux

System ma budowę warstwową przedstawioną na rys. 4.1. Warstwa sprzętu (*ang. hardware*) obudowana jest warstwą jądra systemu (*ang. kernel*), z którym współpracują programy powłoki (*ang. shell*).



Rys. 4.1: Architektura systemu Linux/Unix.

Współpraca odbywa się przez wywołania systemowe (system calls), których jest około 300 (dla porównania w systemie Windows jest ich około 100000). Im mniej jest wywołań systemowych tym system jest bezpieczniejszy. Warstwa powłoki chroni jądro i jest podzielona na dwie części: CLI i GUI. Zewnętrzną warstwę stanowią aplikacje użytkownika. W systemie nie ma możliwości bezpośredniej pracy aplikacji ze sprzętem. Każdy uruchomiony proces posiada własny identyfikator PID. Każdy użytkownik posiada swój unikalny numer UID.

Także grupa posiada swój unikalny numer GID. W systemie Linux/Unix wykonywane są samodzielne programy. Każda komenda to programy (np. otwarcie pliku to wykonanie odpowiedniej komendy). Wykonanie części programów wymaga uprawnień administratora lub hasła administratora w celu uzyskania odpowiednich uprawnień. W związku z bardzo małą liczbą wywołań systemowych i każdorazową koniecznością uwierzytelnienia w przypadku, gdy wymagane jest wykonanie programu z uprawnieniami administratora (*ang. super user*), tworzenie złośliwego oprogramowania stwarza poważne trudności. Bez wejścia w uprawnienia administratora dokonanie ataku na system Linux/Unix nie jest możliwe.

System UNIX od początku projektowany był jako wielozadaniowy i wielodostępny system sieciowy. W związku z tym posiada wszystkie niezbędne narzędzia i programy. Podstawowe cechy systemu UNIX to:

- Większe możliwości pracy wielozadaniowej i wielodostępnej pracy niż inne systemy.
- Bardzo dobra skalowalność.
- Przetwarzanie rozproszone.
- Bardzo stabilna praca.
- Możliwość pracy na wielu platformach sprzętowych, w tym komputerach MainFrame.
- Przezroczysty, sieciowy system graficzny X-Windows.
- Prosty mechanizm przetwarzania (IN/OUT/ERR)
- Konfiguracja programów w plikach tekstowych, co umożliwia pełną kontrolę nad konfiguracją.
- Dostęp do plików konfiguracyjnych tylko za pomocą edytora vi.
- Pełna dokumentacja systemu dostarczana wraz z systemem.
- Niewielkie różnice pomiędzy systemami dostarczanymi przez różnych producentów.

4.1.2 Windows

Rodzina systemów operacyjnych firmy Microsoft obejmuje dwie grupy produktów:

- systemy serwerowe - (Windows Seerver 20xx)
- systemy dla użytkownika końcowego (obecnie Windows 7/8/10)

Windows 7, Windows Vista, Windows Server 2003, Windows XP, Windows 2000 i Windows NT są częścią rodziny Windows NT (w technologii NT) systemów operacyjnych firmy Microsoft. Umożliwiają one między innymi wywłaszczanie oraz wielobieżność i zostały zaprojektowane do pracy na systemach bazujących na architekturze x86 Intela, zarówno jednoprocesorowych, jak i o architekturze SMP. Do obsługi wejścia/wyjścia architektura NT stosuje przetwarzanie pakietowe, które wykorzystuje IRP (I/O request packet - pakiet zamówienia

wejścia/wyjścia), oraz wejście/wyjście asynchroniczne. Poczynając od Windows XP, Microsoft rozpoczął wbudowywanie obsługi trybu 64-bitowego w swoje systemy operacyjne – wcześniejsze wersje korzystały tylko z trybu 32-bitowego. Architektura Windows NT jest wysoce modularna i składa się z dwóch głównych warstw: trybu użytkownika i trybu jądra. Programy i podsystemy w trybie użytkownika są ograniczone do zasobów systemowych, do których mają dostęp, w trybie jądra natomiast posiadają nieograniczony dostęp do pamięci systemowej i urządzeń zewnętrznych. Jądra systemów operacyjnych w technologii NT są określane jako jądra hybrydowe. Jądro to jest właściwie jądrem monolitycznym o strukturze zbliżonej do mikrojądra. Architektura NT składa się z jądra hybrydowego, warstwy abstrakcji sprzętowej (HAL), sterowników i egzekutora. Wszystkie te moduły działają w trybie jądra. Usługi o wyższym poziomie abstrakcji są implementowane przez egzekutor. Tryb użytkownika w technologii Windows NT składa się z podsystemów, umożliwiających przekazywanie zamówień wejścia/wyjścia za pomocą menedżera wejścia/wyjścia do odpowiedniego sterownika programowego, działającego w trybie jądra. Warstwa użytkownika Windows 2000 składa się z dwóch podsystemów: podsystemu środowiska (uruchamia aplikacje napisane dla wielu różnych typów systemów operacyjnych) i podsystemu integralności (uruchamia specyficzne dla systemu funkcje w zastępstwie podsystemu środowiska). Tryb jądra w Windows 2000 ma pełny dostęp do sprzętu i zasobów systemowych komputera. Tryb jądra blokuje dostęp dla usług i aplikacji trybu użytkownika do krytycznych elementów systemu operacyjnego, do których nie powinny mieć one dostępu.

Egzekutor komunikuje się ze wszystkimi podsystemami trybu użytkownika. Obsługuje wejście/wyjście, zarządza obiektami, zabezpieczeniami, oraz procesami. Jądro umieszczone jest pomiędzy HAL i Egzekutorem, zapewniając synchronizację wieloprocesorową, szeregowanie zadań i przerwań wraz z ich przydzielaniem, oraz zarządzanie obsługą pułapek i rozdzielaniem wyjątków. Jądro jest odpowiedzialne również za inicjalizację sterowników sprzętu podczas uruchamiania systemu. Sterowniki poziomu jądra występują na trzech poziomach: wysokim, pośrednim, oraz niskim. Windows Driver Model (WDM - model tworzenia sterowników dla Windows) występuje na poziomie pośrednim i został zaprojektowany tak, aby zachować zgodność binarną i kodu źródłowego pomiędzy Windows 98 a Windows 2000. Sterowniki niskiego poziomu są albo sterownikami Windows NT starszego typu, kontrolującymi urządzenie bezpośrednio, albo szyną systemową typu Plug-and-play.

Tryb użytkownika Tryb użytkownika składa się z podsystemów, które przekazują zamówienia wejścia/wyjścia do odpowiednich sterowników w trybie jądra przez menedżera wejścia/wyjścia (który działa w trybie jądra). Dwa podsystemy, na które składa się warstwa trybu użytkownika w Windows 2000, to podsystem środowiska i podsystem integralności.

Podsystem środowiska został zaprojektowany do uruchamiania aplikacji napisanych dla wielu różnych systemów operacyjnych. Żaden z podsystemów środowiska nie może uzyskać bezpośredniego dostępu do sprzętu i musi złożyć zamówienie na dostęp do pamięci poprzez menedżera pamięci wirtualnej (Virtual Memory Manager), który działa w trybie jądra. Ponadto aplikacje otrzymują niższy priorytet niż procesy w trybie jądra. Obecnie istnieją trzy główne podsystemy środowiska: podsystem Win32, OS/2 i POSIX.

Podsystem środowiska Win32 może uruchamiać 32-bitowe aplikacje dla Windows. Zawiera on obsługę konsoli i okien tekstowych, oraz obsługę wyłączenia i błędów dla pozostałych podsystemów środowiska. Ponadto umożliwia on korzystanie z maszyn wirtualnych DOS (Virtual DOS Machine), które umożliwiają uruchamianie aplikacji dla systemu MS-DOS oraz 16-bitowych Windows 3.x (Win16). Istnieje specjalna maszyna wirtualna DOS (oparta na sprzętowym trybie wirtualnym 8086 obecnym w architekturze x86), która działa we własnej przestrzeni adresowej, emulując procesor Intel 80486 z uruchomionym systemem MS-DOS 5. Programy Win16 natomiast są uruchamiane w maszynie Win16 (do jej uruchomienia niezbędne jest wcześniejsze uruchomienie odrębnej maszyny wirtualnej DOS)). Domyślnie (oprócz systemów NT 3.x) każdy następny program Win16 uruchamiany jest w już działającym procesie Win16 uruchomionym przez pierwszy program Win16 (w związku z tym używa tej samej przestrzeni adresowej, a maszyna Win16 przyznaje każdemu programowi jego własny wątek). Możliwe jest również uruchamianie programu Win16 w oddzielnej maszynie wirtualnej, co umożliwia jego szeregowanie z wywłaszczaniem, gdyż Windows wywłaszcza wtedy cały proces maszyny wirtualnej, który zawiera tylko jeden uruchomiony program – w systemie NT 3.x było to rozwiązanie domyślne, ale w NT 4.0 i nowszych Microsoft to zmienił, ponieważ uruchamianie odrębnej maszyny Win16 zużywało więcej czasu (konieczność uprzedniego uruchomienia maszyny wirtualnej DOS, a potem maszyny Win16) i pamięci. Podsystem OS/2 umożliwia uruchamianie 16-bitowych, działających w trybie znakowym programów dla systemu OS/2 i emuluje OS/2 1.x. Nie udostępnia natomiast trybu 32-bitowego i środowiska graficznego dla OS/2 2.x i nowszych. Podsystem środowiska POSIX umożliwia uruchamianie aplikacji, które ściśle przestrzegają standardu POSIX.1, lub związanych z nim standardów ISO/IEC.

Systemy działające w trybie 64-bitowym nie udostępniają możliwości uruchamiania aplikacji DOS i Win16. Wynika to z tego, że w trybie 64-bitowym (Long) architektura x64 nie dysponuje trybem wirtualnym 8086, a jego programowe emulowanie (przez system) jest nieopłacalne z uwagi na niewielką liczbę stosowanych obecnie aplikacji DOS i Win16. Ponadto dzięki możliwościom wirtualizacyjnym i tak można w razie potrzeby łatwo emulować sprzętowo procesor x86 przy użyciu odrębnej aplikacji.

Podsystem integralności zajmuje się specyficznymi dla systemu operacyjnego funkcjami w zastępstwie podsystemu środowiska. Składa się z podsystemu bezpieczeństwa, usługi stacji roboczej i usługi serwera. Podsystem bezpieczeństwa obsługuje tokeny bezpieczeństwa, udostępnia albo blokuje dostęp do kont użytkowników korzystając z praw dostępu do zasobów, obsługuje logowanie i inicjuje weryfikację loginu, oraz decyduje które zasoby systemowe muszą być audytowane przez Windows 2000. Ponadto obsługuje Active Directory. Usługa stacji roboczej to API dla readresatora sieciowego, który umożliwia dostęp komputera do sieci. Usługa serwera to API, które pozwala na udostępnianie przez komputer połączeń sieciowych.

Tryb jądra Tryb jądra Windows 2000 ma pełny dostęp do sprzętu oraz zasobów systemowych komputera i wykonuje kod w obszarze pamięci chronionej. Kontroluje dostęp do szeregowania, priorytetyzację wątków, zarządzanie pamięcią i komunikację ze sprzętem. Tryb jądra blokuje dostęp usługom i aplikacjom trybu użytkownika do krytycznych obszarów systemu operacyjnego, mogą one

jedynie zażądać od jądra wykonania tych czynności w ich imieniu. Tryb jądra składa się z usług egzekutora, które składają się z modułów przeznaczonych do wykonywania specyficznych czynności, sterowników jądra, jądra i HAL.

Egzekutor Egzekutor porozumiewa się ze wszystkimi podsystemami trybu użytkownika. Obsługuje operacje wejścia/wyjścia, zarządzanie obiektami i procesami, oraz zabezpieczeniami. Zawiera wiele komponentów, m.in. Menedżera wejścia/wyjścia, Monitor odwołań bezpieczeństwa, Menedżera obiektów, Menedżera IPC, Menedżera pamięci wirtualnej, Menedżera PnP i Menedżera zarządzania energią, oraz Menedżera okien, który współpracuje z GDI Windows. Każdy z tych komponentów udostępnia pomocniczą funkcję jądra, która pozwala innym komponentom na komunikację między sobą. Cała ta grupa komponentów może być nazywana usługami egzekutora. Żadna z nich nie ma dostępu do wewnętrznych funkcji innych komponentów egzekutora.

Menedżer obiektów jest specjalnym podsystemem egzekutora, przez który muszą przejść wszystkie inne podsystemy egzekutora, aby otrzymać dostęp do zasobów Windows 2000 - co czyni go usługą zarządzania zasobami. Menedżer obiektów jest używany do zredukowania duplikacji funkcjonalności zarządzania zasobami w innych podsystemach egzekutora, co mogłoby prowadzić do błędów i utrudnić tworzenie Windows 2000. Dla menedżera obiektów wszystkie zasoby są obiektami, niezależnie od tego, czy zasób jest fizyczny (np. system plików lub urządzenie zewnętrzne), czy logiczny (np. plik). Każdy obiekt ma strukturę - typ obiektu, który menedżer obiektów musi znać. Gdy inny podsystem egzekutora żąda stworzenia obiektu, wysyła to żądanie do menedżera obiektów, co powoduje utworzenie pustej struktury obiektu, którą następnie żądający podsystem wypełnia. Typy obiektów definiują funkcje udostępniane przez obiekt, oraz specyficzne dla niego dane. W ten sposób menedżer obiektów sprawia, że Windows 2000 jest systemem operacyjnym zorientowanym obiektowo, ponieważ typy obiektów mogą być uznawane za klasy, definiujące obiekty.

Każda instancja tworzonego obiektu zachowuje swoją nazwę, parametry przekazywane do funkcji tworzącej obiekt, parametry bezpieczeństwa i wskaźnik na typ obiektu. Każdy obiekt zawiera ponadto procedurę usuwającą oraz licznik referencji, który informuje menedżera obiektów o ilości innych obiektów w systemie posiadających odwołanie do danego obiektu, co pozwala na podjęcie decyzji o możliwości zniszczenia go, gdy jest on usuwany. Każdy obiekt znajduje się w hierarchicznej przestrzeni nazw obiektów.

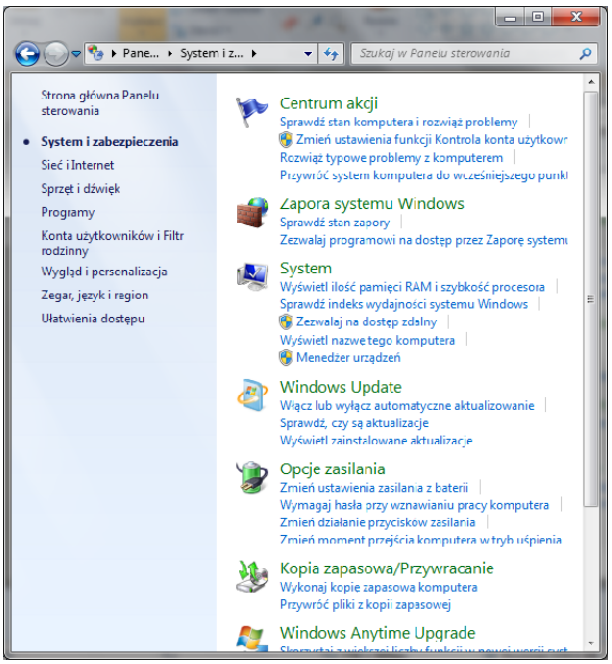
4.2 Zabezpieczenie systemu klienckiego Microsoft Windows

Systemy klienckie Windows serii 7 i 8 wymagają szczególnej uwagi w celu utrzymania w ruchu systemu i zapewnienia minimalnego poziomu bezpieczeństwa. Jest to spowodowane brakiem wymuszenia na użytkowniku odpowiedniego sposobu pracy z systemem. Szczególną uwagę należy zwrócić na:

- Pracę użytkownika na zwykłym koncie, a nie koncie administratora.
- Blokowanie ekranu hasłem, w przypadku nieużywania systemu przez określony czas lub pozostawienie komputera bez dozoru.

- Aktualizację oprogramowania systemowego i programów użytkownika.
- Instalację i konfigurację programu antywirusowego, w tym konfigurowanie sprawdzania nowych nośników i okresowego sprawdzania systemu plików.
- Włączenie i ewentualna konfiguracja zapory systemowej (firewall).
- Konfigurację zdalnego dostępu (zdalny pulpit).
- Konfigurację nazwy komputera, nazwy grupy roboczej Microsoft Network oraz usług udostępniania zasobów.
- Wykorzystanie mechanizmów kontroli rodzicielskiej.
- Konfigurację kopii zapasowej systemu i utworzenie dysku odzyskiwania systemu.
- Konfigurację oprogramowania użytkowników, ze szczególnym uwzględnieniem przeglądarek internetowych i programów pocztowych.

W dalszej części zajęto się poszczególnymi zagadnieniami na przykładzie systemu Windows 7. Konfiguracja systemu realizowana jest z poziomu użytkownika przez tzw. *Panel Sterowania*. Zawarte są w nim programy konfiguracyjne z intuicyjnym interfejsem użytkownika. Umożliwiają one dokonanie podstawowych zmian konfiguracyjnych niewykwalifikowanemu użytkownikowi. Wygląd *Panelu Sterowania* dla sekcji *System* przedstawiono na rys. 4.2.



Rys. 4.2: Panel sterowania.

Konta użytkowników W systemie można założyć dwa rodzaje kont:

- Konto administratora
- Konto z ograniczeniami (zwykły użytkownik)

Praca na koncie administratora systemu obarczona jest dużym ryzykiem, szczególnie praca w sieci. Administrator jest właścicielem wszystkich plików i katalogów i ma prawo do wykonywania wszystkich programów. Ma także uprawnienia związane z instalowaniem i uruchamianiem programów i usług. Pracując w sieci na uprawnieniach administratora można przez przypadek zainstalować złośliwe oprogramowanie - np. umieszczone w załączniku do mail'a, na stronie internetowej, przyniesiony na nośniku, ... Dlatego też do normalnej pracy należy założyć konto zwykłego użytkownika (z ograniczeniami), co uniemożliwia lub utrudnia zainstalowanie złośliwego oprogramowania. Inne systemy operacyjne (np. Linux) uniemożliwiają pracę zwykłego użytkownika na koncie administratora. Na rys. 4.3a przedstawiono okno zarządzania kontami użytkowników. Widać tylko jedno konto administracyjne i kilka kont z ograniczeniami. W systemie Windows można założyć wiele kont administratorom systemu.

Na rys. 4.3b oraz na rys. fig/windows7/KontaHasloZwyklUzytk proces zakładania konta użytkownika z ograniczeniami (zwykłego użytkownika).

Konfiguracja wygaszacza ekranu Odpowiednia konfiguracja wygaszacza ekranu umożliwia ochronę przed nieautoryzowanym dostępem osób trzecich w przypadku pozostawienia komputera bez nadzoru. Należy ustawić żądany czas automatycznego blokowania ekranu (najczęściej kilka minut) oraz możliwość wznowienia pracy po podaniu hasła logowania. Odpowiednie okna konfiguracyjne przedstawiono na rys. 4.4.

Kontrola rodzicielska Mechanizm kontroli rodzicielskiej umożliwia ograniczenia możliwości pracy użytkownika systemu poprzez wyznaczenia godzin pracy, możliwych do uruchomienia programów oraz filtrowanie treści. Okno konfiguracji filtru rodzicielskiego przedstawiono na rys. 4.5.

Możliwe jest także ustawienie klasyfikacji uruchamianych gier, co jest opcją dedykowaną dla dzieci.

Aktualizacje automatyczne Microsoft Update Systemy klienckie Windows mają duże problemy związane z bezpieczeństwem i niepoprawnym działaniem. Dlatego też pojawia się wiele poprawek i uaktualnień systemu jak i oprogramowania. Poprawki mogą być instalowane automatycznie przez mechanizm automatycznej aktualizacji. Należy zwrócić uwagę, że automatyczne instalowanie aktualizacji (rys. 4.6) może w niektórych przypadkach spowodować niedziałanie oprogramowania użytkownika. W przypadku dużej liczby systemów należy najpierw przetestować działanie poprawek na jednym z komputerów. Po pomyślnym przejściu testów można zaktualizować pozostałe komputery (najczęściej ręcznie).

Na rys. 4.6a przedstawiono okno aktualizacji systemu a na rys. 4.6b przedstawiono okno konfiguracji sposobu aktualizacji systemu.

Aktualizację systemu można przeprowadzić na różne sposoby:

- Nie aktualizować systemu o ile pracuje w sieci lokalnej i nie wymienia danych z innymi systemami (obecnie praktycznie niemożliwe).
- Nie aktualizować automatycznie tylko ręcznie.
- Włączyć powiadomienia o nowych aktualizacjach i aktualizować w dogodnym momencie.
- Pobrać automatycznie aktualizacje ale wybrać moment ich aktualizowania.
- Pobrać i zainstalować aktualizacje automatycznie.

Przy wyborze sposobu należy uwzględnić wcześniejsze rozważania.

Kopia zapasowa i odzyskiwanie systemu W systemie Windows istnieją mechanizmy tworzenia kopii zapasowych plików systemowych oraz konfiguracyjnych. Mechanizm ten jest wykorzystywany w przypadku niemożności uruchomienia systemu po awarii. Jest to możliwe np. w przypadku zainstalowania oprogramowania zewnętrznego (np. sterowników) lub niektórych aktualizacji. W takiej sytuacji oprogramowanie umożliwia naprawę systemu i odzyskanie sprawności. Istnieją także możliwości uruchomienia systemu z ostatnią prawidłowo działającą konfiguracją. Na rys. 4.7 przedstawiono konfigurację kopii zapasowych systemu oraz dysku odzyskiwania systemu.

Logi systemowe W trakcie pracy system i usługi zapisują informację o działaniu w logach systemowych. Ze względu na ilość wpisów informacje te zostały podzielone na kategorie, np.: błędy, ostrzeżenia, ... Na rys. 4.8 przedstawiono okno programu do przeglądania logów (zdarzeń) systemowych. Program ten umożliwia sortowanie i wyszukiwanie zdarzeń. Podaje także statystyki zdarzeń.

Zwiększenie szybkości działania systemu W celu podniesienia wydajności (szybkości działania systemu) można dokonać następujących zmian w ustawieniach systemu:

- Ustawić rozmiar pamięci wirtualnej na możliwie najmniejszy 4.9b. W przypadku systemów z dużą ilością pamięci należy zrezygnować z pamięci wirtualnej. Sposób obsługi pamięci wirtualnej w systemie Windows można znaleźć w literaturze.
- Zrezygnować z multimedialnych dodatków w systemie (rys. 4.9a) typu: okna 3D, animacje, itp.
- Przejrzeć listy uruchamianych usług i (4.10b) i wyłączyć usługi niepotrzebne. (rys. 4.10a).

Usługi systemu Usługi mogą być uruchamiane na różne sposoby, np. przy starcie systemy, automatycznie, ręcznie. Z punktu widzenia bezpieczeństwa dobrze jest regularnie przeglądać listę usług i wyłączyć nieużywane i niepotrzebne usługi. Okno z listą usług przedstawiono na rys. 4.10.

Bardzo często słaba wydajność spowodowana jest występowaniem w systemie błędów. W celu lokalizacji ewentualnych problemów należy przejrzeć listę zdarzeń systemowych (rys. 4.8).

Należy zwrócić uwagę na fakt, że istnieją darmowe pakiety oprogramowania (np. IOBit: http://www.iobit.com) umożliwiające optymalizację działania systemu przez usunięcie niepotrzebnych plików, usunięcie błędnych dowiązań, usunięcie błędów rejestru, dobranie parametrów pracy usług, opóźniony start usług, wyłączenie usług nieużywanych.

4.2.1 Praca w sieci

Praca systemów operacyjnych w sieci wiąże się z szeregiem zagrożeń, w tym m.in. możliwością nieautoryzowanego dostępu do systemu, usług i danych. Dodatkowo system podatny jest na zagrożenia ze strony złośliwego oprogramowania oraz ataków z sieci. Zagadnienie jest dosyć złożone i niewykwalifikowany użytkownik nie jest w stanie sprostać ww. zagrożeniom. Z drugiej strony zapewnienie bezpieczeństwa związane jest z ograniczeniami funkcjonalności. W związku z tym w systemach Windows wprowadzono mechanizmy konfiguracji w zależności od miejsca i rodzaju sieci w jakiej pracuje system. Okno konfiguracji przedstawiono na rys. 4.11. Dostępne są trzy rodzaje konfiguracji sieci:

- sieć domowa,
- sieć firmowa,
- sieć publiczna (dostęp do sieci np. na lotniskach, w klubach).

Najmniej restrykcyjnym poziomem zabezpieczeń jest lokalizacja domowa, najbardziej sieci publiczne. Wiąże się to ze zmianą sposobu konfiguracji zapory sieciowej i przeglądarki internetowej. Dodatkowo zmieniane są sposoby udostępniania zasobów w sieci Microsoft Network (np. drukarki, katalogi).

Zdalny pulpit Usługa zdalnego pulpitu umożliwia zalogowanie się do systemu poprzez sieć. W przypadku niekorzystania z funkcji zdalnego dostępu funkcję tą należy wyłączyć - rys. 4.12.

Uwaga! Zdalne zalogowanie powoduje, że osoba mająca dostęp fizyczny do komputera widzi na ekranie wszystko co jest wykonywane zdalnie.

Grupy robocze

Systemy firmy Microsoft udostępniają możliwość pracy systemów w tzw. grupach roboczy *Microsoft Networks*. Każdy komputer posiada ustawioną domyślną nazwę grupy roboczej, w zależności od wersji systemu może to być np.: *Workgroup*, *MSHome*, *Home*. Niestety niesie to za sobą niebezpieczeństwo dostępu do udostępnionych (świadomie lub nie) zasobów komputera innym komputerom pracującym w tej samej sieci. Dlatego też po uruchomieniu nowego komputera należy zmienić nazwę grupy roboczej. W przypadku, gdy komputer nie pracuje w żadnej grupie roboczej należy ją zmienić na jakąkolwiek i nie pozostawiać grupy domyślnej. Okna konfiguracji grupy roboczej przedstawiono na rys. 4.13.

W pracy nie jest omawiany system praw dostępu w domenie *Microsoft Network* przechowywanych bazie *Active Directory* - bazie danych o obiektach. Informacje na temat pracy systemu w domenie można znaleźć w literaturze specjalistycznej. Domenę *Microsoft Network* może obsługiwać serwer *Samba 4* pracujący pod kontrolą systemu operacyjnego *Linux*.

4.2.2 Konfiguracja zapory (firewall) systemowej

W systemach Windows dostarczana jest systemowa zapora ogniowa (firewall. Na rys. 4.14 przedstawiono okna, którą należy włączyć i ewentualnie skonfigurować za pomocą odpowiedniego okna konfiguracji zapory. Konfiguracja samej zapory uzależniona jest od sieci, w której pracuje komputer. Na rys. 4.14a i 4.14b przedstawiono ustawienie zapory w zależności od lokalizacji komputera w sieci. Na rys. 4.14c przedstawiono okno z zaawansowanymi ustawieniami zapory, które umożliwia definiowanie reguł pracy zapory.

Zapora umożliwia skonfigurowanie reguł dla ruchu przychodzącego, wychodzącego oraz dla poszczególnych programów i usług systemu. Okresowo należy śledzić logi zapory. Działanie zapory może unieruchamiać programy działające w sieci, w przypadku błędów obsługi (błędów użytkowników systemów). Okna zaawansowanej konfiguracji zapory dla poszczególnych rodzajów reguł (ruchu) przedstawiono rys. 4.15.

4.2.3 System plików NTFS

NTFS (*ang. New Technology File System*) jest standardowym system plików systemu Windows NT i jego następców (Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8). Wywodzi się od systemu plików HPFS, opracowanego przez Microsoft i IBM dla systemu OS/2. Został wprowadzony w celu zastąpienia starszego systemu *FAT*, używanego w MS-DOS. Zaczerpnięte z HPFS ulepszenia w stosunku do systemu *FAT* obejmują obsługę metadanych oraz dodanie struktur poprawiających szybkość pracy z dużą liczbą plików oraz dyskami o dużej pojemności. Dalsze ulepszenia (w stosunku do HPFS) polegają na wprowadzeniu listy kontroli dostępu (ACL) i dziennika operacji dyskowych (ang. journal). Ponadto NTFS nie ma tak ostrego ograniczenia dotyczącego maksymalnego rozmiaru pliku (do 4GB w FAT32), co umożliwia na przykład przechowanie obrazu płyty DVD na dysku twardym, bez dzielenia go na mniejsze pliki. Do podstawowych możliwości należy:

- księgowanie - (od NTFS 3.0 w Windows 2000); wewnętrzny dziennik zmian znacząco poprawia ochronę danych przed błędami zapisu; wspomaga przy tym działanie narzędzi dyskowych, takich jak CHKDSK;

- szyfrowanie plików i katalogów - (od NTFS 3.0 w Windows 2000) przy pomocy nakładek tworzących EFS - Encrypting File System. Nie ma jednak możliwości zaszyfrowania plików systemowych z systemu Windows XP. EFS dostępny jest tylko w wersjach Professional lub wyższych. Nie jest przeznaczony do szyfrowania prywatnych danych na komputerach domowych lecz do ochrony danych w systemach serwerowych.

Niestety EFS dla systemów serwerowych Windows 2000 i Windows Server 2003 różni się od wersji używanej w późniejszych wersjach Windows i jest z nimi niezgodna.

- kompresja danych *w locie*; pliki kompresowane przy pomocy wbudowanych funkcji NTFS nie mogą być szyfrowane przy pomocy EFS i odwrotnie;

- prawa dostępu dla grup i użytkowników - dostęp do tej funkcji jest ograniczony w Windows XP Home Edition i późniejszych; pełne wykorzystanie praw dostępu, wraz z możliwością wykonania inspekcji praw dostępu z zapisem do dziennika, możliwe jest w Windows 2000 (wszystkie wersje dla komputerów PC), Windows XP Professional, Windows Server 2003 i niedomowych wersjach Windows Vista

- transakcyjność - (od Windows Vista) pozwala na wykonywanie transakcyjnych operacji na systemie plików. Transakcje są optymalizowane tak, aby czas ich zamknięcia był jak najkrótszy, dzięki czemu w normalnych warunkach nie stanowią dodatkowego obciążenia. Transakcje mogą obejmować wiele plików i pozostawać dowolnie długo otwarte.

Wersje Według numeru wersji wpisanego w nagłówku woluminu NTFS, system ten miał dotychczas wersje o następującej numeracji wewnętrznej:

- 1.0 - wersja NTFS używana przez Windows NT 3.1 wydanego w połowie 1993 roku

- 1.1 - wersja NTFS używana przez Windows NT 3.5 wydanego jesienią 1994 roku

- 1.2 - wersja NTFS używana przez Windows NT 3.51 (połowa 1995 roku) oraz Windows NT 4.0 (połowa 1996 roku)

- 3.0 - wersja NTFS używana przez Windows 2000 (1997)

- 3.1 - wersja NTFS używana przez Windows XP, Windows Server 2003, Windows Vista i Windows 7.

Przedstawiona numeracja używana jest w oficjalnej dokumentacji Microsoftu (np. Microsoft TechNet). Często spotyka się nieformalną numerację zgodną z wewnętrznym numerem wersji Windows, np NTFS 3.30 używanego w Windows NT 3.51 i 4.0.

Przy instalacji Windows 2000 lub późniejszego Windows na komputerze, na którym istnieją już woluminy NTFS, numery wersji NTFS zostają zmienione do wersji używanej daną wersję Windows lub pozostawione bez zmian w przypadku wersji nowszej.

Operacje na woluminach NTFS, w tym zmiany wersji mogą doprowadzić do niemożności odczytu danych, należy więc operacje te przeprowadzaj z uwagą i czytać dokumentację techniczną. Najlepiej wykonać wcześniej kopie zapasowe danych. Do szyfrowania danych w systemach domowych lub firmowych pracujących poza domeną Windows 2000 lub Windows Server 2003 do szyfrowania danych lepiej używać oprogramowania niezależnego od EFS czy NTFS.

Jądro Linux od wersji 2.2.0 (od 1999 roku) pozwala na odczyt partycji NTFS (wszystkie aktualne dystrybucje). Występują jednak problemy z pełną zgodnością np. praw dostępu.

W systemach Windows 7 (Ultimate i Enterprise) i 8.1 Pro szyfrowanie dysków możliwe jest za pomocą funkcji *BitLocker*. Ulepszona funkcja *BitLocker* dostępna w wersjach Ultimate i Enterprise systemu Windows 7 pomaga chronić wszystkie informacje - od dokumentów po hasła - szyfrując cały dysk, na którym zapisano system Windows oraz dane użytkownika. Po włączeniu funkcji BitLocker każdy plik zapisany na danym dysku jest automatycznie szyfrowany. *BitLocker To Go* jest nową funkcja systemu Windows 7 i umożliwia blokowanie łatwo ginących przenośnych urządzeń magazynujących, takich jak dyski flash USB i zewnętrzne dyski twarde.

Uwaga! Nowe pliki są szyfrowane automatycznie po dodaniu ich do dysku objętego działaniem funkcji BitLocker. Jednak po skopiowaniu tych plików na inny dysk lub komputer zostają one automatycznie odszyfrowane.

4.2.4 Pakiet oprogramowania Sysinternals

Sysinternals Live jest serwisem, który udostępnia szereg programów i narzędzi systemowych. Narzędzia te są bardziej rozbudowane niż narzędzia dostarczane z systemem operacyjnym. Serwis umożliwia uruchamianie narzędzi pakietu bezpośrednio z przeglądarki WWW, bez konieczności instalowania i zgrywania z sieci oprogramowania. Dostęp do narzędzi możliwy jest z poziomu:

- przeglądarki WWW pod adresem https://live.sysinternals.com. Uruchomienie możliwe jest bezpośrednio z okna przeglądarki przez przez wpisanie jego adresu: https://live.sysinternals.com/nazwanarzedzia.
- z poziomu sieci Microsoft Network za pomocą ścieżki: `live.sysinternals.com\tools\nazwanarzedzia`

W skład pakietu wchodzi szereg programów. Najbardziej interesujące są następujące aplikacje:

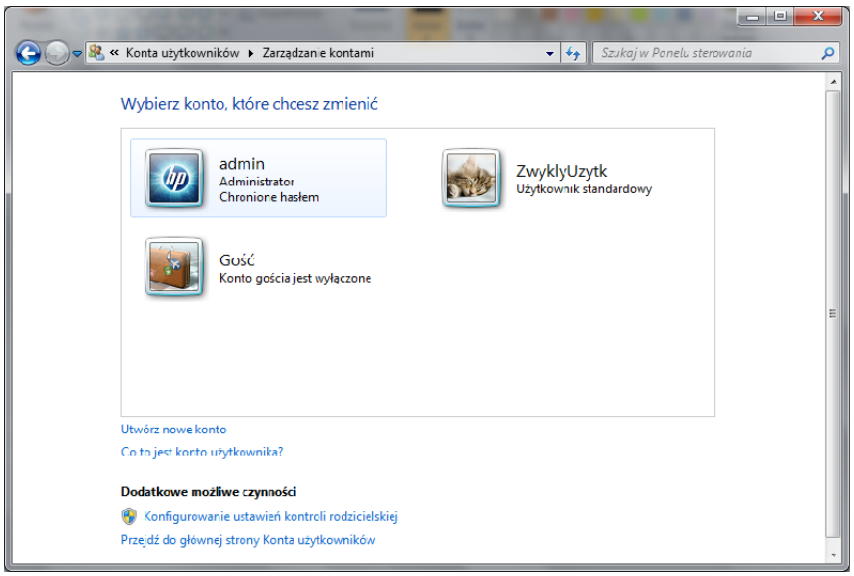
- AutoRuns - program śledzący uruchomione procesy (*ang. autostart execution point manager* - ASEP). Umożliwia wykrywanie wielu programów typu *ang. malware*. Oprogramowanie jest zintegrowane ze skanerem *Virustotal.com*. Okno programu przedstawiono na rys. 4.16.
- Process Explorer - program umożliwiający przeglądanie i obsługę procesów działających w systemie - rys. 4.17.
- Sysmon - program, który zapisuje w logu aktywność procesów systemu Windows. Umożliwia wyświetlenia działających procesów i informacji szczegółowych o każdym z nich.
- TcpView - program umożliwiający podgląd połączeń TCP/IP - rys. 4.18.
- Handle - program pokazujący dostęp poszczególnych programów do plików lub innych zasobów.

4.2.5 Pakiet oprogramowania IObit

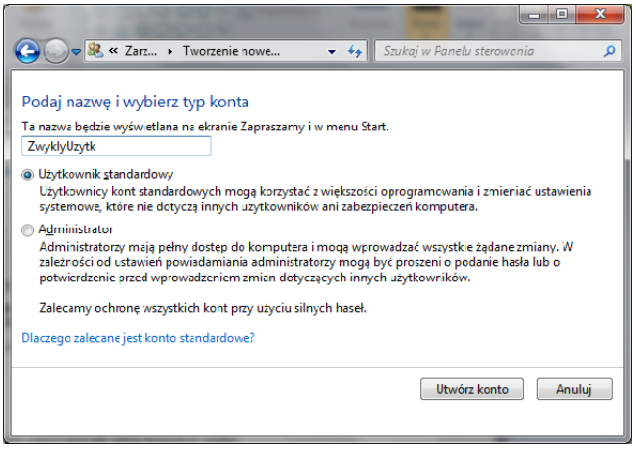
W skład pakietu wchodzi szereg bardzo użytecznych narzędzi, które można instalować w razie konieczności. Pakiet nie jest pakietem darmowym. Umożliwia on:

- aktualizację sterowników systemu,
- optymalizację pracy systemu,
- usuwanie plików prywatnych oraz tzw. prywatności,
- pełne odinstalowanie pakietów oprogramowania z pełnym usuwaniem wpisów rejestrowych oraz plików pozostających na dysku,
- zainstalowanie dedykowanego oprogramowania antywirusowego i antymalware.
- odkasowywanie skasowanych plików,
- wykrywanie złośliwego oprogramowania w pamięci komputera,
- szyfrowanie katalogów.

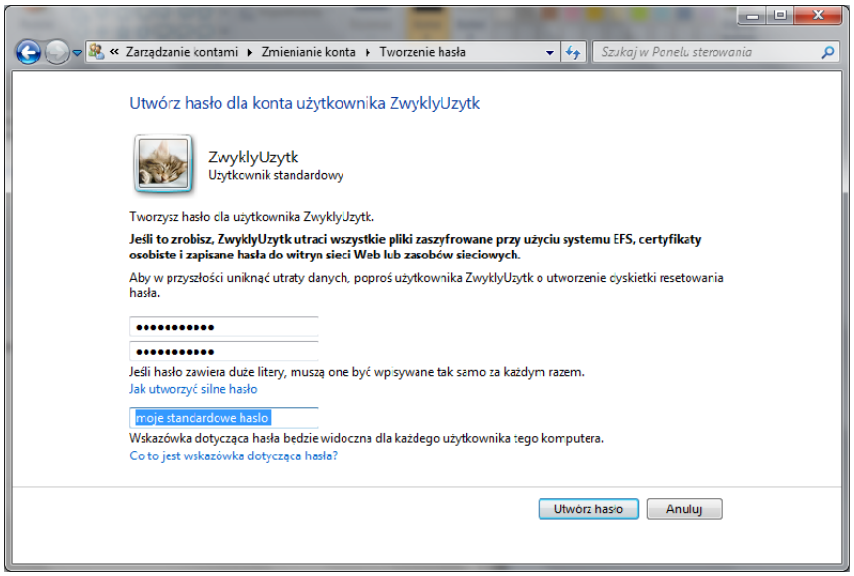
Skuteczność użyteczność pakietu oprogramowania jest bardzo duża. Bardzo dobrze deinstaluje oprogramowanie, nie pozostawiając *śmieci* w systemie. Interfejs użytkownika jest intuicyjny. Szybkość działania programu jest duża. Program współpracuje, praktycznie ze wszystkim wersjami systemu Windows (od wersji XP).



(a) Lista kont.

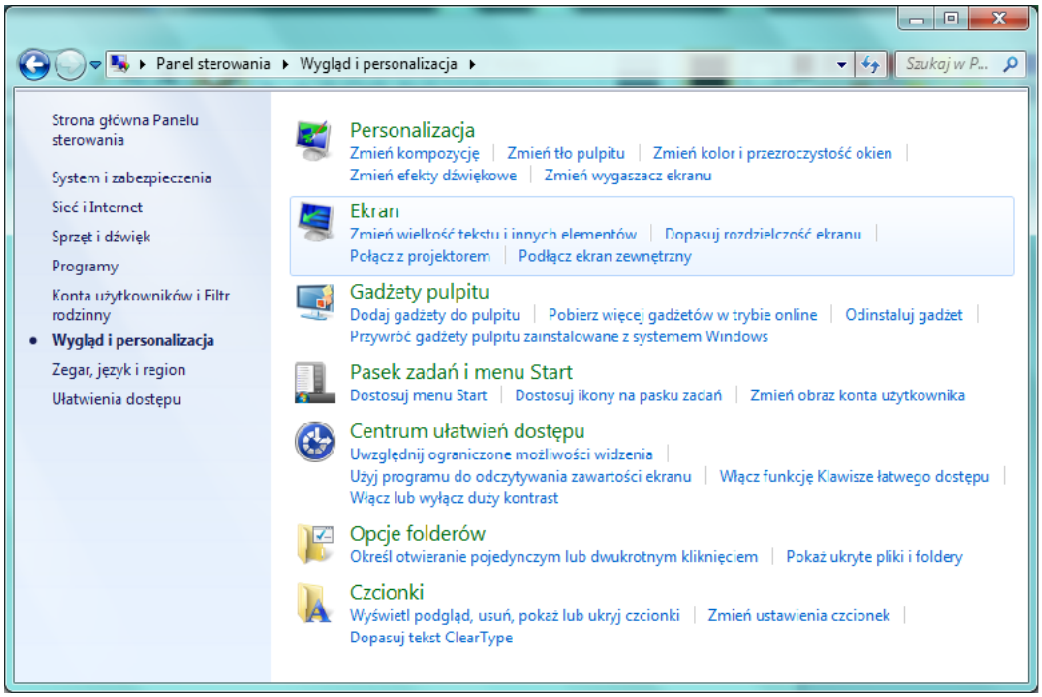


(b) Tworzenie konta zwykłego użytkownika.

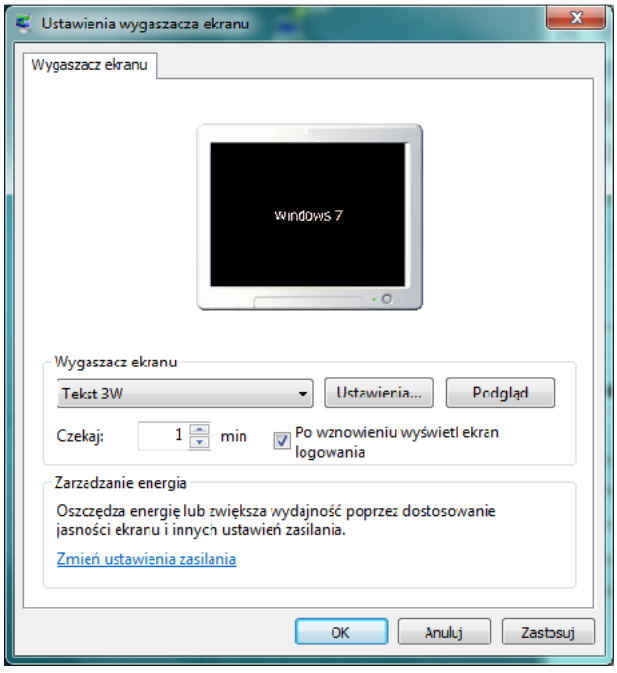


(c) Hasła.

Rys. 4.3: Konta użytkowników.

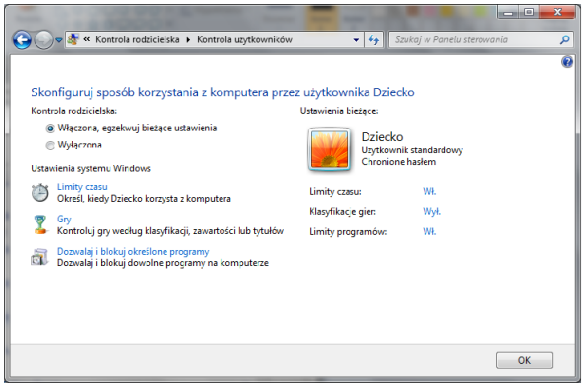


(a) Personalizacja ekranu.

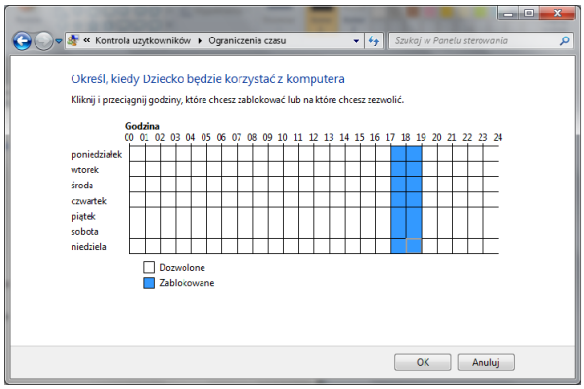


(b) Wygaszacz ekranu.

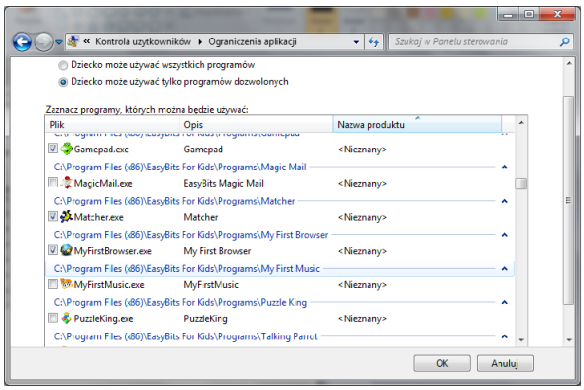
Rys. 4.4: Konfiguracja wygaszacza ekranu.



(a) Okno konfiguracji.

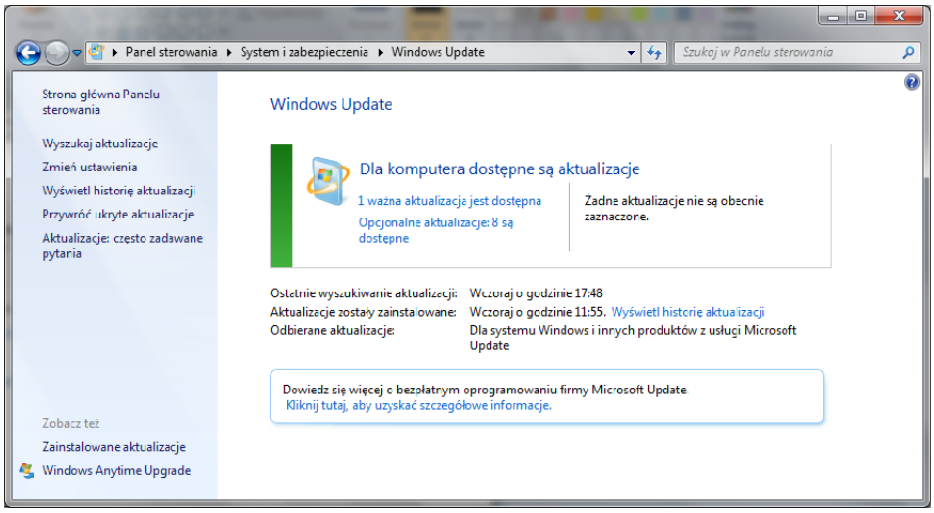


(b) Ustawienie czasu pracy.

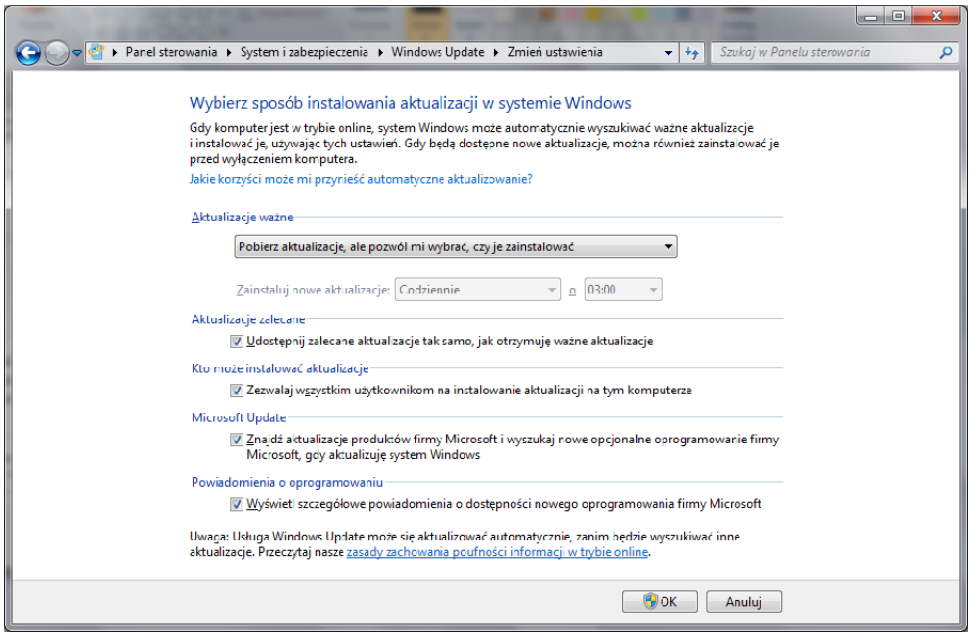


(c) Ograniczenie wykorzystania programów.

Rys. 4.5: Konfiguracja filtra rodzicielskiego.

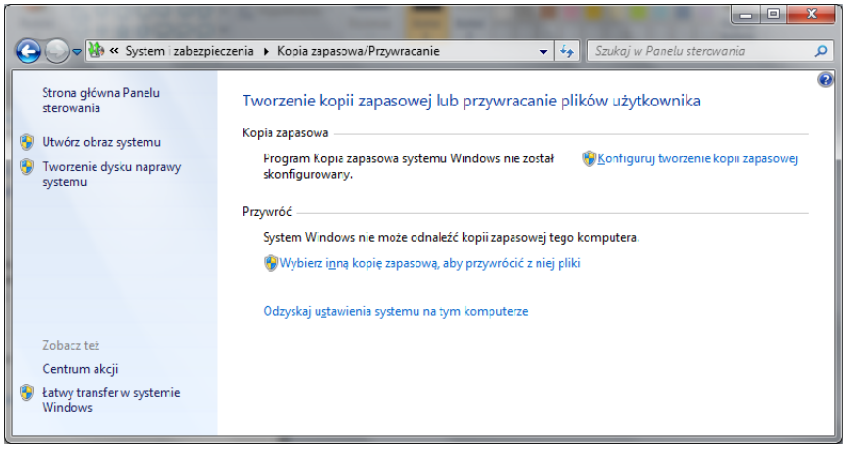


(a) Okno aktualizacji systemu.

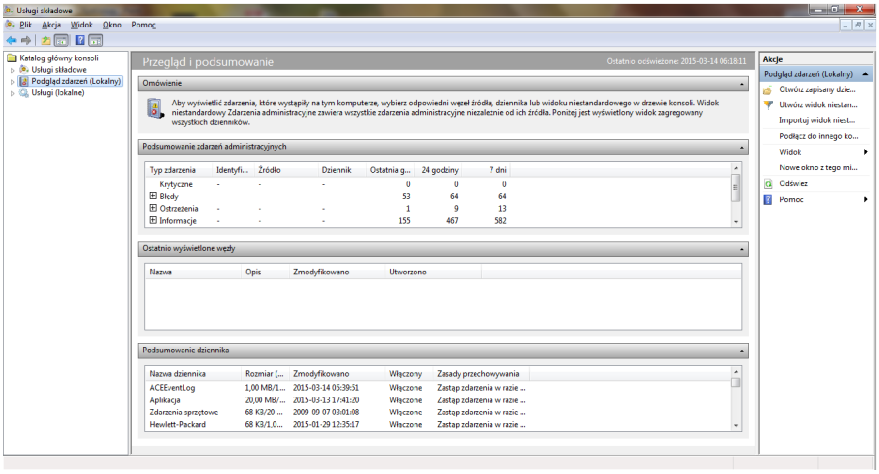


(b) Ustawienia aktualizacji.

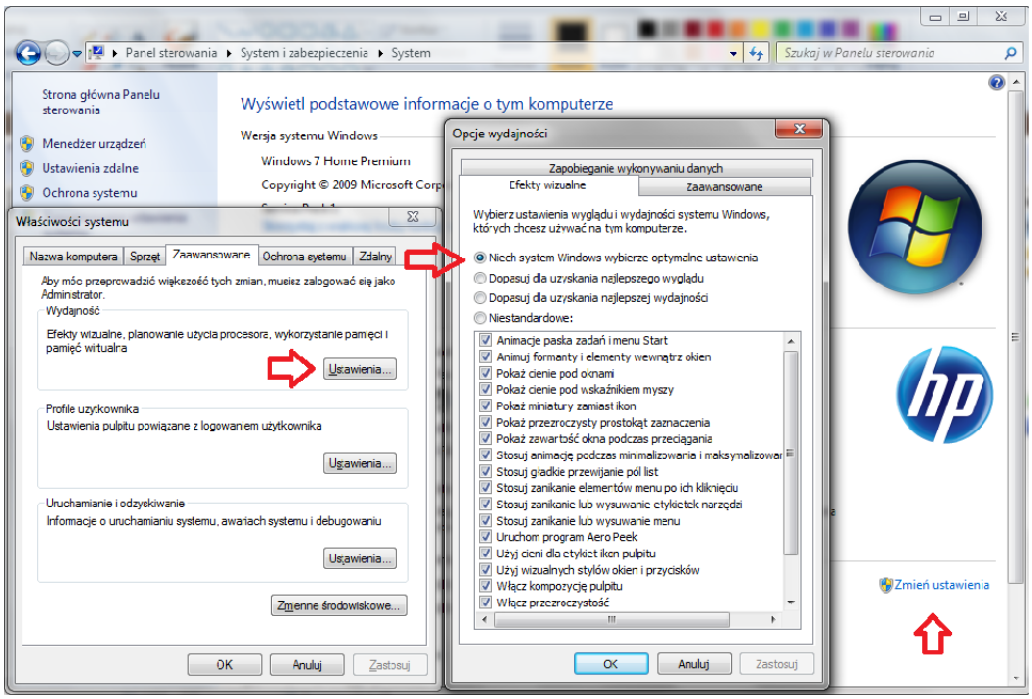
Rys. 4.6: Aktualizacja systemu.



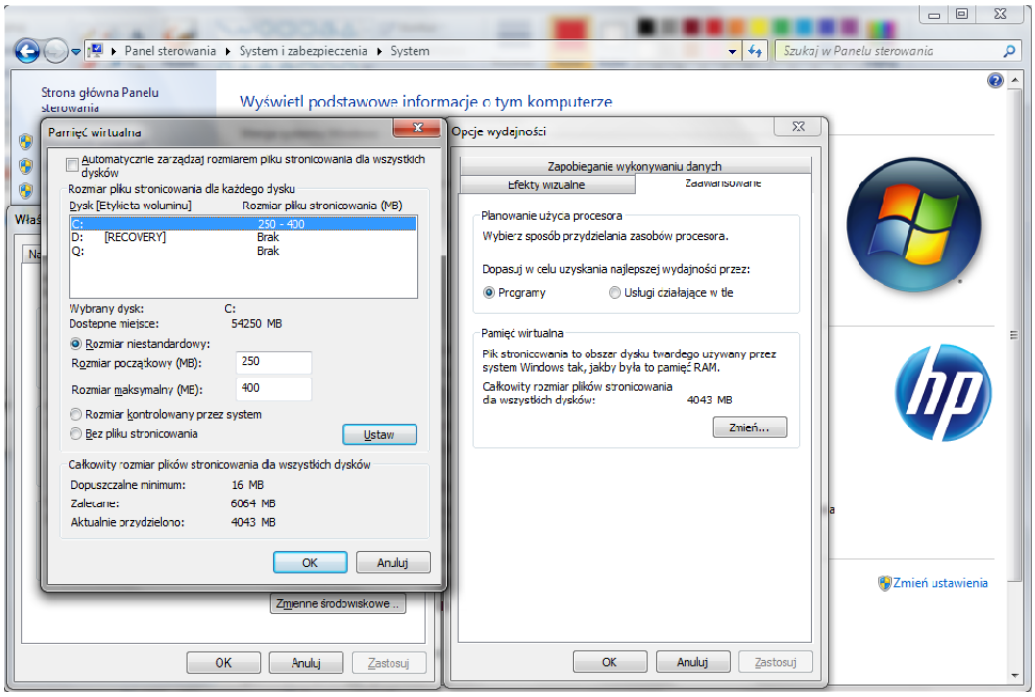
Rys. 4.7: Okno konfiguracji kopii zapasowych systemu Windows 7.



Rys. 4.8: Zdarzenia w systemie.

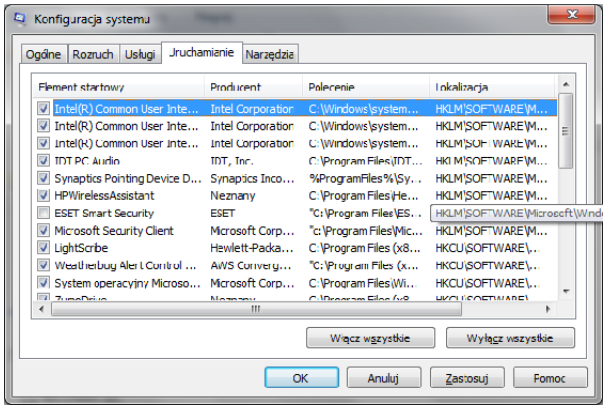


(a) Wydajność.

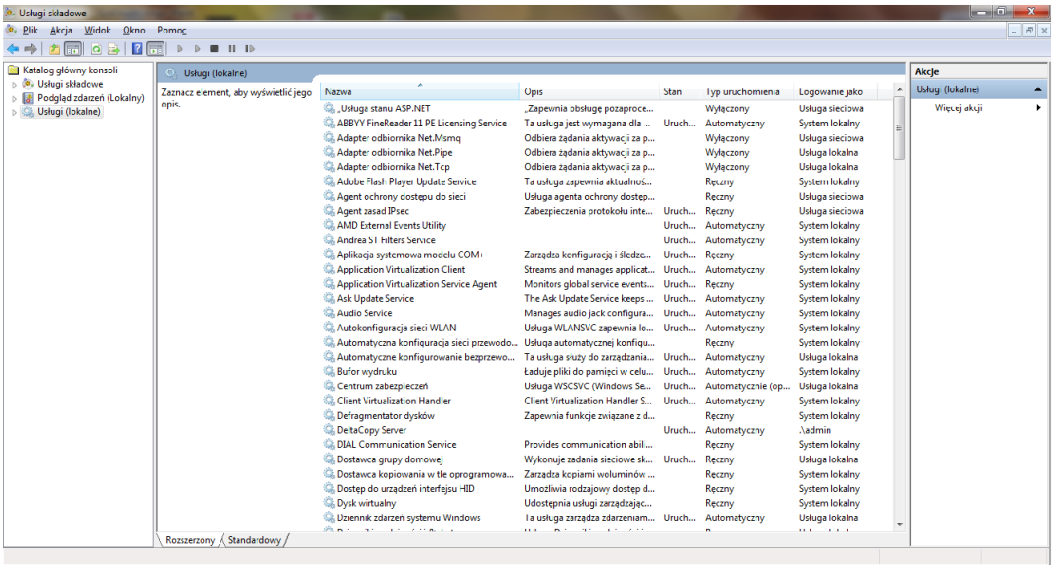


(b) Ustawienia ręcznie pamięci wirtualnej.

Rys. 4.9: Zwiększanie wydajności systemu Windows 7.

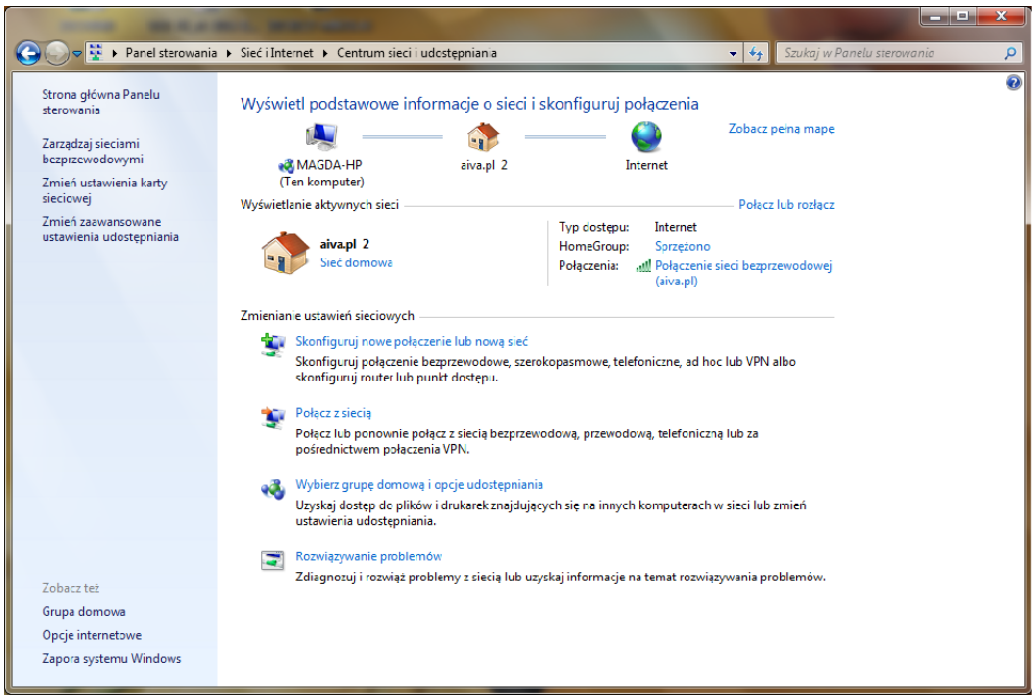


(a) Lista uruchomionych usług.

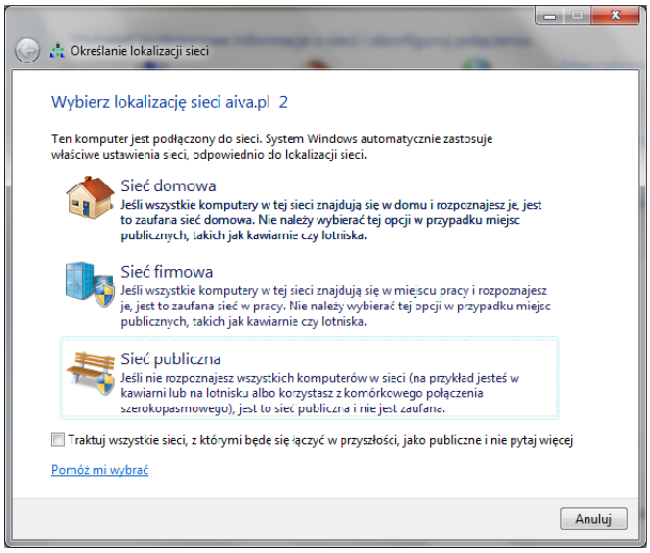


(b) Lista usług systemu.

Rys. 4.10: Konfiguracja usług systemu Windows 7.

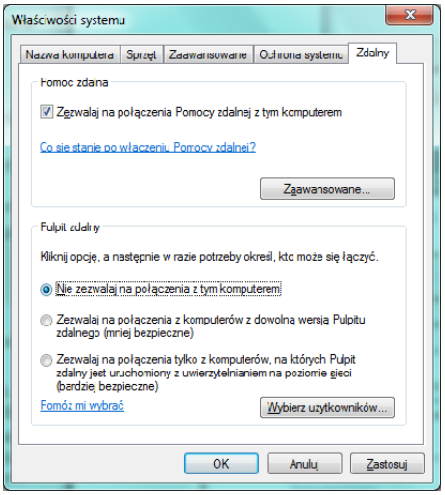


(a) Sieć i udostępnianie.

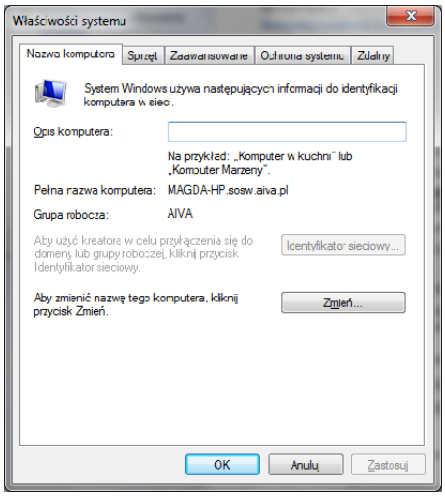


(b) Lokalizacja sieci.

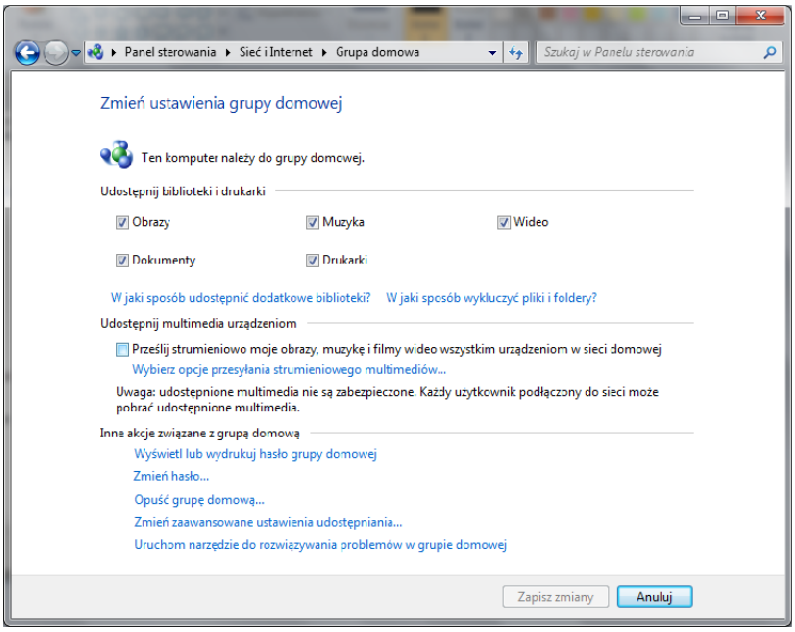
Rys. 4.11: Sieć.



Rys. 4.12: Zdalny pulpit.

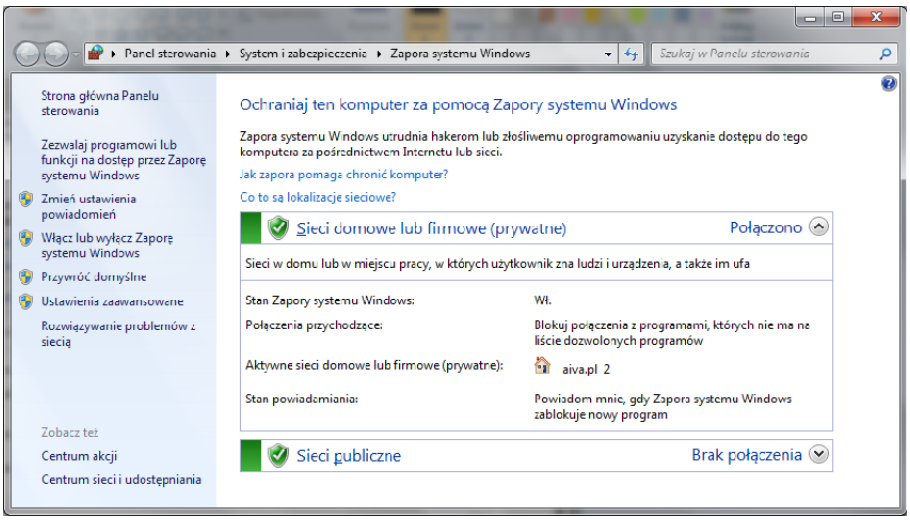


(a) Grupa robocza

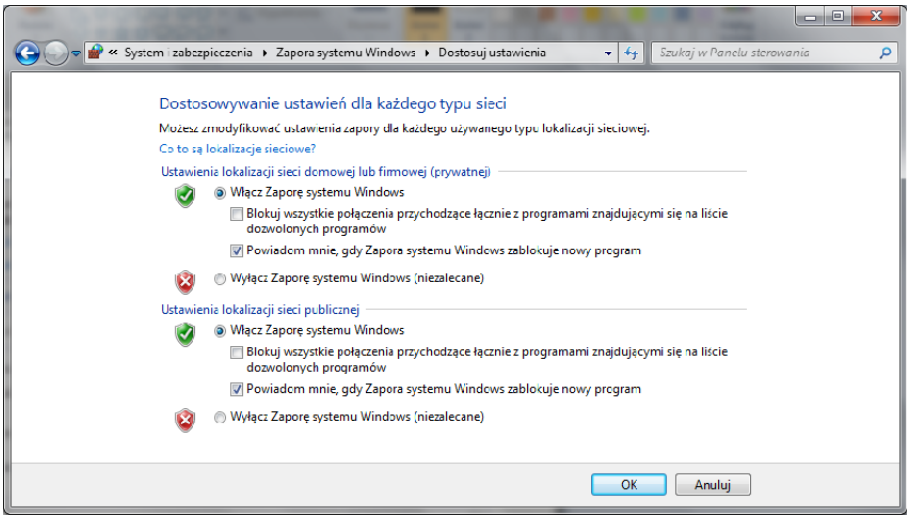


(b) Grupa domowa.

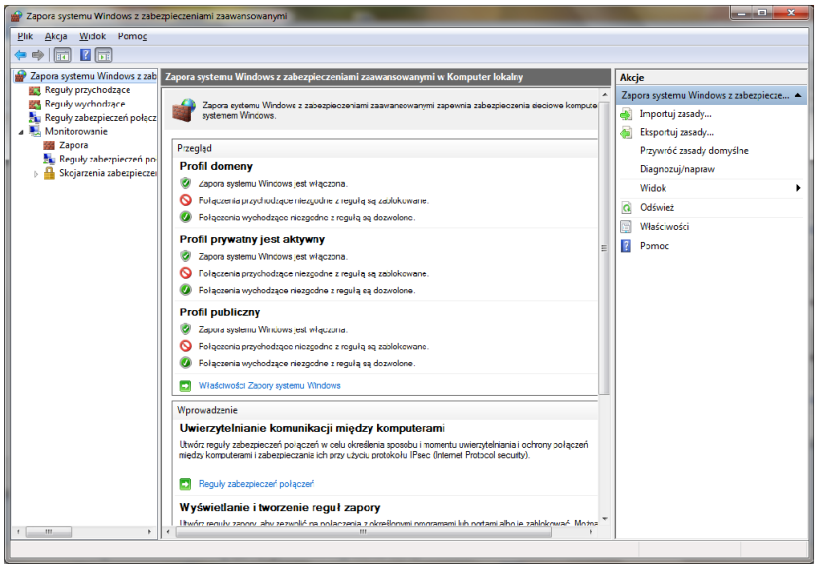
Rys. 4.13: Grupa robocza.



(a) Zapora.

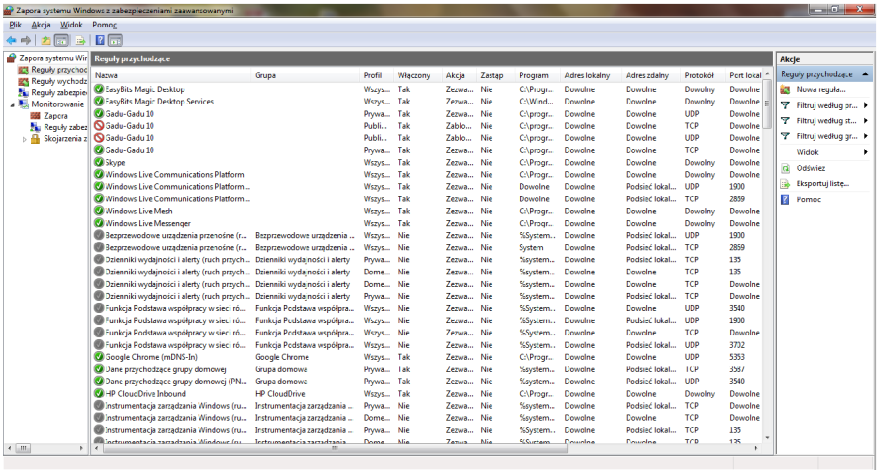


(b) Ustawienia zapory.

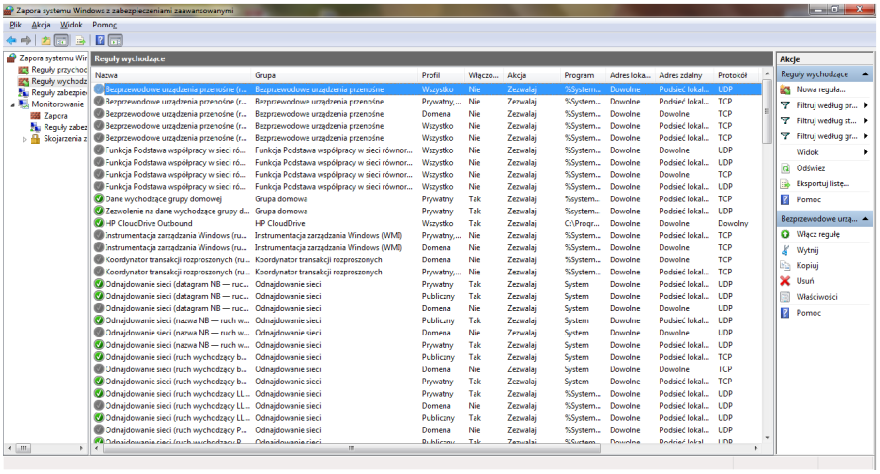


(c) Zaawansowane ustawienia zapory.

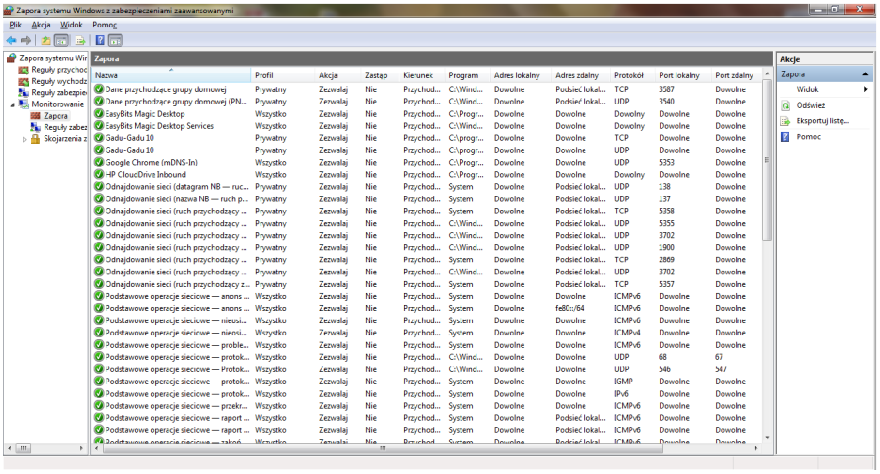
Rys. 4.14: Ustawienia zapory ogniowej w systemie Windows 7.



(a) Reguły dla ruchu przychodzącego.

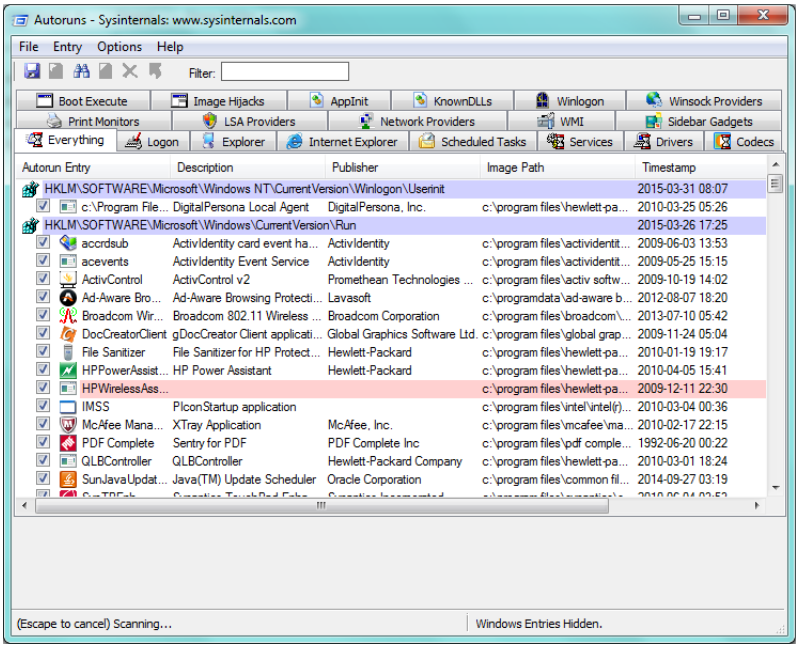


(b) Reguły dla ruchu wychodzące.

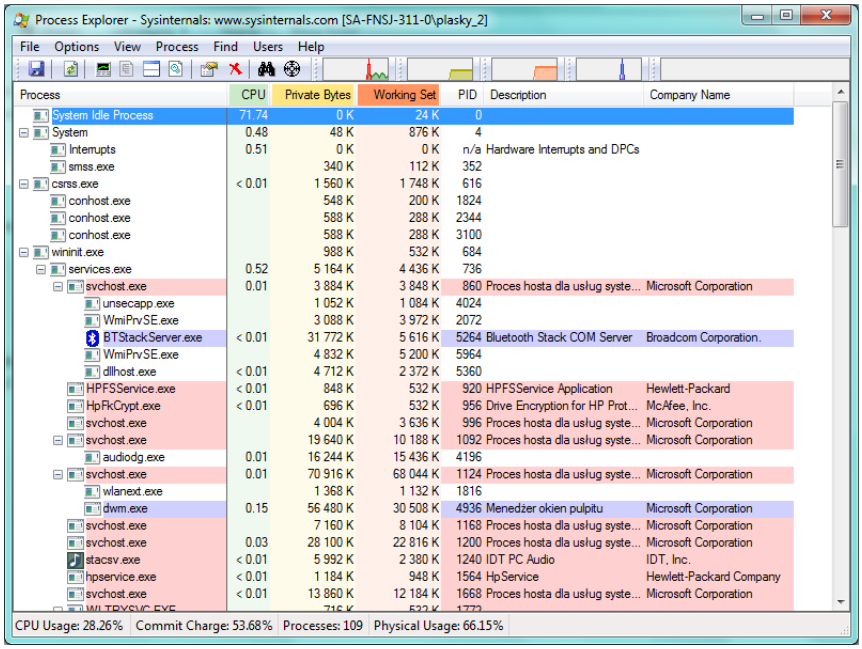


(c) Ruch na zaporze.

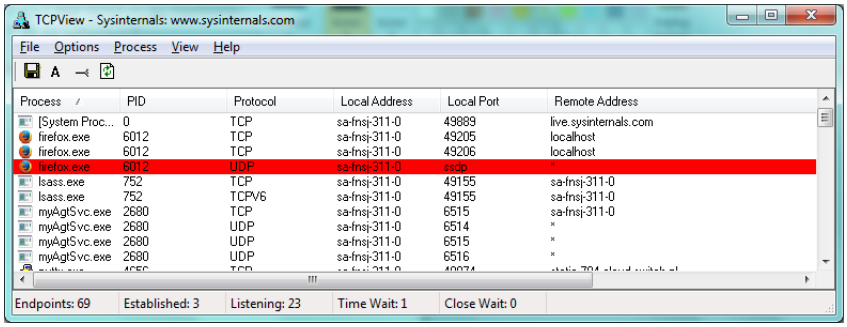
Rys. 4.15: Reguły zapory.



Rys. 4.16: Sysinternals - AutoRuns.



Rys. 4.17: Sysinternals - Process Explorer.



Rys. 4.18: Sysinternals - TcpView.

Rozdział 5

Oprogramowanie złośliwe

Oprogramowanie złośliwe jest szeroko rozpowszechnione szczególnie w środowisku systemu operacyjnego Windows (XP,7,8,10) dla użytkownika końcowego. Jest to spowodowane (po części) lukami w systemie oraz niefrasobliwością użytkowników związaną z pracą użytkowników na kontach administratorów systemu (z uprawnieniami administratora). W takim przypadku łatwo jest zainfekować system oprogramowaniem złośliwym. Termin ten obejmuje szereg różnych rodzajów oprogramowanie. Można go opisać za pomocą def. 5.1.

Definicja 5.1. *Złośliwe oprogramowanie, (malware ang. malicious software) to wszelkiego rodzaju programy działające na szkodę użytkownika komputera. Mogą mieć charakter przestępczy.*

Do najczęściej spotykanych rodzajów złośliwego oprogramowania należą:

- Wirus
- Robak
- Trojan
- Spyware

W dalszej części omówiono także inne rodzaje występującego oprogramowania złośliwego.

Wirus Wirus program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika. Ze względu na różne rodzaje infekcji wirusy dzielą się na:

- wirusy gnieżdżące się w sektorze rozruchowym twardego dysku (*ang. boot sector viruses*),
- wirusy pasożytnicze (*ang. parasitic viruses*),
- wirusy wieloczęściowe (*ang. multi-partite viruses*),
- wirusy towarzyszące (*ang. companion viruses*),
- makrowirusy (*ang. macro viruses*).

Robak Robak (*ang. worm*) - złośliwe oprogramowanie podobne do wirusów, rozmnażające się tylko przez sieć. W przeciwieństwie do wirusów nie potrzebują programu *żywiciela*. Oprogramowanie często powiela się poprzez pocztę elektroniczną.

Wabbit Wabbit - program rezydentny nie powielający się przez sieć. Wynikiem jego działania jest jedna określona operacja, np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera.

Trojan Trojan - to program, który ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje w tle operacje szkodliwe dla użytkownika, np. otwiera port komputera, przez który może być dokonany atak włamywacza (hakera).

Backdoor Backdoor - przejmuje kontrolę nad zainfekowanym komputerem, umożliwiając wykonanie na nim czynności administracyjnych, łącznie z usuwaniem i zapisem danych. Podobnie jak trojan, backdoor podszywa się pod pliki i programy, z których często korzysta użytkownik. Umożliwia intruzom administrowanie systemem operacyjnym poprzez Internet. Wykonuje wtedy zadania wbrew woli i wiedzy użytkownika.

Spyware Programy szpiegujące (*ang. spyware*) - oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody, jak informacje o odwiedzanych witrynach, hasła dostępowe itp. Występuje często jako dodatkowy i ukryty komponent większego programu, odporny na usuwanie i ingerencję użytkownika. Programy szpiegujące mogą wykonywać działania bez wiedzy użytkownika - zmieniać wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Program szpiegujący może pobierać i uruchamiać pliki pobrane z sieci.

- scumware (*ang. scum* - piana; szumowiny, męty) - żargonowe, zbiorcze określenie oprogramowania, które wykonuje w komputerze niepożądane przez użytkownika czynności.
- stealware/parasiteware - służące do okradania kont internetowych,
- adware - oprogramowanie wyświetlające reklamy,
- Hijacker Browser Helper Object - dodatki do przeglądarek, wykonujące operacje bez wiedzy użytkownika.

Exploit Exploit - kod umożliwiający bezpośrednie włamanie do komputera. Do dokonania zmian lub przejęcia kontroli wykorzystuje się lukę w oprogramowaniu zainstalowanym na atakowanym komputerze. Exploity mogą być użyte w atakowaniu stron internetowych, których silniki oparte są na językach skryptowych (zmiana treści lub przejęcie kontroli administracyjnej), systemy operacyjne (serwery i końcówki klienckie) lub aplikacje (pakiety biurowe, przeglądarki internetowe lub inne oprogramowanie).

Rootkit Rootkit - jedno z najniebezpieczniejszych narzędzi hackerskich. Ogólna zasada działania opiera się na maskowaniu obecności pewnych uruchomionych programów lub procesów systemowych (z reguły służących hackerowi do administrowania zaatakowanym systemem). Rootkit zostaje wkompilowany (w wypadku zainfekowanej instalacji) lub wstrzyknięty w istotne procedury systemowe, z reguły jest trudny do wykrycia z racji tego, że nie występuje jako osobna aplikacja. Zainstalowanie rootkita jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie ukryta kradzież danych lub infiltracja.

Keylogger Keylogger - Odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody lub cenne informacje mogą dostać się w niepowołane ręce. Pierwsze programowe keyloggery były widoczne w środowisku operacyjnym użytkownika. Teraz coraz częściej są procesami niewidocznymi dla administratora. Istnieją też keyloggery występujące w postaci sprzętowej zamiast programowej.

Dialer Dialery - programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika, najczęściej są to numery o początku 0-700 lub numery zagraniczne. Dialery szkodzą tylko posiadaczom modemów telefonicznych analogowych i cyfrowych ISDN, występują głównie na stronach o tematyce erotycznej. Obecnie mają mniejsze znaczenie ze względu na odchodzenie od połączeń dodzwanianych (modemodych).

Inne rodzaje szkodliwego oprogramowania Mniej szkodliwe złośliwe oprogramowanie to:

- fałszywe alarmy dotyczące rzekomo nowych i groźnych wirusów (*ang. false positives*); fałszywy alarm to także rzekome wykrycie zainfekowanego pliku, które powodują programy antywirusowe z najwyższym poziomem analizy heurystycznej.
- żarty komputerowe, robione najczęściej nieświadomym początkującym użytkownikom komputerów.

5.1 Wybrane oprogramowanie do usuwania złośliwego oprogramowania

Na rynku oferowanych jest szereg programów do usuwania lub walki ze złośliwym oprogramowaniem. Istnieje kilka głównych firm o ugruntowanej od lat pozycji rynkowej. Działanie skanerów antywirusowych polega na odszukiwaniu tzw. znaczników

MalwareBytes AntiMalware for Business Program zmniejsza wrażliwość na złośliwe oprogramowanie typu zero-hour. Dostarcza odpowiednie narzędzi na poziomie korporacyjnym. Program jest niezwykle skuteczny w usuwaniu oprogramowania złośliwego, które nie jest wykrywane przez inne systemy antywirusowe. Program posiada mechanizm skanowania heurystycznego, umożliwia blokowanie złośliwych witryn, może pracować pod kontrolą systemów serwerowych.

Umożliwia zarządzanie wieloma klientami, nawet do kilku tysięcy z pojedynczej konsoli. Program integruje się z Active Directory.

Eset node Obecny od wielu lat na rynku jeden z najlepszych systemów ochrony komputerów. Oferuje szereg mechanizmów ochrony:

- Antywirus i antyspyware Chroni przed wszelkiego typu zagrożeniami - wirusami, robakami czy rootkitami.
- Antyphishing Chroni dane z kart kredytowych oraz loginy i hasła do kont bankowych, przed próbami ich wyłudzenia.
- Anti-Theft Zabezpiecza komputer na wypadek kradzieży lub zgubienia sprzętu.
- Ochrona bankowości internetowej Zwiększa bezpieczeństwo podczas dokonywania płatności online.
- Ochrona przed botnetami Zabezpiecza przed zagrożeniami, które bez wiedzy i zgody użytkownika przyłączają komputer do tzw. sieci botnet.
- Antyspam Skutecznie filtruje i blokuje niechciane wiadomości spamowe, wysyłane na stacje robocze.

F-Secure System wykorzystuje zautomatyzowane systemy sztucznej inteligencji wykorzystujące analizę heurystyczną i analizy działania złośliwego oprogramowania korzystając z informacji umieszczonych w sieci (*ang. Security Cloud* - informowanie o zagrożeniach w czasie rzeczywistym oparte na chmurze). Oprogramowanie otrzymało szereg nagród Best Protection przyznawaną przez organizację AV-TEST.

Program F-Secure Anti-Virus oferuje ochronę w czasie rzeczywistym przed wirusami, oprogramowaniem szpiegującym, zainfekowanymi załącznikami wiadomości e-mail i innymi formami złośliwego oprogramowania.

McAfee Cały pakiet programów do ochrony komputera przez złośliwym oprogramowaniem. Pakiet preinstalowany jest na wielu komputerach PC, szczególnie laptopach. Przeszukuje następujące obszary systemu: dyski lokalne i sieciowe, tablice partycji, boot sektory, napędy CD-ROM, stacje dyskietek oraz pliki skompresowane. W pakiecie dostępna jest zapora ogniowa. Wadą programy jest duże obciążenie systemu.

5.2 Microsoft Essentials

Dedykowany system antywirusowy firmy Microsoft dla komputerów pracujących pod kontrolą systemu Windows. Program jest darmowy do użytku prywatnego.

Program łączy funkcje programów Live OneCare oraz Windows Defender. Wyróżniającą się cechą aplikacji jest niewielkie obciążenie systemu, niemal niezauważalne podczas codziennej pracy. Program zapewnia ochronę w czasie rzeczywistym, działa w tle i wyświetla alerty tylko w przypadku, gdy wymagane jest podjęcie określonych przez użytkownika działań. Proces skanowania może zostać zaplanowany także według określonego harmonogramu. Microsoft Security

Essentials oferuje funkcję tworzenia punktów przywracania systemu, tworzenia listy wykluczeń, oraz integruje się z zaporą systemu Windows.

Rozdział 6

Ataki na systemy komputerowe i metody obrony

Ataki na systemy komputerowe dotyczą głównie serwerów, które stale podłączone są do sieci i oferują określony zestaw usług. Posiadają stały adres IP, łatwo je zlokalizować. Im ważniejszy serwer tym hakerzy bardziej interesują się nim. Podstawowymi serwerami (usługami) działającymi w sieci są najczęściej:

- serwer pocztowy,
- serwer DNS,
- serwer stron WWW,
- serwer bazodanowy,
- serwer umożliwiający pracę zdalną (telnet, obecnie ssh),
- serwer usług katalogowych

Wymienione wyżej usługi w różnym stopniu narażone są na ataki. Niektóre rodzaje ataków wykorzystują właściwości sieci oraz sposoby jej działania. W dalszej części zostaną omówione niektóre rodzaje ataków na wybrane usługi. Szczegółowa analiza poszczególnych ataków wykracza poza ramy niniejszej publikacji. Sposoby obrony można znaleźć w literaturze specjalistycznej poświęconej administracji i zabezpieczaniu systemów serwerowych. Dobrym źródłem informacji są także najnowsze informacje publikowane w sieci. Stosowane techniki i sposoby konfiguracji zależne są od systemu operacyjnego i konkretnego oprogramowania obsługującego daną usługę.

6.1 Atak Dos

DoS (*ang. Denial of Service*, odmowa usługi) to atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania.

Atak polega zwykle na przeciążeniu usługi serwera. Na skutek wyczerpania się limitu np. wolnych gniazdek do połączenia z usługą dana usługa staje się niedostępna. Atak ten dotyczy także np. zapełnienie całego systemu plików tak,

by nie można było dograć kolejnych informacji, np. w przypadku serwerów FTP. Wykorzystywane są także błędy powodujące powodujące błąd wykonania aplikacji obsługującej usługę. W sieciach komputerowych atak Dos oznacza zwykle zalewanie sieci (*ang. flooding*) nadmiarową ilością danych mających na celu zajęcie całego dostępnego pasma, którym dysponuje atakowany serwer. W takim przypadku usługa niemożliwe staje się połączenie z serwerem, pomimo że usługi pracujące na serwerze są gotowe do przyjmowania połączeń. Przykładem tego typu ataku jest np. fork bomba. Polega on na ciągłym uruchamianiu procesu potomnego bez warunku jego zakończenia. Podstawowa implementacja fork bomby (fork to nazwa funkcji systemowej służącej do tworzenia nowych procesów) jest nieskończoną pętlą która uruchamia ten sam proces. Atak opiera się na założeniu, że w środowisku wieloprocesowym tylko pewna liczba procesów może być efektywnie wykonywana naraz.

Przykłady fork bomby:

- tworzenie procesów potomnych w języku C dla systemu Unix/Linux
  - w postępie liniowym

```
#include <unistd.h>

int main(void)
{
    while(1)
          fork();
      return 0;
}
```

  - w postępie geometrycznym szybszym od liniowego

```
#include <unistd.h>

int main(void)
{
  while(fork()!=-1)
    fork();
  return 0;
}
```

- tworzenie procesów potomnych z linii komendy systemu Unix/Linux (bash)

```
:(){ :|:& };:
```

- tworzenie procesów potomnych za pomocą pliku wsadowego (*.bat) dla systemu Windows:

```
:loop
start %0
goto loop
```

Odmianą ataku DoS jest DDoS (*ang. distributed denial of service*), a także DRDoS (*ang. distributed reflected denial of service*).

Metody obrony Jedną z metod obrony jest ustawienie limitu liczby procesów, które może uruchomić użytkownik. Gdy proces próbuje utworzyć inny proces, a jego rodzic posiada już więcej niż przewiduje maksimum, tworzenie procesów potomnych nie następuje. Maksimum powinno na tyle niskie, aby w razie ataku maszyny przez wielu użytkowników naraz pozostawić wystarczającą ilość wolnych zasobów dla uniknięcia zatrzymania systemu. W systemie Linux dostępny jest program *watchdog*, który kontroluje ilość oczekujących procesów.

6.2 Atak na system DNS

Atak *ang. DNS Amplification* jest odmianą ataku DDos. Polega on wysyłaniu zapytań do serwerów DNS ze sfałszowanym adresem zwrotnym (*ang. spoofing*) w sieci przejętej przez hackerów (*ang. botnet*). Serwery DNS, w odpowiedzi na dziesiątki lub setki tysięcy zapytań kierowanych z komputerów hackera, wysyłają odpowiedzi na komputer będący celem ataku. W ten sposób następuje zajęcie całego pasma, pamięci i mocy obliczeniowej. Obrona przed takim atakiem jest bardzo trudna, gdyż trudno jest odfiltrować odpowiedzi od DNS na odpowiedzi na zadane i na niezadane zapytania.

Metody obrony Możliwość przeprowadzenia ataku wymaga przejęcia sieci przez hackerów. Jest to wykonywane najczęściej poprzez atak na niezabezpieczone routery i podmianę adresów serwerów dns na routerach. Tak więc, przede wszystkim należy chronić konfigurację routerów.

W przypadku serwerów DNS metodą obrony jest wprowadzenie mechanizmów uwierzytelniania serwerów DNS (DNSSEC) wobec siebie oraz takie konfigurowanie serwerów DNS, aby udzielały odpowiedzi na zapytania dotyczące obsługiwanej domeny. Wprowadza się także zabezpieczenia przed wielokrotnymi zapytaniami z jednego adresu IP oraz kolejkowanie zapytań oraz usuwanie zapytań zduplikowanych, minitorowanie pasma i liczby zapytań. Dobrą metodą jest usuwanie nieprawidłowych zapytań (nieprawidłowy format). Opis metod obrony można znaleźć np. w [6].

Atak na system dns Netii - 2014 Poniżej zamieszczono mały fragment artykułu z www.pcworld.pl na temat ataków na systemy DNS.

```
...
Netia kontratakuje

Na ataki sieciowe szybko zareagowała również Netia. W odróżnieniu od Orange,
operator ten nie zdecydował się jednak na całkowite zablokowanie serwerów
DNS-ów należących do oszustów internetowych.

Zamiast tego, zapytania skierowane do fałszywych serwerów DNS są
automatycznie przekierowywane na legalne DNS-y Netii. Według operatora,
rozwiązanie to jest bardziej skuteczne i mniej uciążliwe dla klientów.
Problem w tym, że w ten sposób wielu użytkowników nigdy nie zauważy faktu, że
cyberprzestępcy przejęli kontrolę nad ich routerem.
```

Sprawdzenie podatności routera domowego na ataki można sprawdzić za pomocą narzędzia udostępnionego przez firmę Orange: http://niebezpiecznik.pl/post/orange-wypuszcza-skaner-domowych-routerow/.

Należy także sprawdzić, czy router może być konfigurowany z internetu. Firma Orange udostępniła odpowiednie narzędzie *modemscan* do weryfikacji routerów: http://www.cert.orange.pl/modemscan.

Routery można zabezpieczyć także ręcznie. W tym celu należy:

- Zmienić hasło do zarządzania routerem (hasło administratora).
- Zablokować możliwość dostęp z zewnątrz (z internetu) do panelu administracyjnego.
- Aktualizować możliwie często oprogramowanie routera (*ang. firmware*).
- Ustawić stałe adresy DNS na urządzeniach podłączonych do routera (np. 8.8.8.8, 8.8.4.4)

6.3 Atak na system pocztowy

System pocztowy jest jednym z najbardziej narażonych na ataki części systemu komputowego.

Atak może zostać przeprowadzony na serwer pocztowy lub na klienta pocztowego. Istnieje dwa podstawowe sposoby korzystania z systemu pocztowego:

- za pomocą przeglądarki internetowej poprzez interfejs WWW systemu pocztowego. Poczta przechowywana jest na serwerze. Odczyt następuje na stronie WWW systemu obsługi poczty.
- poprzez klienta pocztowego. W tym przypadku program pocztowy (klient), którym może być np. Microsoft Outllok, Mozilla Thunderbird i inne, łączy się z serwerem i pobiera pocztę z serwera lokalnie na komputer.

Głównym zagrożeniem dla serwera pocztowego jest:

- rozsyłanie niechcianej poczty, np. w przypadku gdy serwer jest *ang. open-relay*.
- spam - przesyłanie na serwer niechcianej poczty.
- atak typu DDos mający na celu unieruchomienie serwera pocztowego.
- włamanie na konto użytkownika przez przejęcie login'u i hasła.
- podszywanie się pod użytkownika systemu pocztowego.

Z punktu widzenia klienta najważniejsze zagrożenia to:

- Przesłanie na konto niechcianej poczty (spam)
- Przejęcie zawartości maili z komputera użytkownika.
- Przesłanie złośliwego oprogramowania zamieszczonego w treści mail'a (np. w załączniku)

- Wykorzystanie klienta pocztowego do przesyłania niechcianej poczty.
- Wyłudzenia danych od użytkownika.
- Wprowadzenie użytkownika w błąd poprzez specjalnie zredagowanego mail'a.

6.3.1 Metody obrony

Metody obrony po stronie serwera to:

- Konfiguracja serwera pocztowego w sposób umożliwiający bezpieczne połączenia klientów: uwierzytelnienie przy pomocy loginu i hasła, nawiązanie połączenia szyfrowanego (np. TLS, SSL).
- Instalacja systemu antywirusowego, który automatycznie skanuje zawartość mail'i pod kątem występowania złośliwego oprogramowania,
- Podłączenie do systemów antyspamowych w sieci. Integracja systemu antyspamowego z lokalnym systemem firewall do automatycznego blokowania hostów rozsyłających spam.
- Instalacja list kontroli dostępu (ACL):

  wprowadzenie blokowania załączników określonych typów: *.com, *vbs, *.bat, *.pif, *.scr.

  zamrażanie załączników zawierających pliki: *.exe i *.doc.
- Sprawdzanie poprawności adresów e-mail odbieranych mail'i.
- Wprowadzanie ograniczania liczby odbiorców mail'a przesyłanego w jednym połączeniu.
- Sprawdzanie adresów IP i adresów mail'i na czarnych listach umieszczonych na odpowiednich serwerach w sieci.
- stosowanie systemu czarnych i białych list lokalnie na serwerze.
- Potwierdzanie istnienia adresu e-mail nadawcy wiadomości przez zapytanie serwera DNS i ustalenie rzeczywistego adresu IP. W przypadku niezgodności poczta jest odrzucana.
- Odrzucania poczty z hostów, które nie posiadają rutowalnego adresu IP.
- Automatyczne blokowanie hostów rozsyłających w jednym połączeniu wiele maili (bardzo skuteczna metoda).

Szczegółowe omówienie serwerów pocztowych wykracza znacznie poza zakres tej publikacji. Porównanie serwerów pocztowych można znaleźć np. pod adresem http://en.wikipedia.org/wiki/Comparison_of_email_clients Serwery różnią się pomiędzy sobą sposobem licencjonowania, poziomem bezpieczeństwa, możliwościami integracji z innymi systemami (antywirusowymi, antyspamowymi). Niemniej jednak poniżej zostaną scharakteryzowane główne serwery pocztowe używane na świecie, do których należą:

sendmail - popularny serwer pocztowy rozwijany od 1979. Oferuje wiele sposobów przesyłania i dostarczania poczty. Sendmail był najpopularniejszym serwerem pocztowym w internecie, m.in. ze względu nato, że był standardowym programem tego typu wielu systemach typu Unix. Program obecnie stracił na popularności ze względu na skomplikowaną konfigurację i problemy z bezpieczeństwem. Jest rozpowszechniany zarówno jako wolne oprogramowanie jak i na licencjach zamkniętych.

exim4 jest serwerem pocztowym, który zastąpił serwer *sendmail* w systemach Linux. Exim jest najbardziej zaawansowanym serwerem pocztowym stworzonym na University of Cambridge. Niestety konfiguracja serwera jest dosyć skomplikowana. Może korzystać z wielu innych systemów, jak systemy antyspamowe, systemy antywirusowe, wykorzystuje czarne i białe listy (także lokalne). System korzysta z list kontroli dostępu (ACL) oraz systemu DNS do blokowania niechcianej poczty. Posiada filtry sprawdzający poprawność maili oraz może filtrować ich zawartość. Umożliwia różne sposoby uwierzytelniania użytkownika, współpracuje z modułami do szyfrowania kanału komunikacyjnego i uwierzytelniania. Może także pośredniczyć w przesyłania poczty (tzw. serwer *ang. open relay*). Posiada wiele innych bardzo zaawansowanych funkcji. Jest systemem bardzo elastycznym. Sposób konfiguracji serwera można znaleźć w [11] lub na stronie projektu http://www.exim.org/.

postfix przeznaczony jest do pracy w systemach Unix/Linux. Opracowany został w firmie IBM. Postfix obsługuje różne protokoły komunikacyjne (SMTP, LMTP, IPv6, TLS, SASL), skrzynki pocztowe w formacie Maildir oraz mbox, a także wirtualne domeny. Ma zaimplementowanych szereg mechanizmów używanych do wykrywania i usuwania spamu (obsługuje czarne listy, SPT, protokół Sendmail Milter) oraz umożliwia filtrowanie na podstawie zawartości maili. Obsługuje różne bazy danych (Berkeley DB, CDB, DBM, LDAP, MySQL i PostgreSQL) do przechowywania danych systemu pocztowego jak: aliasy, nazwy kont, konta wirtualne. Postfix współpracuje z wieloma demonami, które odpowiadają za różne etapy przetwarzania i dostarczania poczty. Minimalizuje to ewentualne skutki istnienia luk w bezpieczeństwie, gdyż każdy z deamonów pracuje z minimalnymi uprawnieniami. System przeznaczony jest do obsługi bardzo dużej ilości poczty. Posiada narzędzia do analizy wydajności.

6.3.2 Czarne listy

Obrona przed spamem może być realizowana przez podłączenie systemu pocztowego do serwerów czarnych list (*ang. black list*). Przechowują one adresy IP i DNS hostów, które rozsyłają spam oraz adresy e-mail spamerów.

Poniżej zamieszczono przykładowe adresy serwerów czarnych list:

- http://www.dnsbl.info/
- bl.spamcop.net
- blackholes.wirehub.net
- blacklist.sci.kun.nl

- block.dnsbl.sorbs.net
- cbl.abuseat.org
- dnsbl.abuse.ch
- dnsbl.anticaptcha.net
- dnsbl.antispam.or.id
- http://www.dnsbl-check.info/
- http.dnsbl.sorbs.net
- new.dnsbl.sorbs.net
- pbl.spamhaus.org
- http://psbl.org/
- sbl.spamhaus.org
- smtp.dnsbl.sorbs.net
- socks.dnsbl.sorbs.net

Niektóre z nich posiadają możliwości sprawdzenia przez stronę WWW adresu - rys. 6.1.

Rys. 6.1: Sprawdzenie adresu IP na czarnych listach.

Serwery prowadzą własne czarne i białe listy, na które administrator może wpisać adresy, z których rozsyłana jest np. niechciana poczta. Są one podłączone często do lokalnego firewalla, który może automatycznie blokować ruch z danego adresu.

Dedykowanym oprogramowaniem w systemie Linux jest pakiet: *greylistd*.

```
greylist add --black xxxx.domain
```

Wypisanie adresów na listach.

```
greylist list
```

Białe listy to listy numerów IP lub adresów DNS, z którymi serwer będzie współpracował i nie będzie sprawdzał ruchu.

Rozdział 7

Ochrona i zabezpieczanie systemów informatycznych

Dla służby ochrony państwa, pionów ochrony, administratorów systemu lub sieci teleinformatycznych istotne jest ustalenie w jaki sposób osoby odpowiedzialne korzystają z systemów informatycznych. W szczególności brane są pod uwagę następujące aspekty korzystania z systemów informatycznych:

- Prawidłową konfigurację systemów komputerowych, w tym:
  - zapewnienie aktualności oprogramowania,
  - prawidłowa konfiguracja i włączenie zapory sieciowej (firewall),
  - instalacja i prawidłowa konfiguracja programu antywirusowego.
- Jakie uprawnienia posiada konto, na którym pracuje użytkownik systemu (konto zwykłego użytkownika, konto administratora)?
- W jaki sposób wykorzystują konto przydzielone do pracy z systemem informatycznym?
- Czy użytkownicy ujawniają przydzielone hasła dostępu, gdzie przechowują hasła, jak często zmieniają hasła i jak tworzą nowe hasła?
- Czy można po nieautoryzowanym logowaniu uzyskać dostęp do zastrzeżonych informacji?
- W jaki sposób chroniony jest dostęp do informacji zgromadzonych w systemie?
- Jakie są najsłabsze miejsca systemu?
- Czy okresowo analizowany jest stan bezpieczeństwa systemu lub sieci teleinformatycznych?

7.1 Zabezpieczenia sieci komputerowych przed atakami z zewnątrz

Zabezpieczenie sieci komputerowych przed atakami z zewnątrz obejmuje następujące zagadnienia:

- Systemy Kontroli dostępu;
- Urządzenia szyfrując;
- Monitorowanie i audyt sieci.

System Kontroli Dostępu weryfikuje tożsamość i autoryzację użytkowników systemów poprzez:

- autentykację - pozytywną identyfikację użytkownika w sieci;
- autoryzację - określenie praw dostępu do poszczególnych zasobów systemu;
- audyt - zbieranie informacji o dostępie do zasobów systemu.

Systemy Monitoringu to specjalne programy (skanery internetowe), które kontrolują ruch w sieci i wykrywają jej słabe punkty. Umożliwiają sprawdzenie, czy w sieci istnieją luki i błędy. Na bieżąco naprawiają wszelkie przekłamania. Pozwalają na sporządzanie szczegółowych raportów na temat bezpieczeństwa sieciowego. Na bieżąco analizują ruch w sieci i wpisy do logów.

Monitoringiem zajmują się również systemy wykrywania wtargnięć intruzów oraz systemy obsługi incydentów, pozwalające na precyzyjny opis próby wtargnięcia i na tej podstawie rekonfigurację sieci w celu uniknięcia podobnych sytuacji w przyszłości.

Obecnie ze względu na prostotę bardzo często wykorzystuje się sieci bezprzewodowe. Zabezpieczenie sieci bezprzewodowej związane jest z prawidłową konfiguracją routerów i/lub serwerów pracujących w sieci. Należy także wziąć pod uwagę kwestie dostępności sieci i szybkości jej działania, gdyż nawet najlepiej zabezpieczona, ale nie działająca sieć bezprzewodowa jest bezużyteczna.

Konfiguracja sieci bezprzewodowej obejmuje następujące zagadnienia:

- dobór odpowiedniego routera posiadającego wystarczające możliwości konfiguracyjne;
- dobór kanału transmisyjnego, który jest najmniej obciążony;
- konfiguracja odpowiednich protokołów zabezpieczających łączność w sieci bezprzewodowej;
- ustalenie odpowiedniego, trudnego do złamania hasła dostępu do sieci, wykorzystując maksymalnie dostępną długość hasła oraz odpowiednie skomplikowanie;
- ustalenie ograniczenia dostępu komputerów do sieci, np. poprzez ustawienie na routerach adresów MAC kart sieciowych komputerów, które mogą łączyć się z siecią;

- ustalenie sposobu przydziału puli adresów IP dla zalogowanych użytkowników, przy czym należy rozważyć możliwość włączenia się do sieci *gości* - komputerów o niedopuszczonych adresach MAC;
- ustalenie polityki separacji (lub nie) komputerów pracujących w sieci lub gałązkach sieci;
- ustalenie metod podnoszenia szybkości działania sieci np. dla transmisji strumieniowych (audio, video);
- ustalenie metod rozszerzenia zasięgu sieci przez współpracę z innymi routerami skonfigurowanymi w trybie mostka (bridge) lub repeatera. Niektóre routery pracujące w trybie mostka WI-FI umożliwiają ograniczenie ruchu w sieci przez zastosowanie algorytmów uczenia się kierowania ramek sieci.

7.2 Backup

Backup i archiwizacja danych to metody zabezpieczenia przed zniszczeniem (być może przypadkowym) danych przetwarzanych w systemach komputerowych. Należy rozróżnić dwa funkcjonujące pojęcia:

- wykonywanie kopii zapasowych danych (*ang. backup copy*) umożliwiające przywrócenie działania systemu po awarii (*ang. disaster recovery*). Kopia zawiera oprócz danych także informacje umożliwiające przywrócenie działania systemu. Kopie zapasowe wykonywane są najczęściej (ze względu na koszty) na nośnikach wielokrotnego zapisu;
- archiwizacja danych (*ang. archiving*) mająca na celu utrwalenie danych, które nie muszą być dalej modyfikowane. Archiwizację przeprowadza się na nośnikach tańszych niż twarde dyski: np. na płytach czy taśmach. Przy wyborze nośnika należy wziąć pod uwagę jego czas życia i sposób przechowywania. Nośniki archiwum często przechowywane są w innych miejscach - np. w skrytkach bankowych. Archiwum udostępniane jest w trybie tylko do odczytu.

Należy zwrócić uwagę, że awaria systemu komputerowego prawie zawsze wiąże się z utratą danych. Nie jest praktycznie możliwe zapewnienie 100% odzyskania danych. Dlatego też przy projektowaniu należy brać pod uwagę dwa wskaźniki:

RTO - *ang. Recovery Time Object* - wskaźnik mówiący jak długo będzie trwało odtwarzanie danych (np. bazy danych) do stanu sprzed awarii, jak długo zajmie przywrócenie funkcjonowania całego systemu oraz ile czasu zajmie ponowne wprowadzenie utraconych danych, które nie zostały zapisane na kopii.

RPO - *ang. Recovery Point Objective* - wskaźnik określający punkt czasu w przeszłości do jakiego będą odtwarzane dane. Wskaźnik ten określa ilość danych jakie zostaną utracone.

Wskaźniki RTO i RPO należy uwzględnić na etapie tworzenia strategii backup'u. Profesjonale wdrożenie systemu backup'u w dużej firmie przebiega wieloetapowa i składa się z wielu kroków:

- Przeprowadzenie analizy potrzeb i możliwości w zakresie systemu backup'u;
- Zaprojektowanie systemu backup'u;
- Wykonanie niezbędnych testów przedwdrożeniowych;
- Wprowadzenie procedur ochrony danych;
- Uruchomienie strategii backup'u i odtwarzania danych;
- Przeszkolenie personelu;
- Uruchomienie systemu.

Z punktu wykonywania kopii stosuje się trzy podstawowe podejścia:

backup pełny - na nośniku archiwizowane są wszystkie dane, bez względu kiedy ostatnio były archiwizowane. Dane mogą być archiwizowane na jednym nośniku lub wielu nośnikach. Wadą jest długi czas archiwizacji.

backup różnicowy - *ang. differential backup* - archiwizacja tylko te dane, które uległy zmianie od ostatniej pełnej archiwizacji. Ilość danych i czas archiwizacji rośnie w z upływem czasu.

backup przyrostowy - archiwizowane są tylko nowe i zmodyfikowane od ostatniej archiwizacji pliki. Jest to najszybsza metoda archiwizacji i najwolniejsza w przypadku konieczności odtworzenia danych. Wymaga wielu nośników.

7.2.1 Schematy rotacji nośników

Schemat GFS Schemat GFS (*ang. Grandfather-Father-Son* - Dziadek-Ojciec-Syn) jest najpopularniejszym algorytmem rotacji nośników. Dobrze sprawdza się w archiwizacji na różnych nośnikach, ale przede wszystkim na taśmach.

Schemat jest trójpoziomowy. Zakładając pięciodniowy tydzień pracy poszczególne poziomy wyglądają następująco:

- S - poziom Syn - w kolejnych czterech dniach tygodnia (poniedziałek, wtorek, środę, czwartek) zostaną wykonane kopie przyrostowe;
- F - poziom Ojciec - w każdy piątek wykonywana jest pełna kopia;
- G - poziom Dziadek - kopia pełna wykonywana jest na koniec każdego miesiąca i archiwizowana (przechowywane) poza miejscem, w którym znajdują się skopiowane dane (serwery).

Ostatecznie, do wykonania rocznego cyklu, potrzeba 21 kompletów nośników danych (nie zawsze wystarczy jedna płyta lub kaseta).

Istnieje także uproszczona wersja omawianego schematu, gdzie na poziomie F można posługiwać się dwoma nośnikami zapisywanymi zamiennie co 2 tygodnie. Wersja uproszczona wymaga posiadania jedynie 6 nośników.

Tab. 7.1: Schemat GFS.

	Pn	Wt	Sr	Cz	Pt	So	Nd	Pn	Wt	Sr	Cz	Pt	So	Nd	...	Mc
S	D	D	D	D				D	D	D	D				...	
F					F							F			...	
G															...	A

D-b. przyrostowy, F-b. pełny, A-b. pełny (archiwizacja)

Tab. 7.2: Ilustracja działania algorytmu rotacji Wieża Hanoi.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A		A		A		A		A		A		A		A	
	B				B				B				B		
			C								C				
							D								
															E

Wieża Hanoi Bardziej skomplikowanym schematem wykonywania kopii zapasowych jest wieża Hanoi. Jest trudniejsza do wdrożenia, lecz charakteryzuje się niższym kosztem przechowywania pełnej rocznej kopii w przypadku przechowywania danych w dłuższym okresie czasu. W poniższym przykładzie wymaga posiadania 5 nośników oznaczonych literami A, B, C. Kopie na nośniku A wykonywane są co drugi dzień, natomiast kopie na nośniku B wykonywane są co 4 dzień cyklu (począwszy od 2 dnia kiedy nie został użyty nośnik A). Kopie na nośniku C wykonywana są wtedy, gdy nie jest wykonywana kopia na nośniku A i B, czyli począwszy od czwartego dnia co 8 dni.

Do wykonywania kopii raz w tygodniu wymagane jest 5 nośników. Wykonywanie kopii codziennie wymaga 8 nośników. Więcej informacji na temat schematów rotacji nośników można znaleźć np. w www.centrum.bezpieczenstwa.pl/artykuly/BITSR_3_o_kopiach_zapasowych.pdf

7.2.2 Kopie zapasowe w chroot

W środowisku chroot możemy wykonywać również kopie zapasowe danych. Co więcej - o ile nie mamy fizycznych problemów np. z kartą sieciową możemy także skonfigurować połączenie z siecią i np. za pomocą programu *scp* przesyłać te dane na inny komputer. Polecenie , netcardconfig, wywołuje nam konfigurator sieci. Kiedy mamy już połączenie z inną maszyną (chociażby w sieci lokalnej), wykonujemy np.

```
tar zcvf /home/* | ssh 192.168.0.5 ,,cat > /root/kopia.tgz"
```

Polecenie utworzy archiwum katalogów domowych i prześle do katalogu /root/ na komputer o numerze 192.168.0.5.

Możemy wykonać także dokładną kopię całego dysku lub partycji:

```
cat /dev/dysk | gzip -c > kopia.dysk
```

Oczywiście żeby odzyskać taką kopię, musimy ją rozpakować na dysk (lub partycję) o identycznym rozmiarze:

```
gunzip -c kopia.dysk >/dev/dysk
```

Do wykonania kopii zapasowej możemy posłużyć się również programem cpio. Przykładowo po uruchomieniu płyty podmontowujemy sobie partycję, której kopię chcemy wykonać do katalogu /mnt/hda1, podmontowujemy także partycje na której ma się znaleźć archiwum (np. /mnt/hda2) i wykonujemy:

```
cd /mnt/hda1/
find . -mount -print | cpio -o > /mnt/hda2/kopia.cpio
```

Żeby odtworzyć powyższą kopię, należy wykonać:

```
cpio -i < /mnt/hda2/kopia.cpio
```

7.3 Konfiguracja przeglądarek internetowych

Z punktu widzenia bezpieczeństwa należy zwrócić uwagę na konfigurację przeglądarek internetowych, które są potencjalnym źródłem zagrożeń:

- uzupełnianie danych w formularzach, w tym zapamiętywanie loginów i haseł logowania do serwisów np. bankowych.
- zapamiętywanie historii przeglądanych stron WWW,
- akceptowanie plików cookie,
- wykorzystanie skryptów oraz technologii: VBScript, Java lub ASP.

Na rynku dostępnych jest kilka najczęściej używanych przeglądarek, które oferują różny poziom bezpieczeństwa:

- Internet Explorer
- Mozilla/FireFox
- Chrome
- Opera

W lipcu 2014 roku udział w rynku poszczególnych przeglądarek wynosił:

1. Mozilla/FireFox v31 $(34,10\%)$,
2. Chrome v36 (34.05%),
3. Internet Explorer v11 (12.51%),
4. Opera]23 (6.05%).

Szczegółowe porównanie przeglądarek można znaleźć w internecie, np. http://www.purepc.pl/oprogramowanie/ Z punktu bezpieczeństwa najgorszą przeglądarką jest Internet Explorer.

7.3.1 Mozilla/FireFox

Na rys. 7.1 przedstawiono zrzuty ekranów okien konfiguracji przeglądarki Mozilla FireFox. Konfiguracja dotyczy:

- blokady wyskakujących okienek - rys. 7.1a,
- historii przeglądania i śledzenia użytkownika przeglądarki - rys. 7.1b,
- uzupełniania i zapamiętywania danych w formularzach oraz zapamiętywania nazw użytkowników i haseł, automatycznego instalowania dodatków, blokowanie niebezpiecznych witryn - rys. 7.1c,
- wyłączenie tzw. telemetrii, czyli przekazywania firmie informacji o sprzęcie i konfiguracji przeglądarki - rys. 7.1d,
- użycia miejsca na dysku na pliki tymczasowe (najczęściej wystarcza ograniczenie do $20MB$, co dodatkowo podnosi efektywność przeglądarki oraz przechowywania danych w trybie offline (bez połączenia z siecią) - rys. 7.1e,
- sprawdzania i instalowania aktualizacji - rys. 7.1f,
- sposobu uwierzytelnienia użytkownika przy pomocy certyfikatu użytkownika oraz sprawdzania ważności certyfikatów - rys. 7.1g.

7.3.2 Chrome

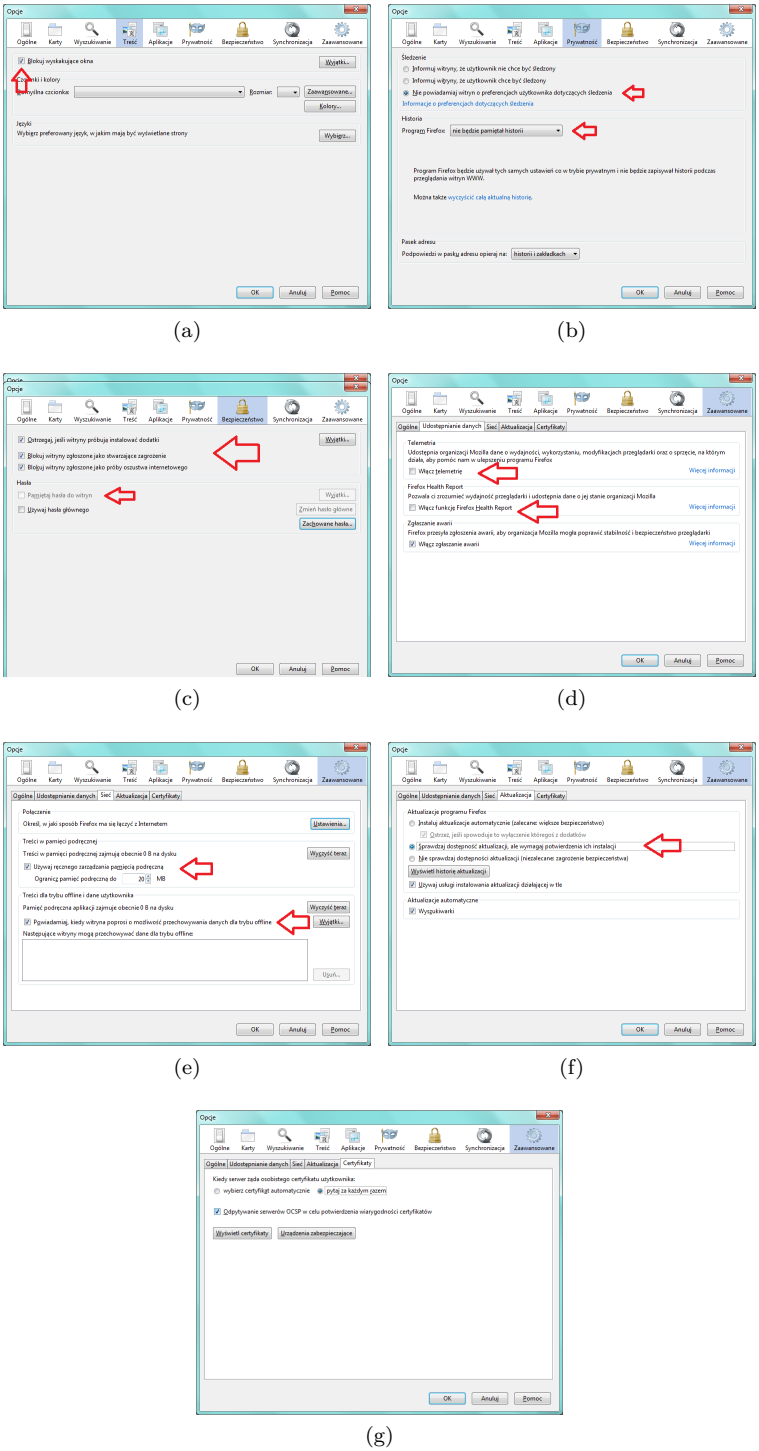
Na rys. 7.2 przedstawiono zrzuty ekranów okien konfiguracji przeglądarki Chrome. Konfiguracja obejmuje:

- uzupełniania i zapamiętywania danych w formularzach oraz zapamiętywania nazw użytkowników i haseł, blokowanie niebezpiecznych witryn (pishing), śledzenia użytkownika - rys. 7.2a,
- blokowania plików cookie - rys. 7.2b,
- zapisywania pobieranych z sieci plików - rys. 7.2c.

7.3.3 Internet Explorer

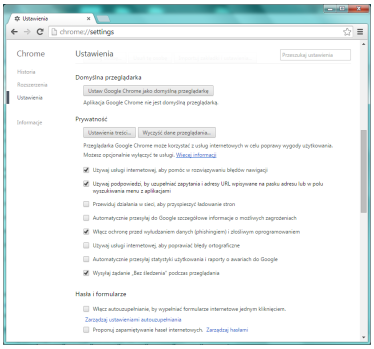
Na rys. 7.3 przedstawiono zrzuty ekranów okien konfiguracji przeglądarki IE. Konfiguracja dotyczy:

- historii przeglądania i sprawdzania wersji strony internetowej (za każdym razem) oraz użycia miejsca na dysku na pliki tymczasowe (najczęściej wystarcza ograniczenie do $20MB$, co dodatkowo podnosi efektywność przeglądarki - rys. 7.3a,
- blokady wyskakujących okienek oraz obsługi plików cookie - - rys. 7.3b,
- uzupełniania i zapamiętywania danych w formularzach oraz zapamiętywania nazw użytkowników i haseł w formularzach - rys. 7.3c.

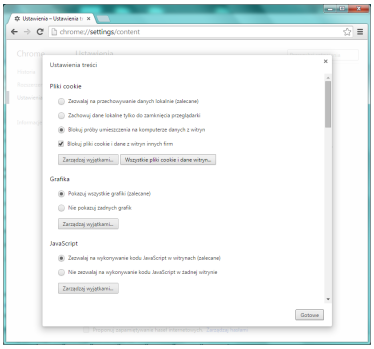


(a) (b) (c) (d) (e) (f) (g)

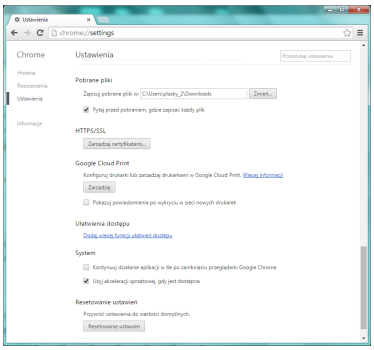
Rys. 7.1: Konfiguracja przeglądarki Mozilla FireFox.



(a)

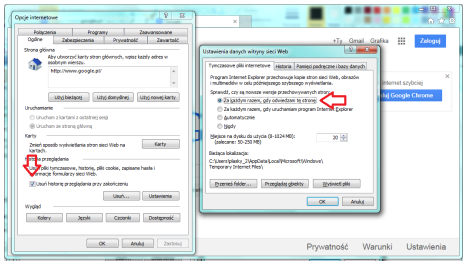


(b)

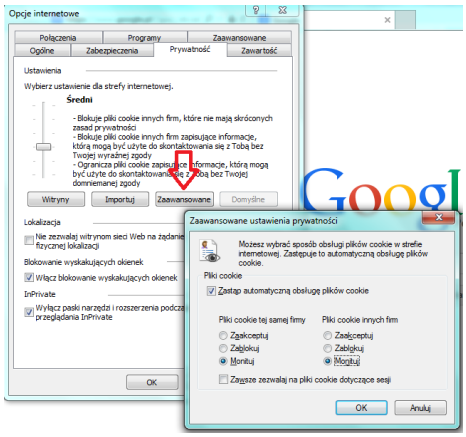


(c)

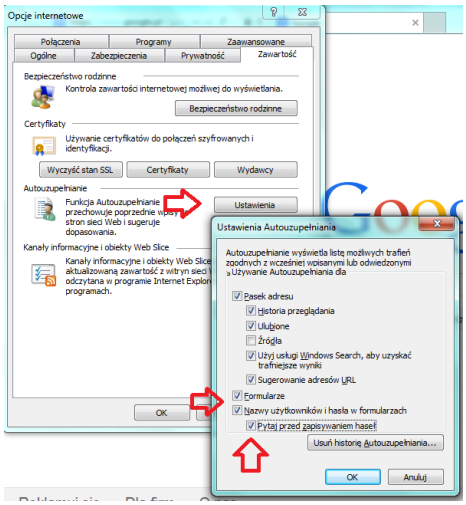
Rys. 7.2: Konfiguracja przeglądarki Chrome.



(a)



(b)



(c)

Rys. 7.3: Konfiguracja przeglądarki Internet Explorer.

Rozdział 8

Kryptografia

Podstawowym pojęciem używanym w kryptografii jest pojęcia algorytmu kryptograficznego zwanego także szyfrem - definicja 8.1

Definicja 8.1. *Algorytm kryptograficzny szyfrujący (szyfr) to funkcja matematyczna, która przekształca informację jawną w informację niezrozumiałą dla człowieka (zaszyfrowaną).*

Definicja 8.2. *Kryptograficzny algorytm deszyfrujący to funkcja matematyczna, która przekształca informację wcześniej zaszyfrowaną w informację jawną (pierwotną).*

Najczęściej do szyfrowania i deszyfrowania używana jest inna funkcja matematyczna. Informacja przed zaszyfrowaniem zwana jest potocznie *tekstem jawnym*, a po zaszyfrowaniu nazywana jest *szyfrogramem*. Proces zamiany informacji jawnej do postaci zaszyfrowanej nazywany jest szyfrowaniem. Historycznie kryptografia dzieli się na kryptografię:

- z kluczem lub kluczami symetrycznymi,
- z kluczem lub parami kluczy asymetrycznych.

Klucz szyfrujący w literaturze nazywane jest sekretem. Podstawowymi usługami ochrony informacji są:

- poufność (*ang. confidentiality*), która ma za zadanie zapewnić nieujawnienie i nieudostępnienie informacji osobom lub innym nieuprawnionym podmiotom. Poufność realizowana jest zwykle przy pomocy szyfrowania oraz kontroli dostępu. Poufność może być także zapewiona przez środki proceduralne i techniczne, takie jak kancelaria tajna.
- niezaprzeczalność (*ang. non-repudiation*), czyli brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie. Niezaprzeczalność jest bardzo ważna np. przy składaniu podpisu elektronicznego.
- integralność informacji/danych (*ang. data integrity*), czyli zapewnienie aby dane nie zostały zmienione (dodane, usunięte) w nieautoryzowany sposób,

Metody realizacji wymienionych usług zostaną omówione w dalszej części pracy.

8.1 Historia

Utajnianie lub ukrywanie informacji jest związane historią człowieka, głównie w okresach konfliktów. Na przestrzeni wieków stosowano różne metody utajniania informacji. Kryptografia była znana już za czasów Cesarstwa Rzymskiego. Wiadomości były już wtedy szyfrowane. Stosowane wtedy metody wydają się dzisiaj bardzo proste i banalne, jednak w swoich czasach spełniały dobrze swą funkcję. Polegał on na zastąpieniu każdej litery w tekście jawnym literą znajdującą się o pewną liczbę pozycji dalej w alfabecie.

W wieku XVII kryptografia pojawiła się w zastosowaniach wojskowych i była używana aż do wieku XX. Były to jednak proste szyfry podstawieniowo - przestawieniowe. Problem był w tym, że ujawnienie metody szyfrowania czyniło ją niezdatną do użytku. Tak jak to było w przypadku Enigmy, wystarczyło zbudować kopię, by złamać niemieckie szyfry. Zatem brak informacji o historycznych systemach kryptograficznych wyjaśnia fakt konieczności całkowitego utajniania używanych metod szyfrowania.

Powszechne były też metody steganofraficzne, takie jak zaznaczanie liter, pisanie niewidzialnym atramentem, czy nakłuwanie szpilką liter.

Następnie powstawały kolejne coraz bardziej skomplikowane szyfry. Rozwój kryptografii symetrycznej postępował dosyć szybko. Powstały szyfry jedno- i wieloalfabetowe, szyfrowanie wieloliterowe, techniki transpozycyjne-omówione, ale nie były to jedyne metody utajniania informacji. Bardzo powszechne były maszyny rotorowe, jak wspomniana już wcześniej Enigma, ale również Purple używana przez Japonię.

W latach 60 IBM zaczął prace nad projektem kryptograficznym zakończone utworzeniem algorytmu Lucifer. Następnie na zapotrzebowanie Narodowego Biura Standardów w 1973r. Został udoskonalony algorytm Lucifer i w 1977r. zatwierdzono standard szyfrowani danych DES, jednakże ze zmniejszonym rozmiarem klucza.

Algorytmem, który miał zastąpić DES jest IDEA. Jest to blokowy szyfr konwencjonalny, stosujący 128-bitowy klucz do szyfrowania w blokach po 64 bity. Wchodzi między innymi w skład PGP (Pretty Good Privacy), którego autorem jest Phil Zimmermann. Umożliwia zapewnienie poufności i uwierzytelnianie. Czyli nadaje się do stosowania w poczcie elektronicznej i przy przechowywaniu plików.

Postęp w kryptografii nastąpił w 1976 roku. Diffie i Hellman przedstawili nowy algorytm szyfrowania danych oparty na kluczach publicznych (parze kluczy, z których jeden był publicznie dostępny - jawny). Dawało to możliwość zaszyfrowania informacji przez dowolna osobę za pomocą klucza jawnego, natomiast odszyfrować mogła ją tylko osoba mająca swój klucz prywatny, związany z kluczem jawnym. Wyeliminowano potrzebę komunikacji się użytkowników celem wymiany klucza.

Powstały takie algorytmy jak MD4 stworzony przez Rona Rivesta w 1990 roku, a poprawiony dwa lata później, w którym to roku powstał też algorytm MD5 tego samego autora. Kolejnym algorytmem był SHA utworzony w 1993r. przez Narodowy Instytut Standardów i Technologii USA. Jest oparty na MD5, a jego budowa jest podobna do MD4.

2 stycznia 1997r. NIST ogłosił poszukiwania nowego standardu szyfrowania danych AES (*ang. Advanced Encryption Standard*), określając minimalne wymogi następująco:

- dokumentacja szyfru musi być powszechnie dostępna
- szyfr ma należeć do grupy blokowych szyfrów symetrycznych
- projekt szyfru musi zakładać możliwość rozszerzenia długości klucza w razie takiej potrzeby
- szyfr musi być łatwy do implementacji zarówno sprzętowej jak i programowej
- nowy szyfr ma być bardziej efektywny oraz bardziej bezpieczny niż 3-DES, czyli: długość klucza to 128, 192 lub 256 bitów, a wielkość bloku: 128, 192 lub 256 bitów.

Spośród wszystkich projektów, najlepszą ocenę uzyskał Rijndael i został wybrany nowym standardem szyfrowania danych (AES). Obie nazwy są obowiązujące. Rijndael jest blokowym szyfrem konwencjonalnym, pracującym na blokach o długości 128, 192 oraz 256 bitów. Dozwolone są również długości 160 oraz 224 bity, ale nie są one uznawane jako standard. Identycznej długości mogą być klucze.

Kryptografia jest dziedziną, która stale się rozwija, ze względu na ciągły wzrost mocy obliczeniowej systemów komputerowych i opracowywanie nowych meto łamania szyfrów. Oznacza to konieczność poszukiwania nowych bądź udoskonalania już istniejących sposobów ochrony danych.

8.1.1 Historyczne szyfry w Europie

Scytale Metoda szyfrowania wykorzystywana w starożytnej Grecji, w Sparcie w V w. p.n.e. Szyfrowanie polegało na zapisaniu tekstu na nawiniętym na walec (laskę) pasku pergaminu lub skóry. Po rozwinięciu pasek zawierał on ciąg nic nieznaczących liter. Odczytanie (odszyfrowanie) było możliwe po ponownym nawinięciu paska na walec (laskę) o takiej samej grubości - rys. 8.1). Walec posiadali np. dowódcy. Pasek skóry z zapisanym tekstem był zawiązywany przez posłańca wokół pasa literami do wewnątrz.

Źródło: https://pl.wikipedia.org/wiki/Skytale#/media/File:Skytale.png

Rys. 8.1: Scytale.

Szyfr Cezara Szyfr Cezara to z jedna z najprostszych technik szyfrowania. Szyfrowanie polega zastąpieniu danej litery w alfabecie inną literą przesuniętą w alfabecie o stałą liczbę pozycji w konkretnym kierunku. Z tego powodu szyfr ten nazywany jest *szyfrem przesuwającym* lub *przesunięciem Cezariańskim*. Jest

to szyfr podstawieniowy monoalfabetyczny. Nie rozróżnia się dużych i małych liter. Nazwa szyfru pochodzi od Juliusza Cezara, który prawdopodobnie używał tego szyfru do wymiany informacji z przyjaciółmi. Używał przesunięcia o 3 miejsca. Obecnie używa się szyfru Cezara z przesunięciem 13. Odpowiedni algorytm nazywa się ROT-13.

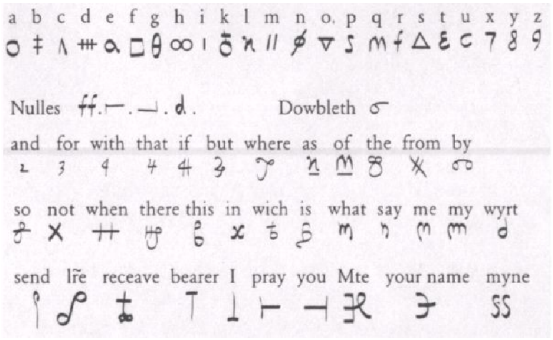
Złamanie szyfru jest obecnie bardzo proste np. przez analizę rozkładu występowania liter w alfabecie. Analizując rozkład dla długiego tekstu i znając język (niekoniecznie), w którym zapisany jest tekst można łatwo wyznaczyć zastosowane przesunięcie.

Szyfr AtBash Szyfr AtBash jest prostym monoalfabetycznym szyfrem podstawieniowym pochodzenia hebrajskiego. Pojawił się prawdopodobnie około 500 r p.n.e. na bliskim wschodzie. Używany przez habrajczyków. Szyfrowanie polega na na przyporządkowaniu literze znaku, który leży w takiej samej odległości od końca, np. *a* na *z*, *f* na *u* (6 od końca). W celu ułatwienia posługiwania się można wyznaczyć tablice kodową.

Szyfr Marii Stuart Szyfr wykorzystywany od początku XV wieku do połowy XIX wieku (wzorowany na sposobie szyfrowania z końca XIV wieku opracowanego przez Gabrielego di Lavinde). Podstawowym składnikiem był szyfr podstawieniowy, który przyporządkowywał literze inną literą oraz tablica kodowa, która przypisywała przyporządkowanej literze kod (nomenklator): sylabę, słowo, cały zwrot i odpowiadających im zamienników - liczb kilkucyfrowych lub zestawów kilku losowo wybranych liter. Dzięki zastosowania stosowanych sylab, słów i zwrotów, w tekście zaszyfrowanym zacierała się struktura szyfrowanego tekstu jawnego.

Początkowo nomenklatory (rys. 8.2) były tworzone w postaci zapisu równoległego w postaci list liter (sylab, słów) i list ich zamienników. Ze względu na uproszczenie odczytywania nomenklatory były ułożone w porządku alfabetycznym lub numerycznym, co było wielką słabością systemu. Wadę tą usunęły tzw. nomenklatory dwuczęściowe złożone z dwóch list:

- ułożonej alfabetycznie listy liter (sylab, słów, zdań) i ich zamienników przypisanych losowo, - listy zamienników - ułożonej alfabetycznie lub numerycznie - i odpowiadających im składników tekstu jawnego.



Rys. 8.2: Nomenklator Marii Stuart.

Podstawową wad szyfru była konieczność zmiany wszystkich list (we wszystkich miejscach gdzie były stosowane) w przypadku, gdy przeciwnik zdobył choćby jeden egzemplarza nomenklatora. Wyprodukowanie i bezpieczna dystrybucja list było w owych czasach dużym problemem logistycznym.

Szyfr ten był zbyt skomplikowany (zbyt dużo znaków) dla systemów telegraficznych wprowadzonych w XIX wieku.

Szyfr Vigenere Jeden z pierwszych szyfrów poli-alfabetycznych szyfrów podstawieniowych. Szyfr błędnie przypisany Blaise'owi de Vigenere, twórcy bardziej zaawansowanego szyfru. Szyfr ten po raz pierwszy został opisany przez Giovana Batista Belaso w 1553 roku.

Działanie szyfru wykorzystuje tablice przedstawioną na rys. 8.3. Tablica zawiera 26 liter (26 kolumn). Kolejne wiersze zaczynają się od kolejnej litery alfabetu (są przesunięte o 1) - 26 wierszy. W tym przypadku było ich aż 26. Każdy kolejny wiersz można traktować jak nowy alfabet. Do zaszyfrowania tekstu potrzebne jest tajne słowo kluczowe. W przypadku, gdy słowo kluczowe jest krótsze niż szyfrowany tekst, należy użyć wielokrotności słowa kluczowego.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

Rys. 8.3: Tablica Vigenere.

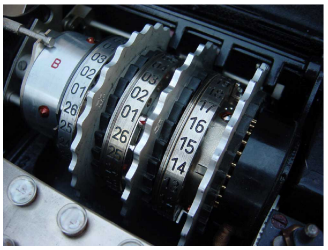
Szyfrowanie przebiega następująco. Litera tekstu zaszyfrowanego (szyfrogramu) jest literą z tabeli znajdującą się na przecięciu wiersza, wyznaczanego

przez literę tekstu jawnego i kolumny wyznaczanej przez literę słowa kluczowego. Np. słowo kluczowe: BELA, szyfrujemy tekst ALA. Po zaszyfrowaniu otrzymamy: BPL. Deszyfrowanie odbywa się w odwrotnej kolejności.

8.1.2 Maszyna szyfrująca Enigma

Pierwszym urządzeniem kryptograficznym, które odniosło duży sukces na rynku była maszyna szyfrująca Enigma, opracowana przez niemieckiego inżyniera Artura Scherbiusa. W czasie drugiej wojny światowej używana była przez siły zbrojne, produkowana była w różnych wersjach, z różną liczbą wirników (od 3 do 8).

(a) Lewa strona wirnika



(b) Ułożenie wirników

(c) Enigma II 8-wirnikowa

(d) Enigma z modułem drukującym

Rys. 8.4: Maszyna szyfrująca Enigma.

Enigma posiadała klawiaturę, taką jak maszyna do pisania, ale zamiast jednego zbioru liter (czcionek), posiadała trzy zbiory (a potem więcej) liter, rozmieszczonych na bębenkach. Naciśnięcie klawisza z literą, np. *a*, uruchamiało na pierwszym bębenku literę odmienną do *a*, tej z kolei odpowiadała inna litera na drugim bębenku i jeszcze inna na trzecim bębenku. Po każdym naciśnięciu kla-

wisza bębenki obracały się i po ponownym naciśnięciu klawisza *a* odpowiadała mu już inna kombinacja liter na bębenkach.

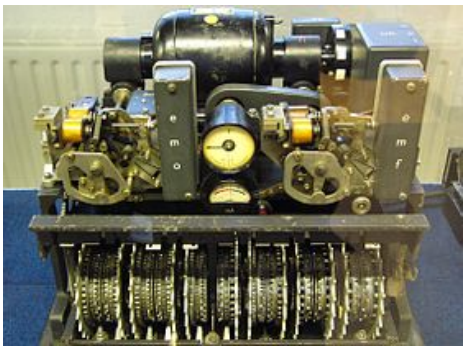
Polscy kryptolodzy słusznie domyślali się, że Niemcy zastosowali maszyny szyfrujące, odkąd nieczytelne okazały się dla nich depesze Kriegsmarine oraz korespondencja Wehrmachtu. Na zwróceniu uwagi na Enigmę dopomógł im przypadek. W 1928 roku wywiad wojskowy został powiadomiony przez Urząd Celny o przesyłce z Niemiec, której zwrotu, jako nadanej omyłkowo, natarczywie żądał, koniecznie przed dokonaniem odprawy celnej, nadawca. W przesyłce miał być sprzęt radiowy, lecz po jej otwarciu ukazała się maszyna szyfrująca.

Schemat okablowania Enigmy wskazujący przepływ prądu podczas naciskania litery 'A', która kodowana jest jako 'D'. Litera 'D' daje także 'A' w wyniku, ale 'A' nigdy nie jest 'A'.

Dobrze opracowany serwis poświęcony Enigmie znajduję się na Wikipedii.

8.1.3 Maszyna szyfrująca Lorenza

Kolejnym niemieckim urządzeniem szyfrującym, również używanym podczas drugiej wojny światowej była Maszyna Lorenza - rys. 8.5. Podobnie jak Enigma korzystała z wirników, ale działała na innych zasadach. Ówczesne dalekopisy nadawały każdą literę zaszyfrowaną kodem Baudot albo podobnym, jako pięć bitów na pięciu równoległych liniach. Maszyna Lorenza produkowała grupę pięciu bitów pseudolosowych i kombinowała ją za pomocą logicznego operatora XOR z bitami litery tekstu jawnego. Bity pseudolosowe były generowane przez 10 *kół kryptograficznych* (rotorów), z których pięć obracało się w sposób regularny (tzw. koła (chi)) a pięć pozostałych w sposób nieregularny (koła (psi)). Krok obrotu kół psi zależał od jeszcze dwóch dodatkowych rotorów, zwanych motorycznymi (napędowymi). Maszyna Lorenza w swej funkcji nieregularnego obracania pięciu rotorów (które albo razem się obracały albo razem pozostawały w spoczynku bez dodatkowych interakcji między liniami) stanowi w praktyce 5 równoległych generatorów pseudolosowych. Liczby igieł na każdym z rotorów były względnie pierwsze.



Rys. 8.5: Maszyna szyfrująca Lorenza.

8.1.4 Wykorzystanie szyfrantów indiańskich

Indiańscy szyfranci (*ang. codetalkers*) - specjalnie przeszkoleni amerykańscy żołnierze, głównie z okresu II wojny światowej, pochodzący z indiańskich plemion i posługujący się zakodowanymi słowami z mało znanych indiańskich języków w celu przekazywania zaszyfrowanych informacji i rozkazów. W czasie II wojny światowej największą grupę indiańskich szyfrantów stanowili Indianie Nawaho (*ang. Navajo*), których ponad 400 przeszło specjalne tajne szkolenie w tym zakresie. Działali głównie na Pacyfiku. Kierowali atakami amerykańskiego lotnictwa, ruchami wojsk, donosili o stanowiskach nieprzyjaciela i przekazywali inne poufne informacje i rozkazów. Dzięki nim przeprowadzono atak na wyspę Iwo Jima.

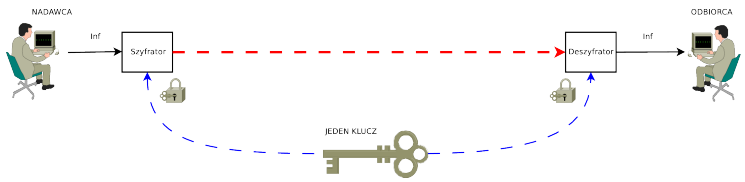
Problemem wykorzystania języka Indian było opracowanie za pomocą określeń przyrodniczych określonych miejsc i rzeczy. Np. określenie *besh-lo - żelazna ryba* znaczyło *okręt podwodny*. Za pomocą słów kodowano także litery, z których składały się wojskowe określenia, nieistniejące w języku Indian. Ze względu na swoją specyfikę żaden z kodów opartych na językach tubylczych Amerykanów nigdy nie został złamany,

8.1.5 Kryptografia asymetryczna

Kryptografia asymetryczna została oficjalnie wynaleziona przez cywilnych badaczy Martina Hellmana, Whitfielda Diffie w 1976 roku. Prawie równolegle prototyp podobnego systemu stworzył Ralph Merkle. W 1974 roku zaproponował algorytm wymiany kluczy, nazwany puzzlami Merkle'a. Dopiero pod koniec XX wieku brytyjska służba wywiadu elektronicznego GCHQ (*ang. Government Communications Headquarters* - Centrala Łączności Rządowej) ujawniła, że pierwsza koncepcja systemu szyfrowania z kluczem publicznym została opracowana przez jej pracownika Jamesa Ellisa ż w 1965 roku, a działający system został stworzył w 1973 roku Clifford Cocks (także pracownik GCHQ). Prace ty były objęte klauzulą tajności do 1997 roku. Obecnie kryptografia asymetryczna jest szeroko stosowana do wymiany informacji poprzez kanały o niskiej poufności jak np. Internet. Stosowana jest także w systemach elektronicznego uwierzytelniania, obsługi podpisów cyfrowych, do szyfrowania poczty (OpenPGP) itd.

8.2 Kryptografia symetryczna

Cechą charakterystyczną kryptografii z kluczem symetrycznym jest wykorzystanie jednego (wspólnego) klucza (sekretu) do szyfrowania i deszyfrowania informacji - rys. 8.6.



Rys. 8.6: Szyfrowanie w systemach symetrycznych.

Algorytm z kluczem symetrycznym znany jest pod różnymi nazwami:

- algorytm konwencjonalny,
- algorytm z kluczem tajnym,
- algorytm z pojedynczym kluczem,
- algorytm z jednym kluczem.

Istnieje także możliwość wykorzystania pary kluczy do szyfrowania/deszyfrowania. Jeden klucz służy do szyfrowania, a drugi do deszyfrowania informacji. Na podstawie jednego z kluczy można odtworzyć drugi klucz, tzn. z klucza szyfrującego można odtworzyć klucz deszyfrujący i odwrotnie. Oznacza to, że utrata jednego z kluczy umożliwia odszyfrowanie zaszyfrowanej wiadomości[12].

Głównym problemem związanym z użyciem kryptosystemów symetrycznych jest konieczność wcześniejszego (poprzedzającego transmisję wiadomości) uzgodnienia klucza pomiędzy każdą parą potencjalnych korespondentów. Ze względu na to, że klucz ma być znany tylko danej parze nadawca-odbiorca, więc jego uzgodnienie musi odbywać się przy użyciu specjalnego, bezpiecznego kanału łączności (np. przy użyciu kuriera). Stwarza to ogromne problemy, zwłaszcza w dużych sieciach, gdyż liczba koniecznych do uzgodnienia (LWK) kluczy rośnie proporcjonalnie do kwadratu liczby użytkowników sieci[1]*. Dodatkowo sprawę komplikuje fakt, że ze względów bezpieczeństwa klucze te powinny być możliwie często zmieniane.*

Algorytmy symetryczne wykorzystywane są do szyfrowania:

- strumieni danych (algorytmy strumieniowe), np. bit po bicie - zwane także potokowymi; algorytmy te przetwarzają wiadomość po jednym bicie,
- bloków danych (algorytmy blokowe).

Algorytmy symetryczne są najstarszymi znanymi algorytmami szyfrującymi (rozdział 8.1).

8.3 Kryptografia asymetryczna

Drugim rodzajem kryptografii jest kryptografia z kluczem asymetrycznym. Powszechnie znana jest pod nazwą *kryptografii klucza publicznego*. System wykorzystujący ten rodzaj kryptografii nazywany jest *Infrastrukturą Klucza Publicznego - ang. Public Key Infrastructure* (PKI).

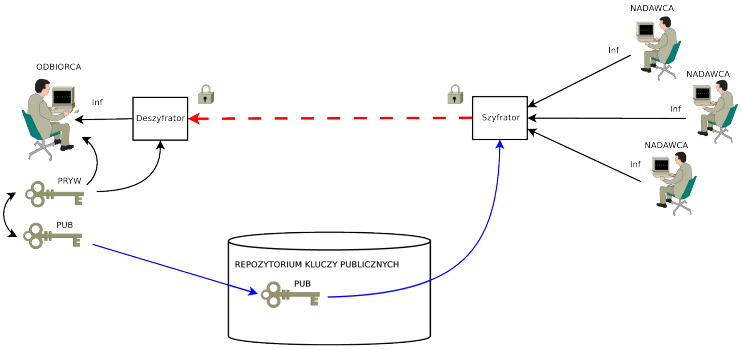
W kryptografii tej wykorzystywane są najczęściej pary kluczy (tzw. klucze komplementarne) umożliwiające wykonywanie różnych operacji kryptograficznych. Jeden z pary kluczy należy udostępnić (klucz publiczny), a drugi należy chronić (klucz prywatny). W niektórych zastosowaniach wykorzystuje się większą liczbę kluczy. Z punktu widzenia bezpieczeństwa informacji, należy używać takich algorytmów szyfrujących, które zapewniają:

- poufność,

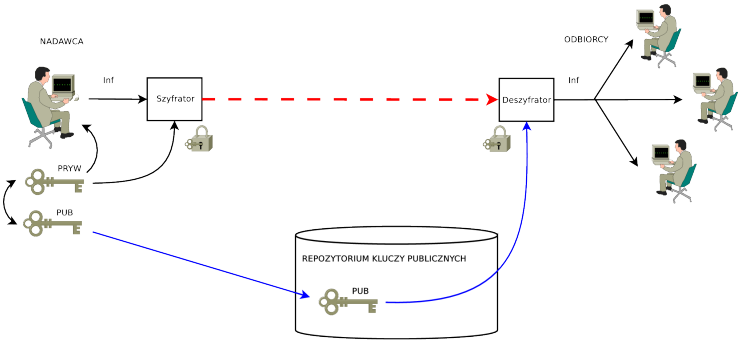
[1] $LWK = N(N-1)/2$, N - liczba użytkowników. Np. dla $N = 100$ liczba koniecznych wymian kluczy $LWK = 4500$.

- niezaprzeczalność,
- integralność informacji.

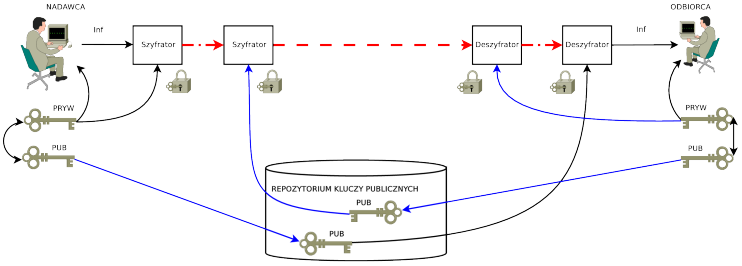
Wymienione wyżej usługi można zrealizować w systemach asymetrycznych. Sposób realizacji został przedstawiony poglądowo na rys. 8.7.



(a) poufność



(b) niezaprzeczalność



(c) niezaprzeczalność i poufność

Rys. 8.7: Realizacja podstawowych usług ochrony informacji w systemach asymetrycznych.

8.4 Cechy systemów kryptograficznych

W tab. 8.1 zamieszczono zestawienie cech systemów symetrycznych i asymetrycznych pod kątem przydatności do realizacji usług ochrony informacji oraz z punktu widzenia dystrybucji kluczy, niezbędnej do realizacji wszystkich usług. Wyróżniono grupy, które najlepiej nadają się do realizacji danej usługi. Własności obu grup i ich widoczna komplementarność skłaniają do zastosowania w praktycznych systemach obu typów przekształceń kryptograficznych, w taki sposób by najlepiej wykorzystać cechy każdego z nich. Główną zaletą systemów symetrycznych jest duża szybkość przetwarzania informacji, kilkaset razy większa niż szybkość przetwarzania informacji przy użyciu analogicznych implementacji kryptosystemów asymetrycznych. Ze względu na duże różnice w szybkości kryptosystemy takie jak DES, potrójny 3DES lub IDEA wykorzystywane są do szyfrowania i odszyfrowywania właściwych wiadomości, a kryptosystemy takie jak RSA jedynie do utajniania i uwierzytelniania kluczy dla kryptosystemów symetrycznych. Ponadto kryptosystemy asymetryczne są wykorzystywane do generowania i weryfikowania podpisów cyfrowych związanych z wiadomościami, a tym samym do realizacji usługi niezaprzeczalności.

Tab. 8.1: Zestawienie cech systemów symetrycznych i asymetrycznych.

Usługi i wymiana kluczy	symetryczne (DES, 3DES, IDEA)	asymetryczne (RSA)
poufność	**duże szybkości szyfrowania i deszyfrowania**	małe szybkości szyfrowania i deszyfrowania
integralność i uwierzytelnienie	**duże szybkości generowania i weryfikowania znacznika uwierzytelnienia MAC**	wolniejsze generowanie i weryfikowanie podpisu cyfrowego
niezaprzeczalność	trudność generowania podpisu cyfrowego	**łatwość generowania podpisu elektronicznego**
wymiana kluczy	trudna w realizacji	**łatwa w realizacji**

8.4.1 Metody realizacji usług ochrony informacji

Każda z usług chroniących przed zmodyfikowaniem lub sfałszowaniem przesyłanej wiadomości czyli przed tzw. podsłuchem aktywnym polega na dołączeniu do transmitowanej w niezmienionej postaci wiadomości pewnego ciągu bitów. Ciąg ten, będący zawsze funkcją wiadomości, otrzymywany jest w różny sposób, ma różne długości i różne nazwy dla każdej z trzech podstawowych usług: integralności, uwierzytelnienia, niezaprzeczalności.

Integralność Dla usługi integralności ciąg bitów ten zwany jest silnym (lub kryptograficznym) skrótem wiadomości (*ang. message digest*). Używa się też nazw znacznik integralności wiadomości lub znacznik wykrywalności modyfikacji i ich angielskich akronimów MIC (*ang. Message Integrity Code*), MDC

(*ang. Modification Detection Code*). Znacznik ten jest otrzymywany jako rezultat działania tzw. silnej funkcji skrótu $h(M)$. Od funkcji tej wymaga się spełnienia następujących, niezwykle ostrych, wymagań:

- funkcja h jest określona dla wiadomości M o dowolnej długości;
- w wyniku przekształcenia h otrzymujemy skrót wiadomości $MDC = h(M)$ o ustalonej długości n_h bitów;
- skrót wiadomości $h(M)$ jest łatwy do obliczenia;
- jest obliczeniowo niemożliwe odtworzenie wiadomości M na podstawie znajomości jej skrótu $h(M)$;
- funkcja h jest wolna od kolizji, tzn. znając funkcję h jest obliczeniowo niemożliwe wygenerowanie takiej pary wiadomości (M, M'), dla której $M \neq M'$ i $h(M) = h(M')$.

Funkcja skrótu nie zależy od żadnego tajnego parametru i stąd jej wartość może być wyliczona przez każdego użytkownika sieci. Realizacja usługi integralności polega:

- po stronie nadawcy - na dołączeniu do wiadomości obliczonego na jej podstawie skrótu;
- po stronie odbiorcy - na porównaniu skrótów wyliczonych po stronie nadawczej i odbiorczej - MDC i MDC'.

Ze względu na własności silnej funkcji skrótu wykrywana jest w ten sposób zmiana choćby jednego bitu przesyłanej wiadomości. Realizowana w opisany powyżej sposób usługa integralności nie zapewnia żadnego zabezpieczenia przed możliwością podszycia się przez intruza pod innego użytkownika sieci. Każdy z użytkowników sieci (a więc w szczególności intruz) może wygenerować skrót do utworzonej przez siebie fałszywej wiadomości, w której przedstawi się on jako ktoś zupełnie inny. Dlatego, usługa integralności nie jest nigdy realizowana samodzielnie, lecz zawsze jako część składowa usług uwierzytelnienia i niezaprzeczalności. Usługa uwierzytelnienia polega na dołączeniu do wiadomości ciągu bitów zwanego znacznikiem uwierzytelnienia wiadomości (*ang. Message Authentication Code*). MAC jest obliczany jako funkcja wiadomości oraz tajnego klucza znanego tylko nadawcy i odbiorcy. Tylko nadawca i odbiorca są w stanie obliczyć prawidłową wartość znacznika, odpowiadającą danej wiadomości. Weryfikacja autentyczności wiadomości polega na obliczeniu przez odbiorcę znacznika uwierzytelnienia jako funkcji wiadomości odebranej M' i porównaniu znaczników wyliczonych po stronie nadawczej i odbiorczej. Niezgodność tych znaczników świadczy o tym, że albo wiadomość, albo dołączony do niej znacznik zostały zmienione w czasie transmisji.

Niezaprzeczalność Realizacja niezaprzeczalności polega po stronie nadawczej na dołączeniu do wiadomości obliczonego na jej podstawie podpisu cyfrowego i weryfikacji tego podpisu po stronie odbiorczej. Najczęściej obecnie stosowane metody generowania podpisu obejmują trzy fazy:

1. obliczenie silnego skrótu wiadomości - MDC;

2. rozszerzenie MDC do postaci EMDC o długości równej długości bloku wejściowego asymetrycznego przekształcenia szyfrującego;

3. zaszyfrowanie rozszerzonego skrótu EMDC przy użyciu przekształcenia szyfrującego wyznaczonego przez klucz prywatny nadawcy.

Skrót wiadomości $h(M)$ otrzymywany jest w wyniku przekształcenia wiadomości przy użyciu funkcji skrótu h.

Użycie funkcji skrótu pozwala podpisywać sam skrót wiadomości $MDC = h(M)$, zamiast wiadomości, co znacznie poprawia wydajność algorytmów, zwłaszcza dla długich wiadomości M.

Opisanej powyżej metodzie generowania podpisu odpowiada następujący sposób jego weryfikacji:

1. na podstawie otrzymanej wiadomości M' jest obliczany silny skrót wiadomości MDC';

2. silny skrót z wiadomości odebranej jest rozszerzany do $EMDC'$ wg takiego samego algorytmu, jaki był używany po stronie nadawczej;

3. z podpisu dołączonego do wiadomości, jest odtwarzany (poprzez odszyfrowanie podpisu z użyciem klucza publicznego nadawcy) rozszerzony, silny skrót z wiadomości obliczony po stronie nadawczej ($EMDC$);

4. skróty wyliczane po stronie nadawczej $EMDC$ i odbiorczej $EMDC'$ są porównywane ze sobą. Jeżeli skróty są różne to może to świadczyć m.in. o tym, że:

   - wiadomość lub dołączony do niej podpis zostały zmienione w czasie transmisji lub

   - nadawca wiadomości nie jest tym za kogo się podaje.

Podpis cyfrowy związany z daną wiadomością, zapamiętany w osobnym pliku może służyć do późniejszego udowodnienia autorstwa wiadomości wobec osoby trzeciej - sędziego.

Weryfikacja przeprowadzana jest w sposób analogiczny do sprawdzania integralności i autentyczności wiadomości przez odbiorcę. Pozytywna weryfikacja wyklucza możliwość sfałszowania wiadomości przez kogokolwiek, wliczając w to odbiorcę wiadomości.

W celu wygenerowania podpisu $SGN(M)$ nadawca wykonuje następujące przekształcenia:

1. Oblicza skrót wiadomości $h(M)$ przy pomocy publicznie dostępnej funkcji skrótu h.

2. Oblicza podpis pod wiadomością szyfrując skrót wiadomości $h(M)$ przy użyciu przekształcenia RSA wyznaczonego przez klucz prywatny $SK = (d, N)$:

$$SGN(M) = h(M)^d (mod N)$$

W celu weryfikacji podpisu pod otrzymaną wiadomością odbiorca:

1. Oblicza skrót $h(M')$ z otrzymanej wiadomości M'.
2. Odszyfrowuje podpis $SGN(M)$ przy pomocy przekształcenia RSA wyznaczonego przez klucz publiczny nadawcy $PK = (e, N)$: $eSGN(M)(modN) = h(M)$.
3. Porównuje wartości $h(M)$ i $h(M')$. Jeśli $h(M) = h(M')$, wiadomość jest autentyczna.

8.4.2 Usługa poufności

Zapewnienie poufności informacji to najstarsze (i do niedawna jedyne) zadanie kryptografii. Współczesne rozwiązania tego problemu bazują na jednej z dwóch klas szyfrów: szyfrach blokowych lub szyfrach strumieniowych.

Szyfry blokowe dokonują jednoczesnej transformacji ustalonej porcji (bloku) znaków wiadomości wejściowej do postaci zaszyfrowanej. Długie wiadomości są wstępnie dzielone na fragmenty odpowiadające długości podstawowego bloku. W przypadku, gdy ostatni fragment (lub cała przesyłana wiadomość, jeżeli jest ona krótka) ma mniej znaków niż ustalona długość bloku dla danego szyfru, zachodzi konieczność uzupełnienia lub dopełnienia (*ang. padding*) wiadomości przed szyfrowaniem do długości będącej wielokrotnością długości podstawowego bloku. Istnieje kilka różnych metod dopełniania wiadomości, wszystkie jednak muszą pozwalać na jednoznaczne odróżnienie wiadomości od dopełnienia po stronie odbiorczej. W przypadku, gdy wiadomość generowana jest współbieżnie z procesem szyfrowania, urządzenie szyfrujące musi czekać aż wygenerowana zostanie liczba znaków odpowiadająca długości bloku. Dopiero wtedy odbywa się szyfrowanie i ewentualne przesłanie zaszyfrowanego bloku. Zasada działania szyfrów strumieniowych polega na zaszyfrowaniu każdego pojawiającego się na wejściu urządzenia szyfrującego znaku wiadomości poprzez połączenie go w pewien odwracalny sposób z wygenerowanym wewnątrz urządzenia znakiem klucza. Kolejne znaki wiadomości łączone są z kolejno generowanymi znakami klucza. W ten sposób szyfruje się *strumień* znaków wiadomości przy pomocy *strumienia* znaków klucza. Po stronie odbiorczej przychodzące, zaszyfrowane znaki poddawane są odwrotnemu przekształceniu przy użyciu identycznego strumienia znaków klucza. Wymaga to, aby urządzenia generujące strumień znaków klucza po stronie nadawczej i odbiorczej były ze sobą zsynchronizowane. Z punktu widzenia bezpieczeństwa tego typu szyfrów ważne jest, aby strumień znaków klucza był nieprzewidywalny i praktycznie niepowtarzalny, tzn. aby jego okres był dostatecznie długi. Cechą, która wskazuje również obszar zastosowań tego typu szyfrów, jest możliwość zaszyfrowania każdego znaku wiadomości niezależnie od pozostałych znaków. Ma to znaczenie na przykład w połączeniach terminal-komputer, gdy istotne jest przesłanie każdego generowanego w terminalu znaku z utajnieniem ale bez opóźnienia. Każda z opisanych dwóch klas szyfrów posiada jeszcze wiele wariantów, nazywanych trybami pracy (*ang. modes of operation*), pozwalających osiągać wymagane własności systemu, w którym te szyfry są używane. Niektóre tryby pracy szyfrów blokowych pozwalają na naśladowanie zasad pracy szyfrów strumieniowych. Tryby pracy dla algorytmu DES zostały opisane w amerykańskiej normie federalnej FIPS 81, wydanej przez Narodowe Biuro Standardów USA (*ang. National Bureau of Standards*). Tryby te są często

wykorzystywane również w połączeniu z wieloma innymi szyframi blokowymi. W szczególności mogą być również wykorzystywane dla 3DES-a i dla systemu IDEA. Norma FIPS 81 definiuje 4 tryby pracy:

- tryb ECB: tryb elektronicznej książki kodowej (*ang. Electronic Code Book Mode*),
- tryb CBC: tryb szyfrowania z wiązaniem bloków szyfrogramu (*ang. Cipher Block Chaining Mode*),
- tryb CFB: tryb szyfrowania ze sprzężeniem zwrotnym z szyfrogramu (*ang. Cipher Feedback Mode*),
- tryb OFB: tryb szyfrowania ze sprzężeniem zwrotnym z wyjścia (*ang. Output Feedback Mode*).

Tryb ECB jest najprostszym trybem pracy, polega na niezależnym szyfrowaniu kolejnych bloków wiadomości. Nie jest on jednak zalecany do szerokiego stosowania ze względu na to, że powtarzające się bloki wiadomości będą przekształcane w powtarzające się bloki szyfrogramu (przy założeniu, że nie zmieni się klucz). Zwiększa to szansę pomyślnej kryptoanalizy oraz grozi m.in. przepustowości, propagacji błędów, samosynchronizacji itp. Obecnie National Institute of Standards and Technology. możliwością celowego ingerowania napastnika w strumień przesyłanych bloków. Tryb CBC chroni przed wymienionymi wyżej słabościami poprzez łączenie każdego bloku niezaszyfrowanej wiadomości z szyfrogramem poprzedniego bloku. Pierwszy blok wiadomości łączony jest z blokiem o losowo wybranej zawartości, tzw. wektorem początkowym (*ang. initialisation vector - IV*). Efektem zastosowania wektora początkowego oraz łączenia bloków jest zróżnicowanie postaci bloków szyfrogramu, nawet gdy odpowiadające im bloki wiadomości są identyczne. Tryby pracy CFB i OFB pozwalają na realizację szyfru strumieniowego na bazie (blokowego) algorytmu DES, który służy w tych trybach do generowania strumienia znaków klucza. Kolejne znaki klucza są łączone z kolejnymi znakami wiadomości za pomocą sumy modulo 2, czyli operacji XOR. Po stronie odbiorczej taki sam strumień znaków klucza i ta sama operacja sumowania modulo 2 pozwala na odzyskanie jawnej wiadomości z szyfrogramu. Różnica pomiędzy tymi dwoma trybami polega na innym sposobie generowania strumienia znaków klucza, co w konsekwencji daje różne własności szyfru (m.in. inna propagacja błędów, inny stopień bezpieczeństwa). W obu trybach urządzenia po stronie nadawczej i odbiorczej wykonują blokowe przekształcenie szyfrujące, a do wygenerowania jednego znaku strumienia klucza potrzebne jest wykonanie jednego przebiegu szyfrowania pełnego bloku - oznacza to, iż efektywność tych trybów pracy jest tyle razy mniejsza od efektywności trybów blokowych (ECB i CBC) ile wynosi stosunek długości pełnego bloku do długości znaku klucza.

Realizacja usług ochrony informacji może być zapewniona przez operatora sieci telekomunikacyjnej (np. poufność). Jednak realizacja usług takich jak uwierzytelnienie czy niezaprzeczalność jest możliwa jedynie przez końcowych użytkowników poprzez zastosowanie odpowiedniego, specjalizowanego oprogramowania lub sprzętu. Dodatkowo, dla wszystkich ww. usług, wprowadzenie zabezpieczeń przez samego użytkownika daje mu najlepszą gwarancję ich bezpieczeństwa bez konieczności pokładania zaufania w siłę zabezpieczeń wprowadzanych przez operatora sieci telekomunikacyjnej.

8.5 Funkcje skrótu

Systemy kryptografii używające klucza prywatnego do podpisywania danych nie operują bezpośrednio na danych jako takich, lecz wykorzystują reprezentację tych danych o określonej skończonej długości. Dzieje się tak z powodu dużych kosztów szyfrowania całych dużych bloków danych. Funkcja skrótu jest odpowiednia do wykorzystania przez tego typu systemy. Dane generowane przez funkcję skrótu mogą być traktowane jak *odcisk palca*, który jest cechą charakterystyczną i unikalną każdego człowieka.

Proces tworzenia reprezentacji danych w postaci skrótu nazywany jest *ang. hashing*. Niestety, ze względu na skończoną długość skrótu istnieją dwa zestawy danych wejściowych, które posiadają ten sam skrót. Jednak, w przypadku gdy funkcja skrótu jest dobrze skonstruowana, znalezienie danych posiadających taki sam skrót jest bardzo trudne, nawet jeśli wiadomo, że istnieją. Funkcja skrótu opisana jest za pomocą definicji 8.3.

Definicja 8.3. *Funkcja skrótu (ang. hash function) jest funkcją kryptograficzną, która przyjmuje jako dane wejściowe ciąg bitów o dowolnej długości. Stosując algorytm deterministyczny wyznacza ciąg bitów o określonej długości. Ciąg ten nazywany wartością funkcji skrótu lub skrótem (ang. hash value lub ang. hash).*

W praktyce spotyka się różne inne określenia: *odcisk palca* (*ang. fingerprint*), skrót z wiadomości (*ang. message digest*).

Z matematycznego punktu funkcja skrótu H, która przyjmuje jako dane wejściowe m oblicza skrót h (8.1) z danych m.

$$h = H(m) \tag{8.1}$$

Kolizje Dane wejściowe m (*ang. preimage*) skrótu h nie są unikalne. Jeżeli istnieje inny zbiór danych wejściowych m', dla którego spełniona jest zależność 8.2 to para (m, m') nazywana kolizją dla funkcji skrótu H.

$$H(m) = H(m') \tag{8.2}$$

> Konsekwencje istnienia kolizji skrótów mają bardzo poważne skutki dla systemów kryptograficznych, gdyż poważnie je osłabiają. W systemach PKI oznacza to, że istnienie ten sam podpis elektroniczny pod różnymi zbiorami danych.

Krótka historia funkcji skrótu Pierwsza funkcja skrótu do zastosowań kryptograficznych została zaprojektowana przez Ron'a Rivest'a w 1990 roku. Długość skrótu wynosiła 128*bit*. Kolizje zostały dla MD4 zostały znalezione w 1995 roku, a w 2005 roku opublikowano metodę znajdowania danych wejściowych (*ang. preimages*). Przy obecnym stanie systemów komputerowych kolizje można generować w ciągu kilku sekund. W związku z tym algorytm ten jest bezużytecznych dla systemów bezpieczeństwa.

W 1993 roku Ron Rivest opublikował następcę MD4 - algorytm MD5, który obliczał skrót o długości 128*bit*. W 1993 odkryto pewne słabości algorytmu, ale dopiero w 2004 roku znaleziono kolizję. Obecnie znalezienie kolizji zajmuje

kilka sekund na komputerach PC. Bardziej zaawansowane kolizje mogą zostać znalezione w ciągu kilku godzin.

Drugą grupą algorytmów jest rodzina algorytmów SHA (*ang. Secure Hash Algorithm*) do liczenia. Zostały one zaprojektowane przez NSA (*ang. National Security Agency*) i opublikowane przez National Institute of Standards and Technology (NIST).

Pierwotny algorytm SHA-0 został opublikowany w 1993 roku i całkowicie wycofany ze względu na nieujawnione oficjalnie wady.

Algorytm SHA-1 z 1995 roku całkowicie zastąpił SHA-0. Oba algorytmy obliczają skrót o długości 160*bit*ów. Maksymalny rozmiar danych, z których można obliczyć skrót wynosi 2^64*bit*ów. Algorytm działa podobnie jak MD5. Obecnie algorytm SHA-1 nie powinien być używany w nowych aplikacjach, ze względu na zbyt małą długość skrótu, co gwarantuje bezpieczeństwo tylko w okresach krótkoterminowych.

W 2001 roku opublikowano kolejną wersję protokołu pod nazwą SHA-2, która zawiera 4 warianty oznaczane jako :SHA-224, SHA-256, SHA-384, SHA-512.

Algorytm SHA został stworzony z myślą o wprowadzeniu w Ameryce Standard Podpisu Cyfrowego (*ang. Digital Signature Standard*).

W 2009 roku NIST ogłosił publiczny konkurs na następcę algorytmu liczenia funkcji skrótu. W 2012 roku wygrał algorytm SHA-3.

8.5.1 MD4 i MD5

Algorytm MD5 (*ang. Message-Digest algorithm 5* - skrót wiadomości wersja 5) służy do obliczania funkcji skrótu, która z ciągu danych o dowolnej długości generuje 128*b*itowy skrót.

Algorytm został opracowany przez Rona Rivesta (współtwórcę RSA) w 1991. W 2004 znaleziono sposób na generowanie kolizji MD5, co obniża jego bezpieczeństwo w niektórych zastosowaniach (np. podpisywaniu plików).

Z powodu znanych ataków kryptoanalitycznych funkcja MD5 zdecydowanie nie powinna być używana w zastosowaniach wymagających odporności na kolizje, na przykład w podpisie cyfrowym. W innych, takich jak HMAC, nadal może zapewniać satysfakcjonujący poziom bezpieczeństwa choć stosowanie jej w nowych rozwiązaniach nie jest zalecane.

Historia MD5 jest jednym z serii algorytmów zaprojektowanych przez profesora Rona Rivesta z MIT (Rivest, 1994). Poprzednikiem był algorytm MD4, który w wyniku analizy przeprowadzonej przez Hansa Dobbertina okazał się zbyt mało bezpieczny. Jego bezpiecznym następcą był MD5 opracowany w 1991.

W marcu 2005 Arjen Lenstra, Xiaoyun Wang i Benne de Weger zaprezentowali metodę umożliwiającą znalezienie kolizji dla algorytmu MD5 i przeprowadzenie ataku polegającego na wysłaniu dwóch różnych wiadomości chronionych tym samym podpisem cyfrowym. Kilka dni później Vlastimil Klima opublikował algorytm, który potrafił znaleźć kolizję w ciągu minuty, używając metody nazwanej tunneling.

Pod koniec 2008 roku niezależni kalifornijscy specjaliści ds. bezpieczeństwa, we współpracy z ekspertami z Centrum voor Wiskunde en Informatica, Technische Universiteit Eindhoven oraz Ecole Polytechnique Fédérale de Lausanne odkryli lukę w MD5 umożliwiającą podrobienie dowolnego certyfikatu SSL w taki sposób, że zostanie on zaakceptowany przez wszystkie popularne przeglądarki

internetowe. Do podrobienia certyfikatu wystarczyła moc obliczeniowa 200 konsol do gier PlayStation 3.

Od lat 90-tych algorytm MD5 nie jest uważany za bezpieczny do większości zastosowań i w jego miejsce zaleca się stosowanie algorytmów z rodziny SHA-2 lub SHA-3.

Algorytm MD5 jest następujący:

1. Doklejamy do wiadomości wejściowej bit o wartości 1
2. Doklejamy tyle zer ile trzeba żeby ciąg składał się z 512$b$itowych bloków, i ostatniego niepełnego - 448$b$itowego
3. Doklejamy 64$b$itowy (zaczynając od najmniej znaczącego bitu) licznik oznaczający rozmiar wiadomości. W ten sposób otrzymujemy wiadomość złożoną z 512$b$itowych fragmentów.
4. Ustawiamy stan początkowy na $0123456789abcdeffedcba9876543210$
5. Uruchamiamy na każdym bloku (jest przynajmniej jeden blok nawet dla pustego wejścia) funkcję zmieniającą stan
6. Po przetworzeniu ostatniego bloku zwracamy stan jako obliczony skrót wiadomości

Funkcja zmiany stanu ma 4 cykle (64 kroki). Stan jest traktowany jako 4 liczby 32-bitowe. W każdym kroku do jednej z tych liczb dodawany jest jeden z 16 32-bitowych fragmentów bloku wejściowego, pewna stała zależna od numeru kroku oraz pewna prosta funkcja boolowska 3 pozostałych liczb. Następnie liczba ta jest obracana (przesuwana cyklicznie z najstarszymi bitami wsuwanymi w najmłodsze pozycje) o liczbę bitów zależną od kroku, oraz jest dodawana do niej jedna z pozostałych liczb. Skróty 128-bitowe są zbyt krótkie, żeby zabezpieczyć przed generowaniem kolizji w oparciu o atak urodzinowy. Z tego powodu do większości zastosowań lepiej jest używać skrótów co najmniej 160-bitowych.

8.5.2 SHA-1

SHA (*ang. Secure Hash Algorithm*) - rodzina powiązanych ze sobą kryptograficznych funkcji skrótu zaprojektowanych przez NSA (*ang. National Security Agency*) i publikowanych przez National Institute of Standards and Technology (NIST).

Pierwszy z nich opublikowany w 1993 oficjalnie nazwany SHA (nieoficjalnie, żeby nie pomylić z następcami określany jako SHA-0).

SHA-1 opublikowany został w 1995 i całkowicie zastąpił wycofanego (ze względu na nieujawnione oficjalnie wady) z użytku SHA-0. SHA-0 i SHA-1 tworzą 160-bitowy skrót z wiadomości o maksymalnym rozmiarze 264 bity i jest oparty na podobnych zasadach co MD5. Algorytm SHA-1 nie powinien być używany w nowych aplikacjach.

W 2001 powstały cztery następne warianty określane jako SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512).

Podstawowym celem publikacji SHA był amerykański Standard Podpisu Cyfrowego (*ang. Digital Signature Standard*). SHA jest podstawą szyfru blokowego SHACAL.

W 2009 NIST przeprowadził publiczny konkurs na następcę dotychczasowych funkcji skrótu, w duchu podobnym do procesu wyłaniania algorytmu szyfrującego AES. Zostało zgłoszonych kilkadziesiąt kandydatur, które zostały rygorystycznie ocenione. Zwycięski algorytm wyłoniony w 2012 nosi nazwę SHA-3. Porównanie algorytmów SHA zamieszczono w tab. 8.2.

Tab. 8.2: Porównanie algorytmów SHA.

Algorytm	Rozmiar skrótu	Rozmiar bloku	Maks. rozmiar danych	Rozmiar słowa	Znalezione kolizje
SHA-0/SHA-1	160*bit*	512*bit*	$(2^{64} - 1)$*bit*	32*bit*	Tak
SHA-2 (SHA-256/224)	256/224*bit*	512*bit*	$(2^{64} - 1)$*bit*	32*bit*	Nie
SHA-2 (SHA-512/384)	512/384*bit*	1024*bit*	$(2^{128} - 1)$*bit*	64*bit*	Nie

Ataki na algorytm SHA-1 Pierwsze udane ataki na SHA-1 opublikowano w 2004 roku. W latach 2005-2008 opisano szereg różnych ataków (wymagały one wykonania około 263 operacji funkcji kompresującej (280 wymagane jest przy ataku typu *ang. brute-force*). W związki z tym NIST zaprzestał stosowania SHA-1 po roku 2010. Został on zastąpiony przez SHA-2.

8.5.3 SHA-2

W kryptografii SHA-2 to zestaw kryptograficznych funkcji skrótu (SHA-224, SHA-256, SHA-384, SHA-512) zaprojektowany przez National Security Agency (NSA) i opublikowany w 2001 roku przez National Institute of Standards and Technology (NIST) jako Federalny standard przetwarzania informacji rządu Stanów Zjednoczonych. SHA oznacza Secure Hash Algorithm. SHA-2 zawiera szereg zmian odróżniających go od poprzednika SHA-1. SHA-2 składa się z zestawu czterech funkcji dających skróty wielkości 224, 256, 384 lub 512 bitów.

W roku 2005 zostały zidentyfikowane luki w bezpieczeństwie SHA-1, stwierdzono że jest zbyt słaby i byłyby pożądane silniejsze funkcje skrótu. Chociaż SHA-2 wykazuje pewne podobieństwo do algorytmu SHA-1, ataki te nie zostały skutecznie rozszerzone na SHA-2.

W 2012 roku wyłoniony został nowy standard SHA-3.

Algorytmy zostały opublikowane w 2001 roku w projekcie FIPS PUB 180-2, w którym to czasie zostały zaakceptowane przegląd i uwagi. FIPS PUB 180-2, który obejmuje również SHA-1, został wydany jako oficjalny standard w roku 2002. W lutym 2004 r. został opublikowany zapis o zmianie FIPS PUB 180-2, określając dodatkowy wariant, SHA-224, zdefiniowany w celu dopasowania do długości klucza dwóch kluczowych Triple DES. Warianty te są opatentowane w (US 6829355) Device for and method of one-way cryptographic hashing.

W Stanach Zjednoczonych ukazał się patent na mocy licencji royalty free.

SHA-256 i SHA-512 są nowatorskimi funkcjami skrótu liczonymi odpowiednio na 32- i 64-bitowych słowach. Używają różnych ilości przesunięcia i dodatkowych stałych, ale ich struktury są poza tym praktycznie identyczne, różnią się tylko liczbą rund. SHA-224 i SHA-384 są po prostu obciętymi wersjami dwóch pierwszych, obliczone z różnych wartości początkowych.

Funkcje SHA-2 nie są tak powszechnie stosowane jak SHA-1, pomimo lepszego bezpieczeństwa. Przyczyny mogą obejmować brak wsparcia dla SHA-2 w systemach Windows XP z dodatkiem SP2 lub starszym, brak postrzegania pilności, gdyż kolizje SHA-1 nie zostały jeszcze znalezione lub chęć czekania na zestandaryzowanie się SHA-3. SHA-256 służy do uwierzytelniania pakietów Debian oraz standardu podpisywania wiadomości DKIM (*ang. DomainKeys Identified Mail* - http://www.dkim.org/. SHA-512 jest częścią systemu uwierzytelniania archiwalnych video z Międzynarodowym Trybunałem Karnym w ludobójstwie w Rwandzie SHA-256 i SHA-512 są proponowane do wykorzystania w DNSSEC. Dostawcy Uniksa i Linuksa zmierzają do korzystania z 256- i 512-bitowego SHA-2 do bezpiecznego hashowania hasła. Dyrektywa NIST mówi, że amerykańskie agencje rządowe muszą przestać używać SHA-1 po 2010 r., a zakończenie prac nad SHA-3, może przyspieszyć migrację od SHA-1.

Obecnie najlepsze publiczne ataki łamią 41 z 64 rund SHA-256 lub 46 z 80 rund SHA-512.

8.5.4 SHA-3

SHA-3 (Secure Hash Algorithm 3) – kryptograficzna funkcja skrótu wyłoniona w 2012 roku w ramach konkursu ogłoszonego przez amerykański NIST. Konkurs na SHA-3 rozpoczął się w 2009 roku. Zgłoszono do niego 30 kandydatów]. W 2012 roku NIST wyłonił jako zwycięzcę algorytm Keccak.

Algorytm Keccak charakteryzuje się wyższą wydajnością niż SHA-2 zarówno w implementacjach sprzętowych jak i programowych (różnica sięga $25 - 80\%$ w zależności od procesora i implementacji). Keccak ma architekturę *gąbki* (*ang. sponge construction*) - bloki wejściowe są stopniowo *wchłaniane* w kolejnych etapach i mieszane z dużym rejestrem stanu. Blok wyjściowy jest konstruowany w podobny sposób, przez *wyciskanie* kolejnych fragmentów danych wyjściowych z rejestru stanu, wielokrotnie go mieszając pomiędzy wyciskanymi blokami. Wchłanianie i wyciskanie odbywa się na małej części rejestru stanu, poprzez wykonanie funkcji binarnej alternatywy wykluczającej (xor) z danymi wejściowymi, lub odczyt tej samej małej części przy odczycie danych wyjściowych. Pozostała część stanu nigdy nie jest bezpośrednio używana do konstrukcji danych wyjściowych, ani nie oddziałuje bezpośrednio z danymi wejściowymi.

Funkcja mieszająca stanu, składa się z wielokrotnej aplikacji funkcji rundy (do 24 razy w przypadku największej wersji algorytmu). Każda runda z kolei, składa się z kompozycji 5 prostych i wydajnych w implementacji funkcji, które dokonują odwracalnych permutacji, rotacji, mieszań albo dyfuzji. Ostatnia z tych funkcji w rundzie, dodatkowo jest parametryzowana stałą wartością zależną od numeru rundy (i wersji algorytmu), w celu usunięcia symetrii z funkcji rundy. Dane wejściowe są dopełniane do całkowitej wielokrotności liczy bitów w pojedynczym bloku, przy pomocy prostego schematu dopełniana zwanego 101: Do ciągu danych wejściowych w postaci ciągu binarnego, dopisz bit o wartości 1, następnie bity o wartości 0, aż do przedostatniego bitu w pełnym bloku,

następnie dopisz bit o wartości 1 dopełniając blok całkowicie.

8.5.5 RIPMED-160

RIPEMD - funkcja skrótu opracowana w ramach projektu Unii Europejskiej o nazwie RIPE (*ang. RACE Integrity Primitives Evaluation*) realizowanego w latach 1988-1992. Funkcja generuje 128-bitowy skrót (stąd też nazywana jest RIPEMD-128). Funkcja została zaprojektowana tak, aby była odporna na znane w czasie opracowywania metody kryptoanalizy. W 1996 roku powstała wersja generująca skrót 160-bitowy nazwana RIPEMD-160. W 2004 roku Xiaoyun Wang, Dengguo Feng, Xuejia Lai oraz Hongbo Yu opublikowali dokument, w którym przedstawili dwie pary wiadomości produkujących te same skróty. Ze względu na mniejszą popularność algorytmu RIPMED niż MD5 czy SHA-1, jest mniej zbadana. Sepcyfikacja algorytmu dostępna jest pod adresem (ISO/IEC 10118-3:2004): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39876.

8.5.6 Aktualny poziom bezpieczeństwa funkcji skrótu

W 2009 roku NIST opublikował raport SP 800-107 na potrzeby zagadnień związanych z podpisem elektroniczny, który zwiera także analizę stanu bezpieczeństwa kryptograficznych funkcji skrótu.

Pod uwagę brana jest funkcja SHA1 oraz funkcje z serii SHA-2 czyli SHA-224, SHA-256, SHA-384 i SHA-512.

Opublikowano tabelę odporności na ataki funkcji skrótu. Odporności mierzono w bitach - tab 8.3.

Tab. 8.3: Odporność na ataki funkcji skrótu w bitach.

Atak / Funkcja	SHA1	SHA-224	SHA-256	SHA-384	SHA-512
Kolizja	< 80	112	128	192	256
Preimage	160	224	256	384	512
Second preimage	$105 - 160$	$201 - 224$	$201 - 256$	384	$394 - 512$

W trakcie wcześniejszych badań prowadzonych przez NIST ustalono, że minimalna złożoność obliczeniowa (odporność) algorytmu kryptograficznego powinna wynosić co najmniej $80 bit$ów.

Dla algorytmu SHA-1 ustalono, że wynosi on $60 bit$ów, czyli jest dużo mniejszy niż wartość minimalna. Podane w opracowaniu podatności moją podstawowe znaczenie dla wyboru wyboru funkcji skrótu w różnych zastosowaniach:

- W internecie serwery SSL (bankowe, sklepy internetowe) wykorzystują powszechnie MD5. Jest to możliwe, gdyż połączenia SSL mają charakter krótkotrwały.
- W przypadku ochrony autentyczności stron WWW za pomocą certyfikatów X.509 wymaga długotrwałej odporności na ataki. W związku z tym stosowanie MD5 w certyfikatach znanego CA umożliwia podrobienie certyfikatu CA.

Z raportu SP 800-107 oraz SP 800-57 wynikają następujące wnioski:

- funkcja skrótu MD5 nie powinna być używana w zastosowaniach związanych z podpisem cyfrowym od 1999 roku.
- funkcja skrótu SHA-1 nie powinna być używana w zastosowaniach związanych z podpisem cyfrowym od roku 2010.

Analogiczne wnioski sformułowano odnośnie wszystkich algorytmów posługujących się kryterium zapewnianej odporności mierzonej w bitach.

- do 2010 roku powinny być używane algorytmy zapewniające minimum 80*bit*ów - nie powinny być stosowane klucze RSA i DSA krótsze niż 1024 bity,
- w latach 2011-2030 powinny być używane algorytmy zapewniające min. 112 bitów. Należy wycofać algorytm 3DES z dwoma kluczami (2TDEA), minimalna długość kluczy RSA i DSA to 2048*bit*ów,
- po roku 2030 powinny być używane algorytmy zapewniające min. 128 bitów - wycofany powinien być każdy każdy algorytm 3DES, minimalne długości kluczy RSA i DSA to 3072*bity*.
- algorytm SHA-1 nie powinien być stosowane w nowych implementacjach.

8.5.7 Implementacje dla popularnych języków

Funkcji SHA mieszania można znaleźć w wielu współczesnych językach programowania, takich jak Java, Python, PHP i Perl. Funkcje skrótu są dostępne w postaci bibliotek lub programów, szczególnie w systemie Linux na licencji GNU.

Libgcrypt Kryptograficzna biblioteka ogólnego zastosowania na podstawie kodu z GNU Privacy Guard.

OpenSSL Szeroko stosowana biblioteka OpenSSL crypto zawierająca darmowe i otwarte implementacje SHA-1, SHA-224, SHA-256, SHA-384 i SHA-512

Cryptlib Biblioteka open source wieloplatformowego oprogramowania narzędzi zabezpieczających

Crypto++ Biblioteka C++ klas public domain systemów kryptograficznych, w tym implementacji algorytmów SHA-1, SHA-224, SHA-256, SHA-384 i SHA-512.

Bouncy Castle Bouncy Castle Library jest bezpłatną biblioteką klas Java i C# która zawiera implementacje algorytmów SHA-1, SHA-224, SHA-256, SHA-384 i SHA-512, jak i innych algorytmów, takich jak Whirlpool,Tiger, RIPEMD, GOST-3411, MD2, MD4 i MD5. jsSHA

Biblioteka JavaScript działająca w wielu przeglądarkach, oblicza hashe SHA pomimo faktu, że JavaScript nie obsługuje 64-bitowych operacji wymaganych przez algorytmy SHA-384 i SHA-512.

LibTomCrypt Przenośny zestaw narzędzi kryptograficznych napisany w ISO C, dostępny w domenie publicznej.

Md5deep Zestaw programów do obliczeń hashów MD5, SHA-1, SHA-256, Tiger, czy Whirlpool na dowolnej liczbie plików. Jest używany w dziedzinie bezpieczeństwa oraz administracji systemów do celów przeprowadzenia dużej liczby plików przez jeden z kilku różnych skrótów kryptograficznych. Jest podobny do sha1sum z GNU Core Utilities i md5sum.

8.6 Algorytmy szyfrujące

Obecnie na rynku jest kilka algorytmów szyfrujących mających duże znaczenie praktyczne. Większość z nich została opracowana w latach 70 XX wieku. Należą do nich algorytmy: RSA, DES, 3DES, IDEA, AES. Zostaną one omówione w dalszej części. Algorytmy szyfrujące były używane od dawna. Krótka historia algorytmów została opisana w rozdziale 8.1.

8.6.1 RSA

Algorytm został stworzony w roku 1977 w MIT w USA przez Ronalda L. Rivest'a, Adi Shamir'a i Leonard'a Adleman'a (RSA). Jest to niesymetryczny algorytm szyfrujący posiadający dwa klucze: publiczny do kodowania informacji oraz prywatny do jej odczytywania. Klucz publiczny (można go udostępniać wszystkim zainteresowanym) umożliwia jedynie zaszyfrowanie danych i w żaden sposób nie ułatwia ich odczytania, nie musi więc być chroniony. Dzięki temu firmy dokonujące transakcji poprzez sieć Internet mogą zapewnić swoim klientom poufność i bezpieczeństwo. Drugi klucz (prywatny, przechowywany pod nadzorem) służy do odczytywania informacji zakodowanych przy pomocy pierwszego klucza. Klucz ten nie jest udostępniany publicznie. System RSA daje możliwość bezpiecznego przesyłania danych w środowisku, w którym może dochodzić do różnych nadużyć. Bezpieczeństwo oparte jest na trudności rozkładu dużych liczb na czynniki pierwsze. Obecnie nie dysponujemy na tyle dużymi mocami obliczeniowymi oraz efektywnymi algorytmami, aby złamać algorytm RSA. Z biegiem lat, szyfr ten może okazać się zbyt słaby. Obecnie minimalna długość klucza RSA, która zapewni odpowiedni poziom bezpieczeństwa wynosi 1024 bity, co daje nam: $n == 2^{1024}$. Każda para kluczy jest wyraźnie określona. Klucz prywatny pasuje tylko do klucza publicznego, przy czym klucz prywatny generowany jest na podstawie klucza publicznego. Wykorzystuje się tu dwa twierdzenia z podzielności liczb oraz liczb pierwszych, jak również funkcję Eulera i działania modulo.

Twierdzenie (Euklidesa) mówi, że jest nieskończenie wiele liczb pierwszych. Twierdzenie to nie podaje jak wyrażają się kolejne liczby pierwsze i w jaki sposób są od siebie zależne. Pozwala jednak stwierdzić, że szukanie największej liczby pierwszej będzie zawsze procesem nieskończonym i że zawsze będzie istniała liczba pierwsza większa od największej znanej. Podstawowe Twierdzenie Arytmetyki określa, że każdą liczbę naturalną $n > 1$ można jednoznacznie przedstawić jako iloczyn liczb pierwszych. To twierdzenie daje już pewne ciekawsze wnioski. Wiedząc dodatkowo, że nie znamy efektywnych algorytmów rozkładu liczby na czynniki pierwsze (inaczej: faktoryzacji) możemy wykorzystać ten fakt, na przykład przy projektowaniu algorytmu szyfrowania, co właśnie jest używane

w RSA. Problem faktoryzacji jest problemem trudnym obliczeniowo. Ma wykładniczą złożoność obliczeniową. Jak bardzo utrudnia to życie, będzie można się przekonać podczas analizy bezpieczeństwa algorytmu RSA. Funkcja Eulera jest wykorzystywana w algorytmie RSA, a zatem jej znajomość jest niezbędna do rozumienia działania szyfru. Funkcja Eulera jest funkcją przekształcającą zbiór liczb pierwszych w liczby naturalne, oznaczana jako $\phi(n)$, i jest ilością wszystkich liczb względnie pierwszych z n i mniejszych od n.

Definicja 8.4. *Liczby m i n są względnie pierwsze, gdy $NWD(m,n) = 1$, gdzie $NWD(x,y)$, to największy wspólny dzielnik liczb x i y.*

Warto wiedzieć, że jeśli: p - liczba pierwsza, to: $\phi(p) = p-1$ Widzimy tu jak ważne w RSA są liczby pierwsze i działania na nich (faktem jest, że większość szyfrów asymetrycznych, czyli opartych na kryptosystemie klucza publicznego, korzysta z arytmetyki modularnej i własności liczb pierwszych). Na zakończenie rozważań, zdefiniujmy działanie modulo i kongruencje. Działanie modulo dla $x, y \in R$ i $y \neq 0$ jest zdefiniowane następująco: $x \; mod \; y = x - y * E(x/y)$, gdzie: E oznacza największą liczbę całkowitą, nie większą od x (inaczej nazywane entier lub podłoga).

Przyjmuje się $x \; mod \; 0 = x$.

Definicja 8.5. *Definicja: Kongruencją nazywamy relację na liczbach rzeczywistych określoną następująco: $a == b(mod\ m) <=> m|(a-b)$, czyli a przystaje do b modulo m, jeśli m jest podzielne przez $a-b$.*

W taki sposób przedstawia się matematyczne podstawy szyfrowania w kluczu RSA. Algorytm RSA składa się z trzech podstawowych kroków:

- generacja klucza publicznego i prywatnego. Klucz publiczny jest udostępniony wszystkim użytkownikom i umożliwia zaszyfrowanie danych. Klucz prywatny umożliwia rozszyfrowanie danych zakodowanych kluczem publicznym. Jest trzymany w ścisłej tajemnicy.

- użytkownik po otrzymaniu klucza publicznego, np. poprzez sieć Internet, koduje za jego pomocą swoje dane i przesyła je w postaci szyfru RSA do adresata dysponującego kluczem tajnym, np. do banku, firmy komercyjnej, tajnych służb. Klucz publiczny nie musi być chroniony, ponieważ nie umożliwia on rozszyfrowania informacji - proces szyfrowania nie jest odwracalny przy pomocy tego klucza. Zatem nie ma potrzeby jego ochrony i może on być powierzany wszystkim zainteresowanym bez ryzyka złamania kodu.

- adresat po otrzymaniu zaszyfrowanej wiadomości rozszyfrowuje ją za pomocą klucza prywatnego.

8.6.2 DES

W szyfrowaniu symetrycznym wyróżniamy system DES. Standard DES został stworzony przez inżynierów IBM, jako udoskonalona wersja projektu LUCIFER powstałego w późnych latach 60. LUCIFER, był szyfrem blokowy, który pracował na blokach 64*b*itowych z kluczem 128*b*itowym. W wyniku przeprowadzonych

prac powstała udoskonalona wersja LUCIFERA, bardziej odporna na kryptoanalizę, za to z kluczem zmniejszonym do 56*b*itów. W roku 1977 został on zaakceptowany przez Narodowy Instytut Standardów i Technologii jako Data Encryption Standard. DES od samego początku był mocno krytykowany, głównie z powodu 56*b*itowego klucza, ale także z powodu tzw. S-bloków, czyli elementów struktury wewnętrznej, który były tajne. Od kilku lat uznawany jest za algorytm niezapewniający odpowiedniego bezpieczeństwa, głównie ze względu na zbyt małą długość klucza (zbyt mała jak na obecne możliwości obliczeniowe przestrzeń kluczy), która sprawia, że jest bardzo podatny na atak siłowy. W związku z tym zaleca się zaniechanie stosowania tego algorytmu w jego podstawowej postaci. W jego miejsce proponuje się najczęściej użycie potrójnego DES-a (3DES), polegającego na trzykrotnym zaszyfrowaniu wiadomości algorytmem DES za pomocą trzech różnych kluczy (co skutecznie chroni przed atakiem metodą przeszukania przestrzeni kluczy), lub użycie szwajcarskiego algorytmu IDEA. W 2001 roku w USA został zastąpiony w ramach standardu federalnego przez AES. Jest jednym z najlepiej przeanalizowanych algorytmów szyfrujących. Funkcja szyfrowania przyjmuje dwa rodzaje danych wejściowych: tekst jawny oraz klucz. Tekst jawny w przypadku DES musi być 64*b*itowy, a klucz jest 56*b*itowy. Przetwarzanie tekstu jawnego na postać zaszyfrowaną obejmuje 3 fazy. Najpierw następuje permutacja wstępna IP, która przestawia bity, tworząc permutowane dane wejściowe. Następnie jest faza 16 iteracji tej samej funkcji, w której skład wchodzą funkcje permutacyjne i podstawiające. Wynik ostatniej iteracji składa się z 64*b*itów, stanowiących funkcję wejściowego tekstu jawnego oraz klucza. Lewa i prawa strona zostają zamienione, tworząc wynik wstępny. Zostaje on poddany permutacji IP-1, która jest odwrotnością permutacji wstępnej. Wynikiem tych wszystkich działań jest 64*b*itowy tekst zaszyfrowany. 56*b*itowy klucz podlega wstępnie permutacji. A na każdą z 16 iteracji tworzy się podklucz (Ki) na drodze kombinacji cyklicznego przesunięcia w lewo i permutacji. Funkcja permutacji jest identyczna dla każdej iteracji, jednak dzięki przesunięciu bitów klucza za każdym razem powstaje inny podklucz. W dokumencie *DES Modes of Operation* określono cztery tryby pracy algorytmu:

- elektroniczna książka kodowa - w tym trybie pracy każdy blok tekstu jawnego szyfrowany jest w blok szyfrogramu, dzięki czemu możliwe jest stworzenie książki kodowej tekstu jawnego oraz odpowiadającego mu szyfrogramu,

- wiązanie bloków zaszyfrowanych - tryb ten wykorzystuje mechanizm sprzężenia zwrotnego: w operacji szyfrowania bieżącego bloku tekstu jawnego wykorzystywany jest poprzedni blok szyfrogramu, w związku z czym każdy blok szyfrogramu zależny jest zarówno od bloku tekstu jawnego, jak i od poprzedniego bloku szyfrogramu,

- sprzężenie zwrotne szyfrogramu - tryb ten umożliwia szyfrowanie danych strumieniowych; do procesu szyfrowania informacji wykorzystywany jest rejestr, najczęściej o pojemności odpowiadającej wielkości bloku, a rozpoczęcie szyfrowania możliwe jest dopiero po odebraniu pełnego bloku danych. W jednym przebiegu n zaszyfrowanych bitów z rejestru sumowanych jest modulo 2 z n bitami tekstu jawnego - tak powstaje pierwszych n bitów szyfrogramu, bity te są następnie dodawane na koniec kolejki,

- sprzężenie zwrotne wyjściowe - tryb ten jest podobny do trybu sprzężenia zwrotnego szyfrogramu - z tą różnicą, że na koniec kolejki dodawane jest n bitów poprzedniego bloku wyjściowego, a nie szyfrogramu.

8.6.3 3DES

Algorytm 3DES został stworzony na bazie algorytmu DES, który będąc zaprojektowanym we wczesnych latach '70 i posiadając klucz o długości 56 bitów, okazał się zbyt słaby i łatwy do złamania za pomocą ataków siłowych. Ze względu na możliwe ataki siła algorytmu 3DES wynosi 112$b$itów.

3DES jest stosowany w płatnościach internetowych (standard EMV), wciąż tworzone są i utrzymywane nowe protokoły bazujące na jego zabezpieczeniach. Jest również używany w niektórych produktach Microsoftu (Microsoft Outlook 2007, Microsoft OneNote, Microsoft System Center Configuration Manager 2012) w celu ochrony ustawień i danych użytkowników. Algorytm 3DES polega na trzykrotnym przetworzeniu wiadomości za pomocą zwykłego algorytmu DES. W najsilniejszej wersji, do algorytmu przekazuje się sekretny klucz szyfrujący o długości 168 bitów, który następnie dzieli się na trzy klucze o długości 56 bitów.

1. Zaszyfrowanie za pomocą pierwszego sekretnego klucza
2. Deszyfrowanie za pomocą drugiego sekretnego klucza
3. Zaszyfrowanie za pomocą trzeciego sekretnego klucza

Operację szyfrowania można zapisać w postaci:

$$c = E3(D2(E1(m)))$$

Operację deszyfrowania wygląda następująco:

$$m = D1(E2(D3(c)))$$

Algorytm w razie konieczności zapewnia kompatybilność z ze zwykłym algorytmem DES. W tym celu za klucze pierwszy i drugi albo drugi i trzeci przyjmuje się dowolny taki sam klucz.

$$c = E3(D1(E1(m))) = E3(m)$$

$$c = E3(D3(E1(m))) = E1(m)$$

Możliwe jest też użycie szyfru 3DES z kluczem sekretnym o długości 112 bitów. W takim przypadku klucze pierwszy i trzeci są równe sobie. Daje to większe bezpieczeństwo niż zaszyfrowanie tekstu dwa razy za pomocą algorytmu DES (z dwoma różnymi kluczami), ponieważ zapewnia obronę przed atakiem meet-in-the-middle (http://pl.wikipedia.org/wiki/Meet_in_the_middle).

$$c = E1(D2(E1(m)))$$

8.6.4 IDEA

IDEA jest algorytmem szyfrowania konwencjonalnego. Został on stworzony przez Xuejia Lai i Jamesa Masseya za Szwajcarskiego Federalnego Instytutu Technologii. IDEA jest jednym z wielu zaproponowanych algorytmów szyfrowania konwencjonalnego, które mają zastąpić DES. IDEA to szyfr blokowy stosujący 128-bitowy klucz do szyfrowania danych w blokach po 64 bity.

Na skuteczność kryptograficzną IDEA mają wpływ następujące czynniki:

- Długość bloków: powinna być ona na tyle duża, aby uniemożliwić skorzystanie z faktu, że częstotliwość powtarzania niektórych bloków jest większa niż innych. Za wartość wystarczająco skuteczną uważa się bloki o długości 64 bitów.
- Długość klucza: co oczywiste im dłuższy klucz, tym większe bezpieczeństwo. Dla IDEA przyjmuje się 128 bitów jako wartość dostatecznie dużą, wykluczającą poszukiwanie klucza.
- Mieszanie: Zależność tekstu zaszyfrowanego od tekstu jawnego i klucza powinna mieć skomplikowany charakter po to, by utrudnić określenie zależności między cechami statystycznymi tekstu jawnego i tekstu zaszyfrowanego.
- Rozpraszanie: Oznacza to, że jeden bit tekstu jawnego wpływa na wiele bitów tekstu zaszyfrowanego, pozwala to na ukrycie struktury statystycznej tekstu jawnego. IDEA jest pod tym względem bardzo skuteczna.

Możliwe są cztery tryby pracy:

- Tryb elektronicznej książki kodowej (electronic codebook - ECB): Każdy 64-bitowy blok tekstu jawnego jest kodowany niezależnie przy użyciu tego samego klucza. Technika ta jest przydatna do szyfrowania niewielkich bloków danych. Na przykład można go zastosować do szyfrowania 128-bitowych kluczy IDEA.
- Tryb wiązania bloków zaszyfrowanych (cipher błock chaining - CBC): Dane wejściowe algorytmu szyfrującego stanowią XOR następnych 64 bitów tekstu jawnego i poprzednich 64 bitów tekstu zaszyfrowanego. W rezultacie, jeżeli taki sam 64-bitowy blok tekstu jawnego pojawi się w strumieniu danych wejściowych więcej niż raz. Za każdym razem otrzymamy inny 64-bitowy blok tekstu zaszyfrowanego.
- Tryb szyfrowania ze sprzężeniem zwrotnym (cipher feedback - CFB): Dane wejściowe przetwarza się w porcjach po J bitów. Poprzedni fragment tekstu zaszyfrowanego używa się jako danych wejściowych algorytmu szyfrującego, który na jego podstawie generuje pseudolosowy wynik. Wynik ten jest odejmowany symetrycznie od tekstu jawnego w celu otrzymania następnej jednostki tekstu zaszyfrowanego. Tryb ten jest przydatny do kodowania długich bloków.
- Tryb sprzężenia zwrotnego wyjściowego (output feedback - OFB): Podobny do CFB z tą różnicą, że jako danych wejściowych dla algorytmu szyfrującego używa się poprzedniego wyniku pracy IDEA. Tryb ten przydaje się do przesyłania strumieniowego przez kanał o dużym poziomie zakłóceń.

8.6.5 AES

Powstanie algorytmu AES (nazwa robocza Rijndael) nastąpiło w wyniku ogłoszonego w 1997 roku konkursu, który został ogłoszony z powodu niewystarczającego poziomu bezpieczeństwa algorytmu DES (siła algorytmu). W wyniku konkursu wyłoniono 5 algorytmów.

1. MARS - szyfr z firmy IBM.
2. RC6 - algorytm opracowany przez Ronalda Rivest'a.
3. Rijandel - robocza nazwa algorytmu AES - algorytm opracowany przez Belgów: Joan Daemen i Vincent Rijmen.
4. SERPENT - algorytm opracowany przez zespół międzynarodowy z Anglii, Izraela i Norwegii.
5. TwoFish - algorytm opracowany przez Bruce'a Schneiera (twórcy BlowFish'a)

Poszczególnym algorytmom przypisano liczbę punktów. Wygrał Rijndael (89 punktów), drugi był SERPENT (59 punktów). Prawdopodobnie najbezpieczniejszym algorytmem był SERPENT, ale był wolniejszy w działaniu od Rijndael i potrzebował więcej pamięci, co było problemem w przypadku np. kart kryptograficznych.

AES jest symetrycznym algorytmem blokowym, działającym na blokach o długości 128*bit*ów. Klucz szyfrujący może mieć długość: 128, 192 lub 256*bit*ów. AES został przyjęty przez NIST jako standard - FIPS-197. Autorami algorytmu byli: Vincent Rijmen i Joan Daemen.

Algorytm AES (Rijndael) jest *iterowanym szyfrem blokowym*, co oznacza, że blok wejściowy oraz klucz przechodzą wielokrotne *rundy* transformacji, zanim wyprodukują wynik. Po każdej rundzie, powstaje szyfr pośredni, zwany *stanem* (*ang. state*). Algorytm może pracować z różnymi długościami kluczy.

AES wykonuje 10 (klucz 128 bitów), 12 (klucz 192 bity) lub 14 (klucz 256 bitów) rund szyfrujących, tzw. *ang. substitution-permutation*. Składają się one z substytucji wstępnej, permutacji macierzowej (mieszanie wierszy, mieszanie kolumn) i modyfikacji za pomocą klucza.

W przyjętej jako standard AES wersji szyfru Rijndael, ograniczono tę różnorodność do możliwości występowania zmiennej liczby kluczy, ale ustalono stałą wielkość bloku na 128*bit*ów. Wersje z różnymi długościami kluczy nazwano AES-128, AES-192 oraz AES-256. Parametry algorytmu dla poszczególnych wariantów przedstawia tab. 8.4.

Funkcja substytucyjna (zastępująca) ma bardzo oryginalną konstrukcję, która uodparnia algorytm na znane ataki kryptoanalizy różnicowej i liniowej. Odmiany algorytmu Rijndael niebędące standardem AES, w zależności od długości klucza i bloku danych wykonują 12 lub 14 rund szyfrujących.

Ocena algorytmu W 2006 opublikowana została praca, w której twierdzi się, że AES nie jest w pełni odporny na atak XSL, ale oszacowanie ilości koniecznych obliczeń obarczone jest dużą niepewnością, w związku z tym oceny, na ile skuteczny jest atak, są różne - zobacz artykuł:

Tab. 8.4: Parametry wariantów algorymtu AES.

Wariant	Wielkość bloku ($*32bity$)	Wielkość klucza ($*32bity$)	Liczba rund
AES-128	4	4	10
AES-192	4	6	12
AES-256	4	8	14

http://www.computerworld.pl/news/102630/Nowe.ataki.na.szyfry.html na portalu www.computerworld.pl.

W 2009 opublikowane zostały dwa nowe ataki z użyciem kluczy pokrewnych (*ang. key related attack*) redukujące złożoność AES-256 do 2^{119}:

- Nowy atak na AES-256 - ipsec.pl: http://ipsec.pl/node/632,
- PDF: https://cryptolux.uni.lu/mediawiki/uploads/1/1a/Aes-192-256.pdf.

W grudniu 2009 opublikowano atak na niektóre sprzętowe implementacje AES umożliwiający odtworzenie klucza ze złożonością 2^{32} przez zastosowanie różnicowej analizy błędów (*ang. differential fault analysis*) - A Diagonal Fault Attack on the Advanced Encryption Standard: http://eprint.iacr.org/2009/581.pdf.

Rozdział 9

Kryptoanaliza

Kryptoanaliza jest dziedziną wiedzy i badań zajmującą się metodami łamania szyfrów. Szyfr jest przełamywalny, jeśli istnieje możliwość odtworzenia tekstu jawnego bądź klucza na postawie tekstu zaszyfrowanego albo określenie klucza na podstawie tekstu jawnego i zaszyfrowanego. Wyróżnia się trzy podstawowe rodzaje przełamywania szyfru:

1. Atak bez tekstu jawnego. Kryptoanalityk musi określić klucz znając tekst zaszyfrowany. Mogą być też znane:

   - metoda szyfrowania,

   - język tekstu jawnego,

   tematyka badanego tekstu oraz słowa charakterystyczne dla tej tematyki z określonym prawdopodobieństwem wystąpienia.

2. Atak z tekstem jawnym. Kryptoanalityk zna pary tekstów jawnego i zaszyfrowanego.

3. Atak z wybranym tekstem jawnym. Kryptoanalityk może zdobyć tekst zaszyfrowany odpowiadający wybranemu fragmentowi tekstu zaszyfrowanego.

9.1 Ataki na schematy generowania podpisów

Zagadnienie bezpieczeństwa algorytmu szyfrującego wobec napastnika próbującego poznać utajnioną treść ma długą i bogatą historię. Inna sytuacja panuje w odniesieniu do prób nadużycia lub ominięcia ochrony zapewnianej przez usługi integralności, uwierzytelnienia lub niezaprzeczalności. Usługi te stosowane są od niedawna i metodyka oceny ich bezpieczeństwa nie jest tak dobrze opracowana. Atak na schemat generowania podpisów cyfrowych ma zwykle na celu sfałszowanie wiadomości, czyli spowodowanie, aby odbiorca przyjął zmodyfikowaną lub spreparowaną przez napastnika wiadomość jako pochodzącą od osoby, której identyfikator występuje pod wiadomością. Przy takim podejściu można rozróżnić następujące klasy ataków:

- atak na klucz prywatny nadawcy,

- atak na funkcję skrótu,
- atak na system dystrybucji kluczy.

Atak na klucz prywatny nadawcy polega na próbie wyznaczenia tego klucza przez napastnika w celu posłużenia się nim do generowania podpisów pod spreparowanymi przez siebie wiadomościami. Wiąże się on z przeprowadzeniem jednego z opisanych w poprzednim punkcie ataków na kryptosystem używany do generowania podpisów. Atak na funkcję skrótu plasuje się zwykle w kategorii ataków z wybranym tekstem jawnym i polega na sprowokowaniu prawowitego użytkownika do podpisania nieszkodliwej wiadomości, a następnie takim zmodyfikowaniu wiadomości aby podpis pod niż był nadal prawidłowy lecz jej treść stała się korzystna dla napastnika (a równocześnie często szkodliwa dla podpisującego). W schematach generowania podpisów wykorzystujących funkcje skrótu działanie napastnika jest następujące:

- przygotowuje on wiadomość z akceptowalną dla podpisującego treścią i znajduje jej skrót,
- znajduje wiadomość o korzystnej dla siebie treści, która ma taki sam skrót,
- prosi użytkownika o podpisanie pierwszej wiadomości i zachowuje podpis, czyli wynik przekształcenia kluczem prywatnym użytkownika skrótu wiadomości,
- w wybranym przez siebie momencie przedstawia zapamiętany podpis oraz przygotowaną wcześniej, korzystną dla siebie wiadomość. Stwierdzi, iż to ona właśnie została świadomie podpisana przez użytkownika. Wiadomość ma identyczny skrót jak oryginalnie podpisana wiadomość, w związku z tym proces weryfikacji podpisu zakończy się pomyślnie (potwierdzeniem związku między wiadomością, podpisem i użytkownikiem, który tego podpisu dokonał).

Ochrona przed tego typu atakiem leży w odpowiednim doborze funkcji skrótu. Musi ona bowiem mieć własność, która uniemożliwi napastnikowi wykonanie drugiego kroku tego ataku, czyli znalezienia wiadomości o z góry zadanej wartości skrótu. Jeszcze mocniejszym wymaganiem, chroniącym przed tzw. atakiem opartym na paradoksie dnia urodzin (*ang. birthday paradox*) jest uniemożliwienie znalezienia dwóch wiadomości, które mają identyczny skrót. Atak na system dystrybucji kluczy wiąże się z przekonaniem wybranego użytkownika do weryfikacji odebranego podpisu przy użyciu niewłaściwego klucza publicznego, najczęściej klucza publicznego napastnika. Napastnik może w takiej sytuacji samodzielnie wygenerować podpis mający uchodzić za podpis innej osoby, a następnie spowodować, aby użytkownik sięgający po klucz publiczny tej osoby w celu weryfikacji podpisu otrzymał klucz publiczny napastnika. Podpis zostanie wtedy pomyślnie zweryfikowany a użytkownik dokonujący tej weryfikacji będzie przekonany, iż odebrana wiadomość została podpisana przez osobę, której podpis napastnik chciał sfałszować. W systemach wykorzystujących certyfikaty tego typu atak wymaga najczęściej penetracji przez napastnika Urzędu ds. Certyfikatów w celu wystawienia fałszywego certyfikatu klucza publicznego.

Znane z historii przypadki łamania szyfru były najczęściej powodowane nie słabością samego szyfru lecz ubocznymi aspektami jego stosowania: słabościami

systemu dystrybucji kluczy, słabościami implementacji szyfrów lub błędami operatorów (szyfrantów). W związku z tym konieczne jest bardzo uważne projektowania i użytkowania wszystkich elementów systemu bezpiecznej łączności, a nie jedynie wyboru najsilniejszego szyfru. System jest bowiem tylko tak bezpieczny jak jego najsłabsze ogniwo.

9.2 Kryptoanaliza metodą anagramową

Metoda ta jest szczególnie przydatna w przełamywaniu szyfrów przestawieniowych (permutacyjnych). Kryptoanalitycy mogą łatwo poznać, czy zastosowany szyfr jest szyfrem przestawieniowym, gdyż częstość wystąpień liter tekstu szyfrowanego jest taka sama jak częstość występowania liter w tekście zaszyfrowanym. Metoda anagramowa polega na odtworzeniu właściwej kolejności przemieszanych znaków z wykorzystaniem tablic częstości występowania digramów (kombinacji 2-literowych) i trigramów (kombinacji 3-literowych).

9.3 Analiza częstości występowania liter

Metoda ta jest efektywna, gdy mamy do czynienia z prostymi szyframi podstawieniowymi. Atak polega na porównaniu częstości występowania liter w kryptogramie z częstościami oczekiwanymi. Metoda ta pozwala z dużym prawdopodobieństwem dopasować litery kryptogramu do liter tekstu jawnego. Wielce pomocną w pracy kryptoanalityka jest znajomość częstości występowania digramów i trigramów.

9.4 Brutalna metoda przełamywania algorytmów kryptograficznych

Brutalna metoda przełamywania algorytmów kryptograficznych polega na przeszukaniu całej przestrzeni klucza. I tak, gdy mamy do czynienia z szyfrem podstawieniowym typu szyfr Cezara to przestrzeń klucza ogranicza się do 25 kombinacji dla alfabetu angielskiego (kolejno sprawdzamy podstawienia dla alfabetu szyfrującego przesuniętego o $1, 2, 3, ..., 25$ pozycje w prawo w stosunku do alfabetu tekstu szyfrowanego). Złożoność obliczeniowa rośnie, gdy atak przeprowadzamy na szyfr podstawieniowy z alfabetem szyfrującym będącym dowolną kombinacją odwzorowań znak alfabetu jawnego - znak alfabetu szyfrującego. W tym przypadku mamy do sprawdzenia 26! (silnia) kombinacji, czyli 403291461126605635584000000 przypadków. Współczesne algorytmy szyfrujące opierają się wprawdzie na alfabecie dwuznakowym $(0, 1)$ ale ilość kombinacji dla klucza 56*b*itowego jest równa 256. Zakładając, że superkomputer może sprawdzić milion kluczy na sekundę, znalezienie właściwego klucza zajmie mu ok. 2000 lat.

9.5 Kryptoanaliza różnicowa

Kryptoanaliza różnicowa została opracowana przez E. Bihama i A. Shamira dla algorytmu DES. Później została zaadoptowana do różnych innych szyfrów ite-

racyjnych. Metoda ta polega na szyfrowaniu par tekstów jawnych różniących się w określony sposób (stąd nazwa metody) i analizie uzyskanych szyfrogramów. W niniejszy rozdziale zostanie opisana merytoryczna strona kryptoanalizy różnicowej algorytmu DES W algorytmie DES zastosowano skrzynki o sześciu bitach wejściowych i czterech wyjścia. Wynika stąd, iż każda skrzynka ma $64 * 64$ możliwe wartości par wejściowych (zakładając, że istotna jest kolejność w parze). Dla każdej pary określić można różnicę jej wartości poprzez wyliczenie ich bitowej sumy modulo 2 (czyli poprzez wykonanie operacji XOR na odpowiadających sobie bitach; rezultat takiej operacji nazywany jest różnicą wartości, ponieważ na pozycjach, na których bity się różnią, w wyniku otrzymujemy jedynki - rezultat niejako informuje nas na jakich pozycjach są różne wartości). Podobnie wartości XOR'rów można wyliczyć dla par na wyjściu skrzynki. Ponieważ wejście skrzynki jest sześciobitowe, natomiast wyjście - czterobitowe, mamy 64*16 możliwych par: XOR wejściowy - XOR wyjściowy. Wynika stąd, że na każdą parę XOR wejściowy - XOR wyjściowy przypadają średnio cztery pary wartości wejściowych. Jednak nie wszystkie kombinacje XOR wejściowy - XOR wyjściowy są możliwe, a te możliwe mają nierównomierny rozkład. Tablicę ilustrującą rozkład XOR'ów wejściowych i wyjściowych wszystkich możliwych par wejściowych skrzynki nazywamy tablicą rozkładu XOR'ów par. Określony element takiej tablicy jest liczbą mówiącą ile jest par wejściowych o XOR'ze określonym przez numer wiersza tego elementu, które dają na wyjściu XOR wyjściowy określony przez numer kolumny.

9.6 Kryptoanaliza liniowa

Liniowa kryptoanaliza jest dziś najbardziej efektywną metodą kryptoanalizy DES. Wymaga średnio 243 par tekst jawny - kryptogram dla znalezienia klucza. Metoda ta została odkryta i opublikowana w latach 90-tych przez Mitsuru Matsui'ego. Inaczej jak w przypadku kryptoanalizy różnicowej, nie była brana pod uwagę przy projektowaniu algorytmu DES. Kryptoanaliza liniowa może być użyta jako:

1. atak ze znanym tekstem jawnym,
2. atak z tekstem zaszyfrowanym.

Jest to atak, który wykorzystuje zależności miedzy bitami danych wejściowych rundy, bitami klucza oraz wynikami rundy. Oczywiście, związki te zachodzą tylko statystycznie dla stosunkowo dużej lub stosunkowo małej liczby danych wejściowych. Kluczową rolę odgrywają tu formuły aproksymujące liniowo pojedyncze S-boksy.

Rozdział 10

System PKI

Infrastruktura klucza publicznego (*ang. Public Key Infrastructure*) PKI to zbiór osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego i certyfikatów elektronicznych.

Historia PKI Opublikowanie w 1976 roku przez Diffiego, Hellmana, Rivesta, Shamira i Adlemana algorytmów bezpiecznej wymiany kluczy i algorytmu asymetrycznego całkowicie odmieniło sposoby bezpiecznej komunikacji. Wraz z dalszym rozwojem szybkich form komunikacji cyfrowej (takich jak Internet i jego przodkowie), potrzebny był zaufany sposób komunikacji między ludźmi a wraz z tym pewność z kim rozmawiamy.

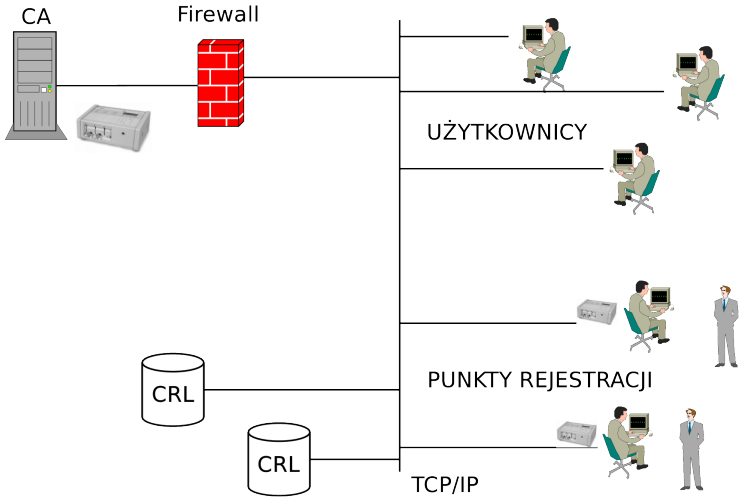
Stworzono różnorodne protokoły kryptograficzne, w których nowe dogmaty mogły zostać efektywnie użyte. Wraz z wynalezieniem Internetu i jego szybkim rozprzestrzenianiem się zaistniała potrzeba bezpieczeństwa i uwierzytelniania uczestników komunikacji. Z powodów handlowych (takich jak e-handel, bezpośredni dostęp do prywatnych baz danych np. banków itp.) problem ten stał się bardzo ważny. Taher Elgamal wraz z innymi pracownikami Netscape przedstawił protokół SSL (*https* w adresie WWW); zawierający między innymi uwierzytelnianie serwera. Tak oto została stworzona infrastruktura klucza publicznego dla użytkowników i stron internetowych, którym zależało na bezpiecznej komunikacji.

Sprzedawcy i przedsiębiorcy zauważyli duży potencjał rynkowy, zaczęto tworzyć nowe przedsiębiorstwa (lub nowe projekty dla już istniejących przedsiębiorstw). W swoim projekcie American Bar Association przeanalizowała możliwe aspekty prawne dotyczące operacji z użyciem PKI i niedługo po tym kilka stanów w USA (jako pierwszy Utah w 1995 roku), oraz inne jurysdykcje na całym świecie, zaczęły uchwalać akty i odpowiednie regulacje prawne. Grupy konsumentów oraz inne kluczowe zagadnienia dotyczące prywatności, dostępu i odpowiedzialności zostały w różnym stopniu wzięte pod uwagę w zależności od jurysdykcji.

Wprowadzone prawa i regulacje różniły się między sobą, zaistniały pewne problemy techniczne i operacyjne w przekształceniu schematów PKI na użytek komercyjny, a postęp w ich wdrażaniu był wolniejszy niż początkowo zakładano.

Przedsiębiorcy z branży PKI odnaleźli swoje miejsce na rynku, lecz nie takie były ich wyobrażenia w latach 90. Szybkość i kierunek rozwoju rynku nie był, taki jak się tego wcześniej spodziewali. Wbrew oczekiwaniom infrastruktura klucza publicznego nie rozwiązała wszystkich problemów, przez co niektórzy sprzedawcy przestali istnieć, lub zostali przejęci przez inne przedsiębiorstwa. Infrastruktura klucza publicznego największy sukces osiągnęła na rynku rządowym.

Działanie systemu PKI Schemat działania systemu PKI przedstawiono na rys.10.1.



Rys. 10.1: System PKI.

W skład systemu wchodzą:

- CA (*ang. Certification Authority*) - urząd certyfikacji, Centrum Certyfikacji Kluczy (CCK) to strona zaufana, która wystawia certyfikaty kluczy, generuje listy CRL i certyfikuje inne CA.
- RA (*ang. Registration Authority*) - urząd rejestracji, punkt rejestracji - zbiera wnioski o wydanie certyfikatu, weryfikuje tożsamość właścicieli certyfikatów (subskrybentów).

Rozwinięciem tradycyjnego modelu infrastruktury klucza publicznego może być zastosowanie podpisu elektronicznego z mediatorem, w którym podpis finalizowany jest online z udziałem mediatora, który przechowuje połówkę klucza prywatnego.

10.1 Funkcje PKI

Do podstawowych funkcji PKI należą:

- Weryfikacja tożsamości subskrybentów

- Wymiana kluczy kryptograficznych
- Wystawianie certyfikatów
- Weryfikacja certyfikatów
- Podpisywanie przekazu
- Szyfrowanie przekazu
- Potwierdzanie tożsamości
- Znakowanie czasem

Dodatkowo, w pewnych konfiguracjach, możliwe jest odzyskiwanie kluczy prywatnych. Podstawowe funkcje, które musi realizować każdy system PKI, aby zapewnić właściwy poziom usług to:

Rejestracja (*ang. Registration*) Użytkownik końcowy składa wniosek do Organu Rejestracji o wydanie certyfikatu. W tym celu dostarcza szereg informacji, wymaganych przez Kodeks Postępowania Certyfikacyjnego (Certification Practices Statement - CPS) danego CA. Dane te to np. nazwa własna podmiotu lub osoby wnioskującej o certyfikat, nazwa domenowa czy adres IP. Przed wystawieniem certyfikatu CA potwierdza (korzystając z wytycznych zapisanych w CPS) zgodność z prawdą danych, podanych przez użytkownika. Jeżeli o certyfikat ubiega się osoba fizyczna, CA weryfikuje także autentyczność własnoręcznego podpisu na wniosku o wydanie certyfikatu.

Certyfikacja (*ang. Certification*) Jeżeli dane, podane przez ubiegającego się o certyfikat, zostaną potwierdzone, CA wystawia nowy certyfikat (zawierający m.in. klucz publiczny posiadacza) i dostarcza go użytkownikowi. Jednocześnie klucz publiczny zostaje udostępniony wszystkim zainteresowanym poprzez złożenie go we właściwym repozytorium.

Generacja kluczy (*ang. Key generation*) Para kluczy (prywatny i publiczny) może zostać wygenerowana samodzielnie przez użytkownika końcowego, może on także powierzyć tę operację CA. W pierwszym przypadku użytkownik przesyła do CA jedynie swój klucz publiczny, w celu poddania go procesowi certyfikacji. Klucz prywatny pozostaje przez cały czas w rękach właściciela, dlatego też metodę tę uważa się za najbardziej bezpieczną. Jeżeli klucze generuje CA, są one dostarczane do użytkownika końcowego w sposób gwarantujący ich poufność, Wykorzystuje się do tego m.in. celu karty mikroprocesorowe (*ang. smartcard*), karty PCMCIA lub tokeny USB, zabezpieczone dodatkowym kodem PIN.

Odnawiania kluczy (*ang. Key update*) Wszystkie pary kluczy oraz skojarzone z nimi certyfikaty wymagają okresowego odnawiania. Jest to kolejne zabezpieczenie na wypadek ujawnienia klucza prywatnego skojarzonego z kluczem publicznym umieszczonym na certyfikacie. Wymiana kluczy jest konieczna, gdy:

Wymiana certyfikatu po okresie ważności Jest to sytuacja normalna, występująca regularnie co pewien czas (np. raz do roku). Odbywa się w możliwie krótkim czasie, bez dodatkowych formalności.

Klucz prywatny, skojarzony z umieszczonym na certyfikacie kluczem publicznym, został skompromitowany Jest to sytuacja wyjątkowa, a więc wymiana kluczy nie będzie już tak płynna i łatwa. W takich przypadkach CA odwołuje certyfikat poprzez umieszczenie jego numeru seryjnego na ogólnodostępnej liście CRL. Od tego momentu stary certyfikat traci ważność i rozpoczyna się procedura wystawiania nowego certyfikatu. Najgorszy przypadek dla każdego CA to kompromitacja klucza prywatnego jego Głównego CA (Root CA). W takim przypadku cała infrastruktura PKI podległa temu CA zostaje uznana za skompromitowaną i musi być tworzona od nowa.

Certyfikacja wzajemna (*ang. Cross-certification*) Ponieważ społeczność międzynarodowa nie stworzyła dotąd Globalnego Organu Certyfikacji (Global Root CA), powstało wiele Głównych Organów Certyfikacji (Root CA), początkowo nie powiązanych relacjami zaufania. Certyfikacja wzajemna rozwiązuje ten problem i pozwala użytkownikom z jednej struktury PKI ufać certyfikatom wystawianym przez CA z innej struktury. Główne CA z różnych struktur certyfikują się wzajemnie - może być to certyfikacja jednokierunkowa albo dwukierunkowa.

Odwołanie certyfikatu (*ang. Revocation*) Istnieją sytuacje, w których zachodzi potrzeba wcześniejszego odwołania certyfikatu. Powodem może być kompromitacja klucza prywatnego, zmiana nazwy przez użytkownika końcowego, bądź odejście pracownika z firmy, która wystawiła mu certyfikat. Zdefiniowana w standardzie X.509 metoda odwoływania certyfikatów wykorzystuje wspomniane już Listy Unieważnionych Certyfikatów (CRL), okresowo publikowane przez CA w repozytorium, w którym są przechowywane certyfikaty. Każdy certyfikat posiada swój unikalny numer seryjny, przypisany przez CA w momencie jego wystawiania. Lista CRL zawiera spis identyfikatorów odwołanych certyfikatów i jest opatrzona znacznikiem czasu, wystawionym przez CA.

Odzyskiwanie klucza (*ang. Key recovery*) Jest to dodatkowe zabezpieczenie na wypadek sytuacji, gdy użytkownik utraci swoje klucze. Jeżeli wszystkie klucze do szyfrowania albo negocjacji kluczy były przechowywane w bezpiecznym archiwum, będzie można je odzyskać i umożliwić dostęp do zaszyfrowanych danych. Najważniejsze jest zagwarantowanie, że klucze będzie mógł odzyskać tylko ich właściciel, nie zaś osoba trzecia.

10.2 Zastosowania PKI

System PKI posiada wiele zastosowań. Należą do nich:

- Zabezpieczanie kanałów komunikacyjnych
- uwierzytelnianie użytkownika
- uwierzytelnianie serwerów w sieci
- składanie podpisu elektronicznego
- szyfrowanie informacji

10.3 Certyfikaty kluczy

Certyfikaty kluczy można podzielić na dwie grupy, zgodnie z zapisami w odpowiednich aktach prawnych (rozdział 3):

- certyfikaty niekwalifikowane,
- certyfikaty niekwalifikowane zaufane,
- certyfikaty kwalifikowane.

Certyfikat niekwalifikowany zaufany jest elektronicznym dokumentem tożsamości uwierzytelniającym danego użytkownika w sieci Internet, zawierającym zbiór określonych danych identyfikacyjnych, poświadczonych przez Zaufaną Trzecią Stronę (Centrum Certyfikacji Kluczy) i powiązany z określoną parą kluczy kryptograficznych.

W Polsce działa kilka centrów certyfikacji kluczy, ale tylko CERTUM PCC jako jedyne w Polsce oferuje certyfikaty niekwalifikowane zaufane (czyli wydawane zgodnie ze standardem WebTrustSM/TM):

CERTUM PCC jest certyfikowanym centrum przez inne globalne CCK. Z tego powodu oferowane certyfikaty zapewniają wysoki poziom bezpieczeństwa i są uznawane za zaufane w skali globalnej, między innymi we wszystkich rozpowszechnionych przeglądarkach internetowych na świecie oraz we wszystkich produktach firmy Microsoft. Certyfikaty mają zastosowanie m.in. do:

- szyfrowania poczty elektronicznej,
- składania zwykłego podpisu elektronicznego,
- logowania do systemów online przez WWW (np. konto bankowe, serwis www, administracja kontem, serwisy hostingowe),
- logowanie do aplikacji.

10.4 Podpis elektroniczny i podpis cyfrowy

W ustawodawstwie rozróżnia się pojęcia *podpisu cyfrowego* (*ang. digital signature*) i podpisu elektronicznego (*ang. electronic signature*).

Definicja 10.1. *Podpis cyfrowy (ang. digital signature) zgodnie z normą ISO 7498-2:1989 to dane dołączone do danych lub ich przekształcenie kryptograficzne, które pozwala odbiorcy udowodnić pochodzenie danych i zabezpieczyć je przed fałszerstwem.*

Definicja 10.2. *Podpis elektroniczny (ang. electronic signature), to zgodnie z Dyrektywę unijną 1999/93/EC, jest to operacja podpisywania dokumentu elektronicznego przez osobę fizyczną.*

Podpis kwalifikowany - jest elektronicznym podpisem równoważnym podpisowi własnoręcznemu. Służy do podpisywania dokumentów i umów, które mają moc prawną.

10.4.1 Zastosowania podpisu elektronicznego

- przesyłanie dokumentów do jednostek administracji publicznej (od 9 lipca 2011 roku darmową alternatywą jest Profil Zaufany)
- podpisywanie umów zapisanych w formie elektronicznej
- składanie zleceń w niektórych aukcjach internetowych
- podpisywanie faktur elektronicznych
- uwierzytelnianie transakcji w Banku

Więcej informacji na temat podpisu elektronicznego można znaleźć na stronie Narodowego Centrum Certyfikacji `http://www.nccert.pl/`

10.4.2 Systemy podpisu elektronicznego

Na rynku istnieją dwa systemy podpisu elektronicznego, działające na różnych zasadach:

- zdecentralizowane, których reprezentantem jest system PGP
- scentralizowane, których reprezentantem jest system X.509.

PGP

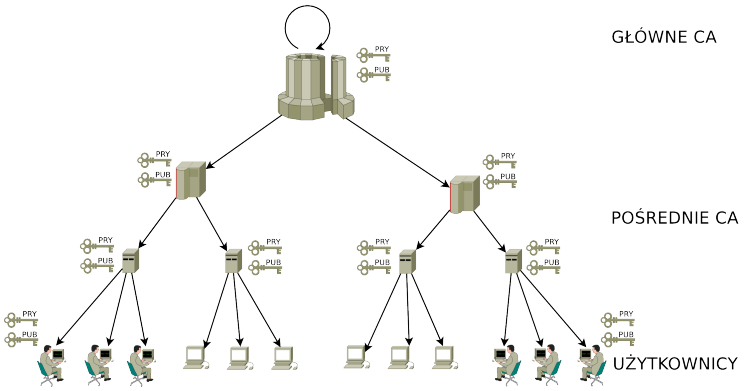
PGP jest systemem zdecentralizowanym, w którym poziom autentyczności danego klucza jest determinowany przez sumę podpisów, złożonych przez różne osoby znające posiadacza klucza (model Sieć zaufania). System ten jest powszechnie wykorzystywany w Internecie oraz w środowiskach korporacyjnych (np. niektóre systemy EDI).

X.509

System X.509 jest systemem scentralizowanym, w którym autentyczność klucza jest gwarantowana przez hierarchię urzędów certyfikacji (rys. 10.2 formalnie poświadczających związek klucza z tożsamością jego właściciela. Ze względu na jednoznaczną odpowiedzialność, łatwiejszą do osadzenia w prawie, X.509 jest obecnie dominującym systemem, na którym opiera się aktualnie obowiązujące prawodawstwo o podpisie elektronicznym.

10.5 Atak na system PKI

W 2008 roku grupie naukowców udało się przeprowadzić udany atak na centrum certyfikacji (CA), używające w podpisie certyfikatu funkcji skrótu MD5. Efektem tego ataku było otrzymanie certyfikatu CA z poprawnym podpisem, pomimo złożenia wniosku o certyfikat kliencki. Certyfikat ten umożliwia podpisywanie certyfikatów klienckich, którym zaufa większość popularnych przeglądarek internetowych, a więc efektywne podszycie się pod dowolną stronę internetową używającą certyfikatów. Praca opisująca ten atak została przedstawiona 30 grudnia 2008 roku na Chaos Communication Congress w Berlinie.



Rys. 10.2: Hierarchia urzędów certyfikacji X.509.

Rozdział 11

Sprzęt

Obecnie produkuje się szereg urządzeń związanych stosowanych w dziedzinie ochrony systemów informatycznych. Jeżeli urządzenia są stosowane do przetwarzania informacji klasyfikowanych, to muszą być certyfikowane. W dalszej części zostaną omówione następujące klasy urządzeń:

- urządzenia klasy tempest, o minimalnym ulocie elektromagnetycznym,
- karty i czytniki kryptograficzne,
- sprzęt i oprogramowanie do realizacji systemu PKI,
- systemy bezpiecznej łączności, telefony i infrastruktura sieciowa zapewniająca bezpieczną komunikację.

Należy zaznaczyć, że na rynku światowym jest szereg firm oferujących tego typu systemy, lecz możliwości produkcji i dostęp do *know-how* jest ograniczany.

11.1 Certyfikacja urządzeń

Certyfikacją urządzeń zajmuje się Służba Kontrwywiadu Wojskowego (SKW), która zamieszcza na swojej stronie WWW listę urządzeń dopuszczonych: http://www.skw.gov.pl/ZBIN/certyfikacja_lista.htm. Na stronie SKW zamieszczone są odpowiednie wnioski o wykonanie certyfikacji urządzeń kryptograficznych. SKW wydaje także szereg zaleceń, które są zgodne z odpowiednimi normami. Stosowane kryteria oceny z zakresu bezpieczeństwa teleinformatycznego (stan na luty 2015) zawarte są w szeregu dokumentach:

- Common Criteria
- ITSEC : Information Technology Security Evaluation Criteria (ITSEC), version 1.2, June 1991
- ITSEM : Information Technology Security Evaluation Manual (ITSEM), version 1.0, September 1993
- JIL : ITSEC Joint Interpretation Library (ITSEC JIL), version 2.0, November 1998

Kryteria stosowane są także w innych krajach.

11.2 Urządzenia klasy tempest

Urządzenia elektroniczne są źródłem promieniowania elektromagnetycznego, które może być źródłem informacji o działaniu systemu (przepływie informacji w systemie). Sygnały te mają określoną częstotliwość związaną z rodzajem podzespołu, który pracuje. W przypadku komputerów najsilniejszym źródłem promieniowania jest monitor komputerowa. Każdy podzespół komputera emituje promieniowanie, w tym kable, gniazda, porty, drukarki, skanery. Emisja promieniowania odbywa się także do sieci energetycznej poprzez zasilacz.

Promieniowanie elektromagnetyczne można odebrać za pomocą specjalizowanych urządzeń (czułych odbiorników pracujących na częstotliwości $10Hz..5GHz$) z odległości nawet kilkuset metrów. Sygnały mogą być odbierane zarówno z sieci energetycznej jak i instalacji grzewczej, klimatyzacyjnej i wodnej. Odebrane sygnały są następnie odszumiane i poddawane obróbce cyfrowej przez odpowiednie programy komputerowe, które umożliwiają np. odtworzenie danych z edytora tekstów. Urządzenia takie nie są dostępne na rynku i nie ma ich w ofercie żadnej z firm.

Istnieją różne metody zabezpieczanie przed ulotem elektromagnetycznym:

- klatka Farraday'a - odpowiednio uziemiona kabina, która znacznie ogranicza poziom promieniowania elektromagnetycznego wychodzący na zewnątrz do poziomu, który uniemożliwia podsłuch;
- stosowanie siatek Farraday'a folii metalowych do wyklejania ścian pomieszczeń, niestety poziom ulotu elektromagnetycznego jest większy niż dla klatek Farraday'a;
- metalowe pudełka, w których umieszcza się urządzenia;
- zabezpieczenie komputerów przenośnych, według amerykańskich norm TEMPEST (*ang. temporary emanation and spurious transmission*, które znane są pod różnymi nazwami: NAG1A, FS222, NACSIM 5100, NSCD.

Obecnie Narodowa Agencja Bezpieczeństwa (NSA) USA jest instytucją upoważnioną do rewidowania oraz przyjmowania wszystkich standardów dla systemów oraz sprzętu związanych z bezpieczeństwem Systemów Informatycznych, w tym także urządzeń klasy TEMPEST. Zarówno normy jak i technologia wytwarzania sprzętu klasy TEMPEST są utajnione, lecz obecnie jest możliwość wytwarzania tego typu sprzętu przez firmy prywatne (po spełnieniu odpowiednich kryteriów).

Krąg użytkowników sprzętu klasy TEMPEST jest ograniczony wyłącznie do instytucji NATO oraz krajów członkowskich. Użytkownikami mogą być:

- siły zbrojne;
- agendy NATO;
- organizacje wywiadowcze;
- służba dyplomatyczna;
- łączność specjalna;
- instytucje odpowiedzialne za ład i porządek;

- instytucje i ośrodki przetwarzania danych niejawnych.

Podstawową normą dla rządzeń klasy TEMPEST jest norma NSTISSAM/1-92 (USA), której odpowiednikiem w krajach NATO jest norma AMSG (AMSG 720 B, AMSG 788, AMSG 784). W Polsce zdefiniowano także poziomy ochrony:

TPZU - techniczny poziom zabezpieczenia miejsca zdefiniowany przez BT SKW

SSOE - sprzętowa strefa ochrony elektromagnetycznej według JC DBTI ABW

Poziomy te wiążą się z poziomami (klasami) bezpieczeństwa elektromagnetycznego urządzeń klasy TEMPEST:

- Level I (poziom 1) - wg normy AMSG 720 B, SDIP-27A, SSOE 0, TPZU 3, NATO ZONE 0 - norma pozwala na użytkowanie sprzętu IT w odległości nie większej niż $20m$ od intruza - odległości mniejsze niż $8m$ wymagają konsultacji;
- Level II (poziom 2) - wg normy AMSG 788, SDIP-27B, SSOE 1, TPZU 2, NATO ZONE 1 - norma pozwala na użytkowanie sprzętu IT w odległości nie mniejszej niż $20m$ od intruza.
- Level III (poziom 3) - wg normy AMSG 784, SDIP-27C, SSOE 2, TPZU 1, NATO ZONE 2 - norma pozwala na użytkowanie sprzętu IT w odległości nie mniejszej niż $100m$ od intruza.

W Polsce urządzenia klasy TEMPEST oferuje firma Siltec Sp. z o.o. - http://www.siltec.pl. W ofercie posiada m.in.: komputery, monitory, skanery, drukarki, notebooki, serwery i sprzęt sieciowy, kabiny ekranujące, inne rozwiązania dedykowane.

11.3 Karty i czytniki kryptograficzne

Urządzenia kryptograficzne są przeznaczone głównie dla użytkowników korzystających z podpisu elektronicznego. Urządzenie kryptograficzne zabezpiecza zapisane na nim klucze prywatne, które służą do składania podpisu elektronicznego. Klucze te są generowane w mikroprocesorze (chipie) bezpośrednio wewnątrz urządzenia, tam również odbywają się wszystkie operacje szyfrujące prowadzące do wygenerowania podpisu elektronicznego. Urządzenia kryptograficzne są skonstruowane w ten sposób, by nie istniała możliwość przechwycenia zapisanych kluczy. Dostęp do urządzenia zabezpieczony jest kodem PIN definiowanym przez użytkownika. Dzięki zastosowaniu tych mechanizmów urządzenia kryptograficzne w znacznym stopniu podnoszą bezpieczeństwo korzystania z różnego rodzaju systemów informacyjnych. Karta kryptograficzna jest urządzeniem, które ma na celu zabezpieczenie fizyczne i logiczne kluczem prywatnym. Zabezpieczenie fizyczne polega na takiej konstrukcji urządzenia, aby nie było możliwości ingerencji w jego wnętrze, bez jednoczesnego zniszczenia wszystkich poufnych danych, przechowywanych w jej wnętrzu.

Karty umożliwiają wykorzystanie najnowocześniejszych technologii z dziedziny ochrony danych i identyfikacji. Gwarantują wysoki poziom bezpieczeństwa w obszarze identyfikacji, przesyłania danych i przeciwdziałania fałszerstwu. Czytniki kryptograficzne to urządzenia pozwalające na korzystanie z kart

kryptograficznych. Do komputera użytkownika podłączane jest zazwyczaj do portu USB. Niektóre komputery posiadają wbudowane czytniki kart. Czytniki kart służą do komunikacji karty kryptograficznej z aplikacją podpisującą. Dzięki temu można złożyć podpis elektroniczny, który zostanie wygenerowany na karcie i dotrze do aplikacji podpisującej. Działanie karty jest identyczne jak w przypadku nośnika kryptograficznego USB, z tą różnicą, że korzystanie z karty kryptograficznej wymaga dodatkowo posiadania czytnika kart procesorowych (zewnętrznego, podłączanego do komputera np. przez port USB, bądź też wewnętrznego, wbudowanego w komputer). Specjalistyczne karty i czytniki kryptograficzne można zastosować w:

- systemie PKI: podpis elektroniczny i szyfrowanie;
- systemach kontroli dostępu do pomieszczeń;
- rejestracji czasu pracy;
- systemach identyfikacji wizualnej (identyfikacja kart pracowniczych / korporacyjnych);
- systemach komunikacji miejskiej;
- systemach ochrony dostępu do komputera.

11.3.1 Karty kryptograficzne firmy Unizeto

Firma Unizeto jest producentem kart kryptograficznych. Karty współdziałają z systemami kryptograficznymi produkowanymi w Polsce.

Unizeto cryptoCertum 3.2 Jest to najnowsza wersja karty kryptograficznej. Wyróżnia się nowym systemem operacyjnym kart procesorowych. Karta została wyposażona w sprzętową realizację algorytmu RSA o długości klucza do 2048*b*itów. Karta kryptograficzna spełnia wymagania techniczne komponentu technicznego określone w rozporządzeniu Rady Ministrów do ustawy o podpisie elektronicznym. Wraz z oprogramowaniem proCertum CardManager posiadającym deklarację zgodności wchodzi w skład zestawów CERTUM do składania bezpiecznych podpisów.

Unizeto cryptoCertum 3.0 Karta kryptograficzna spełnia wymagania techniczne określone w rozporządzeniu Rady Ministrów do ustawy o podpisie elektronicznym - posiada certyfikat Common Criteria EAL4+. Wraz z oprogramowaniem proCertum CardManager posiadającym deklarację zgodności wchodzi w skład zestawów do składania bezpiecznych podpisów.

Giesecke & Devrient Starcos SPK3.0 Starcos SPK3.0 to system operacyjny kart procesorowych dla najbardziej wymagających użytkowników. STARCOS SPK3.0 umożliwia wykorzystanie kart procesorowych w wielu obszarach, m.in: jako dowód osobisty, chip w paszportach, identyfikacja wizualna i elektroniczna klientów firm, korporacji, klinik, uczniów szkół, PKI: podpis elektroniczny i szyfrowanie, kontrola dostępu do pomieszczeń, rejestracja czasu pracy, identyfikacja wizualna (identyfikacyjna kart pracownicza / korporacyjna), karta komunikacji miejskiej, ochrona dostępu do komputera.

Giesecke & Devrient Sm@rtCafe Expert Sm@rtCafe Expert to system operacyjny przeznaczony dla kart Java i zgodny ze specyfikacją SUN Java Card, GlobalPlatform, ISO 7816 i zgodny ze specyfikacją SUN Java Card, GlobalPlatform, ISO 7816 i EMV. Dzięki systemowi operacyjnemu pracującemu w technologii Java karty wykorzystujące go mają więcej zalet niż standardowe karty procesorowe. W praktyce przekłada się to na tańszą i uproszczoną implementację oraz maksymalną elastyczność i bezpieczeństwo.

11.3.2 Czytniki kart kryptograficznych

W rozdziale omówiono rozpowszechnione czytniki kart kryptograficznych. Są one używane w wielu miejscach, np. w działach księgowości do autoryzacji transakcji bankowych (np. system NBP). W opisach podano możliwe zastosowanie oraz podstawowe cechy.

ACS ACR38 USB Czytnik ACR38 łączy w sobie nowoczesny design z osiągnięciami najnowszych technologii i stanowi doskonałe rozwiązanie dla najbardziej wymagających środowisk. Nadaje się idealnie, między innymi, do zastosowań w obrębie bezpieczeństwa sieci, systemów płatności elektronicznych czy identyfikacji oraz innych.

ACS ACR38U-I1 Czytnik ACR38 łączy w sobie zaawansowaną technologię i nowoczesne wzornictwo. Dodatkowo spełnia rygorystyczne wymagania stawiane m.in. systemom płatności czy systemom identyfikacji elektronicznej, w którym największy nacisk kładziony jest na wysoki poziom bezpieczeństwa.

ACS ACR 101 SIMicro Łącząc w sobie czytnik kart inteligentnych formatu ID000, Micro-czytnik kart SD oraz układ Mifare 1k w kompaktowej obudowie ACS ACR 101 SIMicro oferuje pełne wsparcie dla wysoce bezpiecznych aplikacji mobilnych. Czytnik kart inteligentnych formatu ID000 daje możliwość wykorzystywania go do operacji związanych z podpisem elektronicznym oraz usługami PKI.Układ Mifare przekształca urządzenie w bezdotykowego tokena wykorzystywanego do różnych zastosowań bezstykowych, takich jak dostęp logiczny i fizyczny. Czytnik pamięci Micro-SD obsługujący karty pamięci do 8GB kart pamięci. Z uwagi na te wszystkie funkcje, ACR101 SIMicro (CCID) jest doskonałym narzędziem dla inteligentnych aplikacji kart wymagających wysokiego poziomu bezpieczeństwa i elastyczności.

ACS ACR 1281U - C1 ACR1281U-C1 DualBoost II to czytnik z podwójnym interfejsem, dzięki któremu można uzyskać dostęp do aplikacji za pomocą kart bezstykowych (zbliżeniowych kart procesorowych) oraz stykowych kart procesorowych. Dodatkowo wyposażony jest we wbudowane gniazdo kart SAM (formatu ID000). Jest czytnikiem podłączanym do komputera przez port USB zalecanym do użytku w systemach informatycznych, których użytkownicy posiadają karty procesorowe o podwójnym interfejsie. Jego wielofunkcyjność pozwala ograniczyć koszty związane z kupnem dwóch czytników (stykowego i zbliżeniowego). Czytnik kart ACS ACR 1281U - C1 to wygoda, szybkość i bezpieczeństwo funkcjonalnej technologii bezstykowej przy logowaniu do sieci, stron internetowych

oraz aplikacji. Stosowany również do bezpiecznego przechowywania nazw użytkowników i ich haseł oraz informacji osobistych. Można śmiało powiedzieć, że ilość możliwych zastosowań bezstykowych kart procesorowych ogranicza tylko wyobraźnia.

ACS ACR APG8201 - A1 z generatorem OTP ACS ACR APG8201-A1 stanowi doskonałe rozwiązanie dla potrzeb handlu elektronicznego, fizycznej kontroli dostępu do pomieszczeń, bezpiecznego dostępu do sprzętu komputerowego oraz narzędzi aplikacyjnych dla transportu i GSM, home banking czy portfela elektronicznego. Jest czytnikiem kart elektronicznych formatu ID1 i dodatkowo posiada funkcjonalność generatora haseł jednorazowych . Może pracować podłączony do PC lub niezależnie wykorzystując zasilanie bateryjne. Czytnik kart elektronicznych wyposażony jest w klawiaturę oraz wyświetlacz. Posiada wsparcie dla technologii bezpiecznego wprowadzania kodu PIN (SPE). Generator jednorazowych haseł umożliwia jednokrotne autoryzowanie transakcji online co sprawia, że są one bardzo dobrze chronione.

ACS ACR 38U-N1 ACR38U PocketMate jest czytnikiem inteligentnych kart typu SAM. Dzięki zastosowaniu najnowszej technologii, ACR38U PocketMate został zaprojektowany tak, aby spełnić potrzeby bezpieczeństwa w różnych zastosowaniach, np. w bankowości elektronicznej, płatnościach elektronicznych i e-administracji.

Omnikey CardMan 3021 USB Cardman 3021 cechuje się niezawodnością powszechnie znaną z innych modeli czytników OMNIKEY. Zastosowana w urządzeniu wydajna technologia procesorowa opracowana wspólnie z firmą Atmel pozwala na uzyskanie transmisji pomiędzy czytnikiem a kartą na wysokim poziomie 420 kbsp.

ACS ACR 100l Czytnik elektronicznych kart stykowych formatu ID000. Posiada wbudowaną pamięć flash NAND o dużej pojemności. Dodatkowo czytnik wyposażony jest we wbudowany moduł Mifare 1k umożliwiający logowanie logiczne i fizyczne zapewniając dużą elastyczność w jego użyciu. Jest wielofunkcyjnym urządzeniem. Wymiary jakie posiada to zaledwie $76,0x26,0x12,0mm$ co sprawia, że ACR100I jest czytnikiem mobilnym.

ACS ACR38T Nowy czytnik ACR38T typu SIM to niewielkie urządzenie USB o nowoczesnym wyglądzie. Posiada taką samą funkcjonalność jak standardowy czytnik ACR38. Obsługuje karty zgodne z ISO 7816, karty pamięci i GSM. Zapewnia interoperacyjność oraz daje możliwość zastosowania na różnych platformach informatycznych. Waga czytnika jest tak sama jak standardowej pamięci USB.

ACS ACR38T CCiD Czytnik kart elektronicznych ACS ACR38T CCiD przystosowany jest do kart spełniających wymogi specyfikacji GSM typu SIM. Charakteryzuje się kompaktową budową, pracuje w oparciu o interfejs USB a brak okablowania sprawia, że jest wygodny w użyciu.

ACS ACR38F Smart Floppy USB ACR38F Smart Floppy stanowi idealne rozwiązanie do łatwej integracji czytnika kart w środowisku komputera stacjonarnego. Interfejs USB umożliwia wykorzystanie wewnętrznego zasilania komputera oraz konfigurację najbardziej odpowiadającą preferencjom klienta. Czytnik ACR38F Smart Floppy jest bardzo łatwy w użyciu i montażu. Stanowi idealne rozwiązanie dla handlu elektronicznego, home banking czy portfela elektronicznego.

ACS ACR38ET DualKey2 USB ACR38ET DualKey2 jest bogatszą wersją czytnika ACR38TCCiD. Działa jako czytnik kart SIM oraz jako karta bezstykowa, wykorzystując obsługę standardu Mifare. Może zabezpieczać dostęp do sprzętu komputerowego, sieci wewnętrznych i zewnętrznych, drzwi, sejfów, banków danych, itp. Jest przy tym bardzo prostym urządzeniem zapewniającym funkcjonalność w zakresie technologii karty stykowej formatu ID-0 umieszczonej w czytniku jaki i wbudowanej karty bezstykowej. Stanowi doskonałe rozwiązanie dla potrzeb handlu elektronicznego, fizycznej kontroli dostępu, home banking czy portfela elektronicznego, bezpiecznego dostępu do sprzętu komputerowego oraz narzędzi aplikacyjnych dla transportu i GSM

Klawiatura z czytnikiem ACS ACR38K USB Klawiatura ACR38K łączy w sobie funkcje klawiatury oraz czytnika kart, co umożliwia łatwą implementację systemów kartowych lub aplikacji w środowisku komputerowym. Wyposażona jest w poręczny i wygodny w użyciu czytnik kart inteligentnych wykorzystujący moduł ACR30, dzięki czemu staje się sprawnym elementem systemu bezpieczeństwa w handlu elektronicznym i innych aplikacjach.

Omnikey CardMan 1010 RS232 Omnikey CardMan 1010 to czytnik, który posiada certyfikat PC/SC. Do komputera podłączany jest za pomocą portu RS232 (tzw. serial).Wykorzystywany jest do obsługi kart mikroprocesorowych. Jego współpraca z aplikacjami opiera się na standardowych interfejsach.

Omnikey CardMan 3111 CardMan 3111 jest czytnikiem typu Plug&Play podłączanym do komputera przez port RS 232 (tzw. serial). Ma certyfikat EMV. Jest łatwy w instalacji, obsługuje karty pamięciowe i mikroprocesorowe. Został zaprojektowany tak, aby w pełni zgadzał się z powszechnie znanymi standardami.

Omnikey CardMan 3121 CardMan 3121 to czytnik typu Plug&Play podłączany do komputera przez port USB. Łatwo go zainstalować, obsługuje karty pamięciowe i mikroprocesorowe. Został zaprojektowany tak, aby w pełni zgadzać się z powszechnie znanymi standardami. Współpraca z aplikacjami opiera się na standardowych interfejsach. Wsparcie USB CCID sprawia, że można go zainstalować w istniejących systemach łatwiej niż do tej pory: sprowadza się do podłączenia czytnika do portu USB bez potrzeby instalacji jakichkolwiek sterowników. Poniższe cechy sprawiają, że dostarczany przez Unizeto czytnik Omnikey CardMan 3121 to idealna odpowiedź na rosnące zapotrzebowanie rynku.

Omnikey CardMan 3621 CardMan 3621 oparty jest na technologii procesorowej opracowanej wspólnie z firmą Atmel i posiada PIN pad klasy drugiej z wyświetlaczem. Osiąga prędkości transmisji danych pomiędzy czytnikiem a kartą na poziomie $420kBaud$. To rekordzista w klasie czytników kart procesorowych. CardMan 3621 jest zgodny z wieloma standardami i dlatego też umożliwia wykorzystanie praktycznie każdej stykowej karty procesorowej dostępnej na rynku. Umożliwia bezpieczne wprowadzanie kodu PIN, a fakt wykonywania operacji na karcie sygnalizują diody. Dane wrażliwe nie są przekazywane do komputera ani też nie są przesyłane przez niebezpieczne połączenie komputer - czytnik, lecz pozostają cały czas w środowisku czytnik - karta.

Omnikey CardMan 3921 CardMan 3921 to wbudowany czytnik plug & play USB do gniazda 3,5ó szybkości transmisji na kartę do 420kbps. Dzięki zgodności ze wszystkimi normami, czytnik ten jest kompatybilny praktycznie ze wszystkimi kartami i systemami operacyjnymi. Przeznaczony do szerokiego zastosowania. Prowadzone w szerokim zakresie badania i rozwój zapewniają, że obecne i przyszłe systemy kartowe będą współpracować z tym urządzeniem. CardMan 3921 jest dostępny w wersji niezależnej z wewnętrznym kablem do USB do połączenia z płyta główną lub w wersji detalicznej z kablem wewnętrznym, kablem zewnętrznym z wtyczką USB A i śrubami montażowymi.

Omnikey CardMan 4040 PCMCIA CardMan 4040 jest zaprojektowany tak, aby spełniał wszystkie najważniejsze standardy. Interfejs PCMCIA sprawia, że CardMan 4040 to rozwiązanie, które poleca się do komputerów przenośnych, PDA lub innych systemów wykorzystujących PC-Bus. Jego praca opiera się na standardowych interfejsach. Wsparcie natywne umożliwia wykorzystanie go w środowiskach niestandardowych.

Omnikey CardMan 4321 ExpressCard CardMan 4321 jest jednym z pierwszych dostępnych na rynku czytników kart ExpressCard. Nowy standard interfejsu przystosowany do mniejszych i szybszych rozwiązań kratowych dla komputerów przyszłych generacji, został już zastosowany w ostatnich laptopach zamiast, albo jako zamiennik do tradycyjnych gniazd rozszerzających. Nowy, szybki czytnik ExpressCard produkcji OMNIKEY doskonale spełnia zadania niezależnie od wymagań dla bezpieczeństwa mobilnych aplikacji kartowych. Wykorzystuje interfejs USB 2.0 określony przez normy ExpressCard do szybkiej integracji z urządzeniem mobilnym. Dzięki małym wymiarom nadaje się do masowej dystrybucji drogą pocztową lub w postaci niewielkiej paczki z kartami albo oprogramowaniem.

Omnikey CardMan 5321 RFID CardMan 5321 stanowi doskonałe połączenie technologii stykowej i bezstykowej w jednym urządzeniu. Obudowa jest optymalna pod kątem wygody użytkownika w zastosowaniach bezstykowych. Udoskonalone pole bezstykowe zapewnia wysoką szybkość transmisji do $848kbps$ w zależności od zastosowanej karty. Podobnie, jak CardMan 5121, spełnia wymogi trzech standardów ISO dla kart bezstykowych oraz standardów przemysłowych dla kart stykowych. CardMan 5321 zapewnia użytkownikowi wygodę, szybkość i bezpieczeństwo technologii bezstykowej dla aplikacji obejmujących

między innymi rejestrowanie się w systemie Windows, stronach www i aplikacjach. Zapewnia bezpieczne przechowywanie nazw użytkowników, haseł i informacji osobistych.

Omnikey CardMan 6121 Jest to czytnik Plug&Play z certyfikatami CCID & EMV przeznaczony do komputerów z interfejsem USB 2.0. Łatwo go zainstalować, a poza tym obsługuje karty pamięciowe i mikroprocesorowe. CardMan 6121 został stworzony zgodnie z powszechnie znanymi standardami, specyfikacją PC-2001 oraz wieloma innymi. CardMan 6121 pracuje w oparciu o standardowe interfejsy. Wsparcie USB CCID umożliwia łatwą instalację, która sprowadza się do podłączenia czytnika do portu USB bez potrzeby instalowania dodatkowych sterowników.

11.4 Sprzęt kryptograficzny firmy Enigma

Firma Enigma Systemy Ochrony Informacji jest producentem oprogramowania kryptograficznego, w tym kompletnego systemu PKI o nazwie Centaur. Firma ściśle współpracuje z firmą Techlab 2000 będącą producentem sprzętu kryptograficznego. Enigma SOI jest obecnie częścią firmy COMP. Produkowane oprogramowanie stosowane jest m.in. w bankowości (NBP), administracji, w wojsku i policji. Listę certyfikowanych urządzeń i oprogramowania można znaleźć na stronach SKW (http://www.skw.gov.pl).

Oferowane produkty obejmują następujące grupy:

- Sprzętowe szyfratory IP.
- Szyfratory wojskowe.
- Sprzęt i oprogramowanie dla centrum certyfikacji kluczy.

Poniżej zamieszczono skrócone opisy produkowanego sprzętu.

11.4.1 Sprzętowe szyfratory IP

CompCrypt ETA-VPN 100P

Urządzenie szyfrujące IP CompCrypt ETA-VPN 100P (umożliwia tworzenie bezpiecznych wydzielonych sieci VPN (Virtual Private Networks). Zapewnia bezpieczną komunikację pomiędzy stacjami roboczymi, systemami lub sieciami lokalnymi (LAN). Dzięki wykorzystaniu mechanizmu opartego na infrastrukturze klucza publicznego (PKI) urządzenie zapewnia wysoki poziom bezpieczeństwa transmisji oraz uwierzytelniania urządzeń, a także elastyczność zastosowanych rozwiązań.

Rozwiązanie jest przeznaczone przede wszystkim dla jednostek administracji rządowej przetwarzających i przesyłających między swymi lokalizacjami informacje zgodnie z ustawą o ochronie informacji niejawnych.

Główne zalety:

- Certyfikat ochrony kryptograficznej do klauzuli POUFNE ważny do 30.11.2019,

- Antypenetracyjna obudowa - norma FIPS-140-2 poziom 3,
- Automatyczne szyfrowanie sesji bez udziału użytkownika,
- Moduł bezpieczeństwa z podtrzymywanym zasilaniem przechowujący wszystkie krytyczne parametry urządzenia,
- Przechowywanie logów oraz konfiguracji w zaszyfrowanej postaci,
- Wykorzystywane algorytmy szyfrowe: Algorytm Niejawny, AES, RSA, SHA.

Parametry techniczne:

- Logowanie do urządzenia przy pomocy kart mikroprocesorowych
- Klawiatura i wyświetlacz wbudowana w panel przedni urządzenia
- 5 interfejsów sieciowych 100 Mb
- Zasilanie z sieci 220-240V, 50Hz
- Zasilanie awaryjne modułu bezpieczeństwa
- Wymiary (szer., wys., gł.) 482,5 x 88 x 482,5 mm
- Waga: 12 kg

11.4.2 Szyfratory wojskowe

Wygląd szyfratorów wojskowych można obejrzeć na stronach internetowych firmy Engoma.

CompCrypt ETA-MIL 10P Urządzenie szyfrujące IP CompCrypt ETA-MIL 10P to urządzenie klienckie do utajniania informacji w sieci IP i tworzenia wydzielonych sieci VPN (Virtual Private Networks). Pozwala na dołączanie pojedynczych stacji roboczych lub systemów bezpiecznej łączności IP, bazujących na kompleksowym rozwiązaniu CompCrypt ETA-MIL. Szyfrator przeznaczony jest do wykorzystania w obudowie klasy tempest stacji roboczej. Urządzenie może być wykorzystywane zarówno w systemach wojskowych, jak i cywilnych. Posiada certyfikat do ochrony kryptograficznej nr 40/2011/JC SKW o klauzuli: POUFNE, NATO CONFIDENTIAL oraz CONFIDENTIEL EU.

Do głównych zalet urządzenia można zaliczyć:

- Certyfikat do ochrony kryptograficznej do klauzuli: POUFNE, NATO CONFIDENTIAL, CONFIDENTIEL UE, ważny do 31.08.2018
- Automatyczne szyfrowanie sesji bez udziału użytkownika,
- Generowanie głównego klucza IPSec wewnątrz urządzenia,
- Logowanie do urządzenia przy pomocy kart mikroprocesorowych,
- Fizyczny generator ciągu losowego zgodny z normą FIPS-140-2,
- Zarządzanie kluczami kryptograficznymi oparte na infrastrukturze PKI z wykorzystaniem certyfikatów X.509v3
- Zasilanie awaryjne modułu bezpieczeństwa

Parametry techniczne urządzenia

- Logowanie do urządzenia przy pomocy kart mikroprocesorowych
- Klawiatura wbudowana w panel przedni urządzenia
- Interfejsy komunikacyjne: 2 x Ethernet 10/100 Base-T
- Interfejsy zarządzania: 2 x RS-232
- Zasilanie: zewnętrzne, stabilizowane $+12V$, $< 20W$
- Zasilanie awaryjne modułu bezpieczeństwa
- Wymiary (szer., wys., gł.): 150 x 41,5 x 197 mm
- Waga: 1,5 kg

CompCrypt ETA-MIL 10P-EX Urządzenie szyfrujące IP CompCrypt ETA-MIL 10P-EX to urządzenie do utajniania informacji w sieci IP z możliwością dołączania pojedynczych użytkowników lub całych sieci /obiektów/ lokalizacji do systemów bezpiecznej łączności IP, bazujących na kompleksowym rozwiązaniu CompCrypt ETA MIL. Szyfrator ETA-MIL 10P-EX jest urządzeniem wolno stojącym posiadającym odpowiednią konstrukcję obudowy spełniającą najwyższe wymagania zgodnie ze standardem NATO SDIP-27 Level A (dawniej norma AMSG 720B). Urządzenie może być wykorzystywane zarówno w systemach wojskowych, jak i cywilnych. Urządzenia posiadają certyfikat do ochrony kryptograficznej nr 41/2011/JC SKW do klauzuli: POUFNE, NATO CONFIDENTIAL oraz CONFIDENTIEL EU.

Do głównych zalet urządzenia można zaliczyć:

- Certyfikat do ochrony kryptograficznej do klauzuli: POUFNE, NATO CONFIDENTIAL, CONFIDENTIEL UE, ważny do 31.08.2018,
- Certyfikat ochrony elektromagnetycznej SDIP-27 level A (TEMPEST),
- Antypenetracyjna obudowa zgodna z normą FIPS-140-2 poziom 3,
- Logowanie do urządzenia przy pomocy kart mikroprocesorowych,
- Przechowywanie logów oraz konfiguracji w zaszyfrowanej postaci,
- Moduł bezpieczeństwa z podtrzymywanym zasilaniem przechowujący wszystkie krytyczne parametry urządzenia,

Parametry techniczne urządzenia

- Logowanie do urządzenia przy pomocy kart mikroprocesorowych,
- Klawiatura wbudowana w panel przedni urządzenia,
- Interfejsy komunikacyjne: 2 światłowody 100 Base-FX, złącze SC, światłowód MMF 50/125, 62,5/125 mm,
- Interfejsy zarządzania: 2 x RS-232,

- Zasilanie: zewnętrzny zasilacz impulsowy,
- Zasilanie awaryjne modułu bezpieczeństwa,
- Wymiary (szer., wys., gł.): 167,5 x 93,5 x 253 mm,
- Waga: 3,25 kg.

CompCrypt ETA-MIL 10P N7 CompCrypt ETA-MIL 10P N7 jest kolejnym szyfratorem do utajniania informacji w sieci IP i tworzenia tzw. Virtual Private Networks (VPN) pozwalający na dołączanie pojedynczych użytkowników do systemów bezpiecznej łączności IP.

CompCrypt ETA-MIL 10P N7 jest jedynym urządzeniem szyfrującym IP na pole walki z certyfikatem Służby Kontrwywiadu Wojskowego. Powstało na potrzeby rynku wojskowego. Może być instalowane w wozach bojowych, łączności, dowodzenia, jak również w innego rodzaju pojazdach lub też poza nimi, w warunkach polowych. Urządzenie spełnia wymogi środowiskowych norm NO-06-A103 dla urządzeń grupy N7. Jest przygotowane do pracy w temperaturach -30° +50° C, szerokim zakresie wilgotności powietrza oraz ciśnienia atmosferycznego. Posiada odpowiednią konstrukcję obudowy spełniającą najwyższe wymagania zgodnie ze standardem NATO SDIP-27 Level A. Urządzenia posiadają certyfikat do ochrony informacji niejawnych o klauzuli: POUFNE, NATO CONFIDENTIAL oraz EU CONFIDENTIAL do 30.04.2018 r.

Do głównych zalet urządzenia można zaliczyć:

- Certyfikat ochrony kryptograficznej do klauzuli: POUFNE, NATO CONFIDENTIAL, CONFIDENTIEL UE ważny do 30.04.2018 r
- Spełnianie wymogów środowiskowych NO-06-A103 dla urządzeń grupy N7,
- Obudowy spełniającą najwyższe wymagania zgodnie ze standardem NATO SDIP-27 Level A,
- Wytrzymałość w temp. od -40°C do +60°C,
- Uwierzytelnienie oparte na PKI,
- Możliwość użycia krzywej eliptycznej w procesie zestawiania tuneli w protokole uzgadniania kluczy Diffiego-Hellmana.

Parametry techniczne urządzenia

- Automatyczne szyfrowanie sesji bez udziału użytkownika,
- Możliwości skonfigurowania wielu redundantnych sieci zarządzania i audytu,
- Wymiary (szer., wys., gł.): 482,5 x 88 x 300 mm,
- Waga: ok. 15 kg.

11.5 Urządzenia dla systemu PKI

CompCrypt LAMBDA HSM CompCrypt LAMBDA HSM (Hardware Security Module) jest następcą urządzenia szyfrującego DELTA 1 do ochrony informacji w rozległych sieciach informatycznych o złożonej strukturze organizacyjnej. Zapewnia ochronę do poziomu *poufne* kluczy prywatnych urzędu Centrum Certyfikacji w Infrastrukturze Klucza Publicznego (PKI).

Główne cechy urządzenia:

- posiada zabezpieczenia antypenetracyjne zgodne z FIPS 140-3,
- wykorzystuje algorytmy kryptograficzne: RSA o długości 2048/4096 bitów, EC(p) 521 bitów, SHA2-256, SHA-512,
- posiada wbudowany fizyczny generator ciągów losowych,
- posiada wbudowany czytnik kart kryptograficznych,
- umożliwia współbieżną obsługę wielu urzędów certyfikujących.

CompCrypt Delta Rozwiązania należące do grupy CompCrypt Delta wykorzystywane są w sieciach rozległych typu Klient-Serwer pracujących w Infrastrukturze Klucza Publicznego (PKI). Urządzenia mogą być wykorzystywane do realizacji podpisu elektronicznego oraz jako niezależne szyfratory i deszyfratory informacji przesyłowych. W skład rodziny urządzeń CompCrypt Delta wchodzą:

- CompCrypt Delta 1 - stacja certyfikacji kluczy
- CompCrypt Delta 2TLS - urządzenie dla serwerów i grup roboczych (urządzenie niewspierane)
- CompCrypt Delta 3 - urządzenia klienckie
- CompCrypt Delta 4 - urządzenia dla Punktów Rejestracji (urządzenie niewspierane)

CompCrypt Delta 1 Delta 1 jest urządzeniem kryptograficznym przeznaczonym do wykorzystania w Infrastrukturze Klucza Publicznego i pełni rolę Stacji Certyfikacji Kluczy. Funkcje:

- generowanie pary kluczy RSA do podpisów w Centrum Certyfikacji,
- certyfikowanie kluczy publicznych użytkowników systemu,
- podpisywanie list unieważnionych certyfikatów (listy CRL).

11.6 Systemy telefonii firmy Techlab 2000

Firma Techlab 2000 jest obecnie częścią firmy COMP. Firma produkuje sprzęt do bezpiecznej łączności telefonicznej wykorzystujący system PKI. Produkowane są różne rodzaje telefonów oraz przystawki do np. faksów. Główną częścią systemu jest stacja zarządzania kluczami (Teacup). W dalszej części zostaną omówione poszczególne urządzenia całego systemu.

11.6.1 Stacja Zarządzania Kluczami

Stacja zarządzania kluczami Teacup (SZK) realizuje funkcje Urzędu Certyfikacji (UC), najważniejszego elementu Infrastruktury Klucza Publicznego (IKP), oraz Punktu Rejestracji (PR). Powiązanie w jednym elemencie systemu zarówno UC jaki i PR jest optymalne ekonomicznie w przypadku małych i średnich sieci (do kilkuset, pojedynczych tysięcy użytkowników).

Sercem SZK jest Bezpieczny Moduł Kryptograficzny (BMK) będący specjalizowanym wieloprocesorowym komputerem pracującym pod kontrolą niejawnego systemu operacyjnego czasu rzeczywistego. BMK jest zabezpieczony elektronicznie i mechanicznie przed penetracją i innymi atakami. BMK wyposażony jest w 4 czytniki kart elektronicznych. Dwa z nich służą kartom będącym nośnikami klucza prywatnego UC, który przechowywany jest na nich w taki sposób, że do odtworzenia klucza wewnątrz urządzenia potrzebne są dwie karty włożone jednocześnie do dwóch czytników BMK. Trzeci czytnik jest przeznaczony do współpracy z kartami personelu, w celu jego uwierzytelnienia przed systemem. Zadaniem czwartego czytnika jest personalizacja kart użytkowników systemu. Czytniki skonstruowane i sterowane są w taki sposób, że zabezpieczają karty przed wydaniem osobom nieuprawnionym. Wszystkie operacje istotne z punktu widzenia bezpieczeństwa wykonywane są wewnątrz BMK. Urządzenie prowadzi dwa dobrze strzeżone logi: bezpieczeństwa i aktywności zapewniające rozliczalność działania SZK.

Z BMK współpracuje aplikacja (ASZK) będąca wygodnym interfejsem użytkownika oraz baza danych (BSZK) przechowująca wszystkie niezbędne informacje związane z IKP. Obie działają na standardowym komputerze PC, którego interakcje z otoczeniem powinny być ściśle kontrolowane. Bezpieczeństwo obu tych elementów jest zapewniane przez BMK. Przede wszystkim ASZK i BMK wzajemnie się uwierzytelniają przed sobą. Co więcej kluczowy element ASZK jest pobierany z BMK. Dodatkowo wszystkie polecenia istotne z punktu widzenia bezpieczeństwa systemu potwierdzane są na interfejsie użytkownika (wyświetlacz graficzny + klawiatura) wbudowanym w BMK. Wszystkie rekordy BSZK są podpisane przez BMK. Dodatkowo wrażliwe rekordy są przechowywane wyłącznie w postaci zaszyfrowanej przez BMK i nigdy nie są wydawane w postaci jawnej na zewnątrz. SZK pozwala zdefiniować politykę funkcjonowania UC a także ułatwia i wymusza jej stosowanie, odciążając realizatorów systemu od tworzenia wielu procedur oraz wspomagając operatorów w codziennych działaniach.

Istotną cechą SZK jest możliwość utworzenia wielu sieci przy wykorzystaniu jednego stanowiska SZK, gdyż jedna SZK może kreować dowolnie wiele niezależnych UC z możliwością utworzenia hierarchii pomiędzy nimi. Ograniczeniem jest tu jedynie wielkość pamięci dyskowej współpracującego komputera PC.

Względy bezpieczeństwa, czyli zasada wielu par oczu, oraz wymaganie zapewnienia ciągłości pracy wymagają aby personel obsługujący BMK był dosyć liczny, choć poza operatorami niezbyt obciążony pracą. W jego skład wchodzi kilka osób (od 4 do 8) dysponujących nośnikami zawierającymi elementy składowe klucza prywatnego UC, operator lub operatorzy wykonujący codzienne czynności obsługowe, administrator odpowiedzialny za prawidłowe skonfigurowanie systemu i nadzór nad jego pracą od strony informatycznej oraz inspektor bezpieczeństwa i audytor, których zadaniem jest nadzór nad zachowaniem procedur bezpieczeństwa.

11.6.2 Szyfrujące telefony GSM

TechLab 2000 oferuje dwa różne rozwiązania do zabezpieczenia komunikacji mobilnej:

- Xaos Gamma to telefon o znakomitych parametrach kryptograficznych, dużej wygodzie użytkowania oraz świetnej jakości głosu przeznaczony dla użytkownika biznesowego. Rozwiązanie znajduje się w sprzedaży w Orange.
- Krypton szyfrujący telefon komórkowym przeznaczony dla odbiorcy wymagającego dodatkowych zabezpieczeń. Jego cechą wyróżniającą jest efektywna implementacja infrastruktury klucza publicznego.
- szyfrująca bramka GSM zapewniającą poufną łączność pomiędzy mobilnymi telefonami szyfrującymi a wewnątrzfirmową siecią telefoniczną. Zastosowanie szyfrującej bramki GSM pozwala na oszczędności oraz większy komfort użytkowania w porównaniu z wyposażeniem wszystkich pracowników stacjonarnych w telefony szyfrujące.

Xaos Gamma Xaos Gamma jest szyfrującym aparatem komórkowym przeznaczonym do pracy w standardowej sieci GSM, także w roamingu. Aparat realizuje typowe dla telefonów komórkowych funkcje, a ponadto umożliwia:

- Realizację szyfrowanych połączeń głosowych.
- Szyfrowanie transferu danych.
- Wysyłanie szyfrowanych wiadomości tekstowych (SMS).

Wszystkie funkcje kryptograficzne wkomponowane zostały w standardową funkcjonalność telefonu GSM (połączenia, wiadomości, baza kontaktów, etc.) w sposób naturalny i są proste w użyciu. Cechy wyróżniające telefon to:

- Duża nawiązywania połączenia szyfrowanego: ok. $1.5s$.
- Niewielkie, stałe opóźnienie głosu przy połączeniu szyfrowanym ($450ms$).
- Bardzo silne mechanizmy kryptograficzne, między innymi zastosowanie kryptografii eliptycznej do ustalania kluczy szyfrujących.

Xaos Gamma jest telefonem kierowanym do klienta biznesowego, ceniącego bezpieczeństwo własnych danych, jak również przekazywanych informacji oraz poszukującego rozwiązania dającego gwarancję dobrej jakości połączeń szyfrowanych.

Aparat posiada sprawnie działającą, rozbudowaną bazę kontaktów, uwzględniającą również numery telefonów szyfrujących, zdolną pomieścić do 5000 wpisów. Dzięki silnej integracji funkcji kryptograficznych ze standardową funkcjonalnością aparatu użytkownik, który nie musi posiadać żadnej specjalistycznej wiedzy, otrzymuje wsparcie przy realizacji takich działań jak: wybór pomiędzy połączeniem jawnym lub szyfrowanym, wysyłanie wiadomości tekstowych jawnych lub szyfrowanych, oddzwanianie we właściwym trybie, etc.

Rozwiązanie zostało w całości zaprojektowane w Polsce, gdzie jest również produkowane. Producent oferuje też użytkownikom pełne wsparcie techniczne.

W ramach systemu łączności niejawnej Sylan, Xaos Gamma jest interoperacyjny z innymi rozwiązaniami telekomunikacyjnymi, projektowanymi i produkowanymi przez TechLab 2000, obejmującymi telefony analogowe, cyfrowe, GSM, IP i satelitarne, w tym także z aparatem GSM Krypton przeznaczonym dla administracji państwowej.

Krypton Krypton jest opracowanym i wykonanym w Polsce bezprzewodowym telefonem szyfrującym GSM kierowanym do odbiorców o bardzo wysokich wymaganiach w dziedzinie bezpieczeństwa informacji, jakimi są administracja publiczna, policja, wojsko i inne służby, a także firmy procedujące informację zgodnie z ustawą o ochronie informacji niejawnych.

Krypton zapewnia poufność oraz uwierzytelnienie sesji łączności. Daje możliwość pracy nie tylko w trybie szyfrowym, ale również nawiązuje połączenia z dowolnym innym aparatem telefonicznym w trybie jawnym. Wspiera wszystkie usługi oferowane w polskich sieciach GSM. Może działać w sieciach innych operatorów, również w roamingu, pod warunkiem spełniania przez nich standardu GSM.

W ramach systemu Sylan, Krypton jest interoperacyjny z innymi rozwiązaniami telekomunikacyjnymi, projektowanymi i produkowanymi przez TechLab 2000, obejmującymi telefony analogowe, cyfrowe, GSM, IP i satelitarne. Krypton to trzy urządzenia w jednej obudowie: aparat GSM, telefon szyfrujący, modem (standardowy: EDGE/GPRS, CSD oraz szyfrujący: CSD).

Poza usługą poufności Krypton oferuje automatyczne uwierzytelnienie stron połączenia. Proces uwierzytelnienia odbywa się z wykorzystaniem mechanizmów Infrastruktury Klucza Publicznego. Dzięki specjalnej technologii zabezpieczeń aparat staje się bezpiecznym nośnikiem kluczy użytkownika i współpracuje ze Stacją Zarządzania Kluczami SZK (Teacup).

Do szyfrowania połączenia używany jest algorytm AES oraz algorytm niejawny. Klucz sesyjny generowany jest za pomocą algorytmu Diffie-Hellmana opartego o krzywe eliptyczne. Telefon zapewnia pełne bezpieczeństwo transmisji i przechowywanych danych. Krypton posiada mechanizmy pozwalające na stwierdzenie różnego rodzaju ataków i zagrożeń, oraz zapewnia obronę przed wieloma z nich.

Urządzenie odznacza się prostotą obsługi, a od użytkownika nie wymaga specjalistycznej wiedzy w dziedzinie kryptografii.

Cygnus Titanium Cygnus Titanium jest opracowanym i wykonanym w Polsce aparatem szyfrującym kierowanym do odbiorców o wysokich wymaganiach w dziedzinie zabezpieczeń jak i do zastosowań specjalnych: policja, wojsko. Przeznaczony jest dla użytkowników, którzy chcą chronić przesyłane dane, gdy stanowią one tajemnicę handlową, jak również dla tych którzy działają w myśl ustawy o ochronie informacji niejawnych. Zapewnia poufność oraz uwierzytelnienie sesji łączności do klauzuli *Poufne*. Daje możliwość pracy nie tylko w trybie szyfrowym, ale również nawiązania połączenia z dowolnym innym aparatem telefonicznym w trybie jawnym. Wspiera wszystkie usługi oferowane w polskich sieciach publicznych, a ponadto umożliwia szyfrowane połączenie trójstronne z aparatami analogowymi i cyfrowymi rodziny Cygnus. Przeprowadzone testy potwierdziły jego poprawność pracy także na łączach IP i satelitarnych. Jest interoperacyjny z innymi rozwiązaniami telekomunikacyjnymi projektowanymi

przez TechLab 2000 obejmującymi telefony analogowe, cyfrowe oraz GSM. Proces uwierzytelnienia stron połączenia odbywa się z wykorzystaniem mechanizmów Infrastruktury Klucza Publicznego. Nośnikami danych użytkownika są karty elektroniczne, zaś same dane generowane są przez Stację Zarządzania Kluczami TEACUP. Cygnus Titanium to trzy urządzenia w jednej obudowie: luksusowy aparat ISDN, telefon szyfrujący, modem (standardowy oraz szyfrujący). Urządzenie odznacza się prostota obsługi. Od użytkownika nie wymaga się specjalistycznej wiedzy w dziedzinie kryptografii.

- Urządzenie automatycznie rozpoznaje typ urządzenia zdalnego i w zależności od tego realizuje połączenie jawne lub szyfrowane.
- Wykorzystuje protokół multilink PPP ze statycznym lub dynamicznym przydziałem pasma.
- Realizuje podzbiór standardu V.34 w trybie pracy szyfrowej przy połączeniach z aparatami analogowymi.
- Połączenie z komputerem obywa si za pomocą interfejsu USB 2.0 full-speed. Cygnus Titanium stanowi element systemu łączności niejawnej Sylan, na który składają się również:

  - Stacja zarządzania kluczami TEACUP odpowiedzialna za generację danych w obrębie infrastruktury klucza publicznego.

  - Karty elektroniczne jako nośniki danych użytkownika.

  - Urządzenia końcowe: aparaty analogowe Cygnus Gold, Cygnus Platinum; aparaty cyfrowe Cygnus Diamond, Cygnus Titanium, Cygnus Titanium Plus; aparaty GSM Xaos Gamma, Krypton.

Praca w trybie szyfrowania połączenia

- Podczas nawiązywania połączenia szyfrowanego aparat automatycznie ustala najwyższy możliwy poziom kryptograficzny, na podstawie danych odczytanych z karty użytkownika, lub ewentualnie na podstawie jej braku.
- Połączenie szyfrowane pomiędzy aparatami cyfrowymi nie powoduje utraty jakości głosu (kodowanie transparentne) oraz wyczuwalnego opóźnienia.
- Przy połączeniu z aparatami analogowymi jakość zakodowanego głosu odpowiada technologi wykorzystywanej w sieciach komórkowych.
- Przy połączeniach ustalonych na poziomie *Poufne* stosowany jest niejawny, opracowany przez DBTI ABW, algorytm symetryczny.
- W pozostałych przypadkach szyfrowanie algorytmem symetrycznym AES 256 lub AES 192.
- Uzgadnianie kluczy sesyjnych schematem Diffie-Hellmana do 4096*b*itów.
- Uwierzytelnienie z wykorzystaniem kluczy RSA do 4096*b*itów.
- Umożliwienie przeciwdziałania atakom typu *maskarada*, przy braku danych użytkownika.

- Wysokiej jakości generator losowy oparty na zjawisku fizycznym.
- Nawiązanie połączenia w trybie jawnym, przejście w tryb szyfrowania połączenia przez naciśniecie jednego przycisku, czas przejścia od 0,5 do kilku sekund w zależności od rodzaju połączenia oraz typu uwierzytelnienia (np: Diffie-Hellman 3072 bity, dane użytkownika 2048 podpisane kluczem 4096, całkowity czas nawiązywania sesji szyfrowanej 3 sekundy).
- Automatyczna propagacja list unieważnionych certyfikatów (CRL).
- Informacja akustyczna i wizualna o procesie uwierzytelnienia oraz przejściu w tryb pracy niejawnej.
- Zaimplementowane mechanizmy zabezpieczeń antyemisyjnych oraz antypenetracyjnych.

Rozdział 12

Sieci komputerowe

Przesyłanie informacji w sieci komputerowej obarczone jest ryzykiem. Zagrożenia mogą się pojawić z przyczyn losowych (np. zmiana zawartości wiadomości w wyniku błędów w czasie transmisji) lub mogą być związane z celową akcją ze strony intruza. Celowa akcja intruza może mieć charakter podsłuchu pasywnego, kiedy intruz ma możliwość jedynie poznania treści przesyłanych wiadomości lub stwierdzenia faktu przepływu wiadomości, lub podsłuchu aktywnego, kiedy ma on również możliwość ingerencji w przesyłane wiadomości - w ich zawartość lub kolejność.

W celu zapobieżenia pojawiającym się zagrożeniom konieczna jest realizacja podstawowych usług ochrony informacji. W tab. 12.1 zestawiono typowe zagrożenia dla wiadomości przesyłanych w sieci, oraz usługi, które przed tymi zagrożeniami chronią.

Poniżej przedstawiono grupę podstawowych usług służących do ochrony informacji w sieciach teleinformatycznych i omówiono skrótowo podstawowe metody realizacji poszczególnych usług.

Integralność zawartości wiadomości Integralność zawartości wiadomości (*ang. message content integrity*) zapewnia możliwość sprawdzenia tego, czy przesyłane dane nie zostały w żaden sposób zmodyfikowane podczas transmisji. Jest ona osiągana poprzez dołączenie do wiadomości znacznika integralności wiadomości (*ang. Message Integrity Code, Modification Detection Code*). Znacznik ten jest ciągiem bitów obliczonym na podstawie wiadomości.

Integralność sekwencji wiadomości Integralność sekwencji wiadomości (*ang. message sequence integrity*) chroni przed przechwyceniem i opóźnionym przesłaniem wiadomości, zmianą kolejności wiadomości oraz przed powieleniem, dodaniem lub usunięciem wiadomości. W celu wykrycia utraty wiadomości lub zmiany kolejności wiadomości:

- nadawca zawiera w wiadomości, a odbiorca sprawdza, numer sekwencyjny wiadomości (*ang. message sequence number*), związany z przepływem komunikatów pomiędzy nadawcą i odbiorcą;
- nadawca może również zażądać potwierdzenia otrzymania wiadomości przez odbiorcę.

Tab. 12.1: Zestawienie zagrożeń i usług chroniących przed zagrożeniami dla informacji w sieciach teleinformatycznych.

Usługa/Zagrożenie	integralność zawartości	integralność sekwencji	uwierzytelnienie nadawcy	niezaprzeczalność nadania	poufność zawartości
Nieuprawniony odczyt zawartości wiadomości					X
Wprowadzenie do sieci fałszywych wiadomości			X		
Modyfikacja zawartości wiadomości	X				
Powielenie wiadomości lub jej przejęcie i opóźniona transmisja		X			
Skasowanie wiadomości		X			
Skasowanie wiadomości Zaprzeczenie wysłania wiadomości				X	

W celu wykrycia dodanych, powielonych lub przechwyconych i przesłanych z opóźnieniem wiadomości:

- nadawca zawiera w wiadomości, a odbiorca sprawdza numer sekwencyjny komunikatu;
- nadawca zawiera w wiadomości, a odbiorca sprawdza znacznik czasu (*ang. timestamp*).

W celu zapewnienia pełnej ochrony, integralność numeru sekwencyjnego wiadomości oraz znacznika czasu muszą być zagwarantowane przy użyciu usługi integralności zawartości wiadomości lub jednej z usług omówionych poniżej.

Uwierzytelnienie nadawcy wiadomości Uwierzytelnienie nadawcy (*ang. message origin authentication*) zapewnia możliwość sprawdzenia czy nadawca wiadomości jest tym użytkownikiem sieci, za którego się podaje. Uwierzytelnienie nadawcy może być osiągnięte poprzez dołączenie przez nadawcę do wiadomości tzw. znacznika uwierzytelnienia wiadomości (*ang. MAC - message authentication code*). Wartość znacznika jest funkcją wiadomości oraz tajnego klucza. Klucz nie jest znany żadnemu użytkownikowi sieci poza nadawcą i odbiorcą wiadomości.

Poufność zawartości wiadomości Poufność (*ang. confidentiality of content*) polega na takim przekształceniu przesyłanych danych, by były one niemożliwe do odczytania przez żadną inną osobę poza właściwym odbiorcą wiadomości. Usługa ta może być osiągnięta przez zaszyfrowanie zawartości wiadomości.

Niezaprzeczalność nadania wiadomości Niezaprzeczalność nadania wiadomości (*ang. non-repudiation of message origin*) chroni przed możliwością wyparcia się przez nadawcę faktu wysłania określonej wiadomości. Usługa ta dostarcza osobie trzeciej (arbitrowi) dowodu co do integralności zawartości wiadomości oraz co do autentyczności nadawcy wiadomości. Usługa niezaprzeczalności zabezpiecza m.in. przed próbą zmiany treści wiadomości (w szczególności części umowy lub zlecenia bankowego) przez nadawcę lub odbiorcę i przedstawienia takiej wiadomości w sądzie jako autentycznej. Usługa niezaprzeczalności realizowana jest poprzez wykorzystanie idei podpisu cyfrowego. Podpis cyfrowy jest ciągiem bitów (zazwyczaj krótszym od wiadomości, którą reprezentuje) będącym funkcją:

- podpisywanej wiadomości,
- tajnej informacji znanej tylko autorowi podpisu (tzw. klucza prywatnego nadawcy).

Podpis cyfrowy może być weryfikowany przy użyciu publicznie znanej informacji (tzw. klucza publicznego nadawcy), odpowiadającej tajnej informacji użytej podczas generowania podpisu.

Podpis cyfrowy pełni funkcje analogiczne do funkcji podpisu ręcznego tj.:

- identyfikuje osobę podpisującą,
- stanowi dowód akceptacji treści podpisywanego dokumentu, oraz zgody na ponoszenie konsekwencji prawnych, które z tej akceptacji mogą wynikać.

W tab. 12.2 zawiera zestawienie cech wspólnych oraz różnic pomiędzy podpisem ręcznym i podpisem cyfrowym. Warto zauważyć, że istotną różnicą jest to, że podpis cyfrowy nie jest taki sam dla wszystkich dokumentów, lecz zmienia się wraz z dokumentem, którego dotyczy. Usługa niezaprzeczalności stanowi rozszerzenie usługi uwierzytelnienia nadawcy o możliwość autentyczności komunikatu przez osobę trzecią, różną od nadawcy i odbiorcy.

Niezaprzeczalność odbioru wiadomości Niezaprzeczalność odbioru wiadomości (*ang. non-repudiation of message receipt*) chroni nadawcę komunikatu przed wyparciem się przez odbiorcę faktu odebrania komunikatu. Realizacja usługi polega na wysłaniu przez odbiorcę potwierdzenia odebrania wiadomości zawierającej podpis cyfrowy odbiorcy, będący funkcją oryginalnej wiadomości.

Tab. 12.2: Porównanie podpisu ręcznego i podpisu cyfrowego.

Podpis ręczny	Podpis cyfrowy
Cechy wspólne	
Przypisany jednej osobie.	
Niemożliwy do podrobienia.	
Uniemożliwiający wyparcie się go przez autora.	
Łatwy do weryfikacji przez osobę niezależną.	
Łatwy do wygenerowania.	
Różnice	
Związany nierozłącznie z dokumentem.	Taki sam dla wszystkich dokumentów.
Stawiany na ostatniej stronie dokumentu	Może być składowany i transmitowany niezależnie od dokumentu.
Jest funkcją dokumentu.	Obejmuje cały dokument

Związki pomiędzy usługami ochrony informacji Część usług, ze swej natury, zawiera w sobie inne, prostsze usługi. W tab. 12.3 zamieszczono zestawienie relacji pomiędzy wybranymi usługami. Najbardziej podstawową usługą jest usługa integralności. Uwierzytelnienie zapewnia integralność, a dodatkowo daje odbiorcy pewność, że wiadomość pochodzi od określonego nadawcy. Niezaprzeczalność zapewnia wszystko to, co daje uwierzytelnienie, a dodatkowo chroni przed możliwością wyparcia się przez nadawcę faktu wysłania określonej wiadomości (ewentualny spór pomiędzy nadawcą i odbiorcą może być rozstrzygnięty przez osobę trzecią - arbitra).

Tab. 12.3: Związki pomiędzy usługami ochrony informacji.

Zawiera Usługa	integralność zawartości	uwierzytelnienie nadawcy	niezaprzeczalność nadania	poufność zawartości
integralność zawartości	x			
uwierzytelnienie nadawcy	x	x		
niezaprzeczalność nadania	x	x	x	
poufność zawartości				x

12.1 Zagrożenia ze strony sieci

Internet, stanowiąc sieć globalną, pozwala na połączenie ogromnej ilości komputerów na całym świecie, które jednocześnie stanowią potencjalny przedmiot

ataków.

Internet nie jest kontrolowany odgórnie, z różnorodnymi regulacjami prawnymi wewnątrz danego państwa (co stanowi szczególny absurd biorąc pod uwagę brak granic sieci) i niezestandaryzowaną polityką, jest wyjątkowo trudna w dochodzeniu i ściganiu przestępców.

Uwzględniając dodatkowo słabości wynikające z istniejących i wciąż powstających (przy stałym i dynamicznym rozwoju technologicznym) luk w systemach operacyjnych oraz protokołu można stwierdzić, że:

Internet jest najgroźniejszym z możliwych źródeł niebezpieczeństw dla systemu komputerowego.

Klasy zagrożeń ze strony Internetu obejmują:

- Uzyskanie dostępu do danych przesyłanych przez sieć lub przechowywanych w komputerach przez osoby niepowołane
- Uzyskanie dostępu do innych zasobów przez osoby niepowołane
- Utrata danych na skutek działań z zewnątrz, fałszerstwo danych
- Uniemożliwienie korzystania z pewnych usług/zasobów przez legalnych użytkowników

12.1.1 Programy w sieci, które zagrażają systemowi komputerowemu

Korzystanie z zasobów Internetu to ciągły proces obustronnego transferu plików. W przypadku ściągania pliku niepewnego pochodzenia często zdarza się, iż zawiera on dodatkowe podprogramy, pozwalające na swobodny dostęp do zasobów komputera lub jego zniszczenie. Programy te mają swoją specyfikę i dlatego też zostały pogrupowane. Poniżej wymieniono najważniejsze grupy.

- robak (worm) - powiela się na komputerach w całej sieci. Wiele kopii tego samego programu powoduje przepełnienie pamięci, a w efekcie - dezorganizację pracy całego systemu,
- wirus - najczęściej jest przenoszony przez różne aplikacje lub pliki. Jest nieszkodliwy, póki nie zostanie uruchomiony (do tego czasu pozostaje w ukryciu). Po aktywacji atakuje system osłabiając go. Obecnie są całe setki wirusów, od prawie niegroźnych (ograniczających się do wypisywania głupawych komunikatów na ekranie), do bardzo niebezpiecznych, które zniekształcają całe programy,
- koń trojański - stwarza wrażenie użytecznego programu, będąc w rzeczywistości pułapką. Uruchamiany przez pewne dane lub kluczowe słowo, służy włamywaczowi do zdobywania określonych informacji,
- bomba logiczna - podprogram, który uruchamia się w pewnym określonym czasie (jakim jest np. data lub słowo) i atakuje system, dokonując zniszczeń,
- wrogi applet Java - program napisany w języku Java, który jest podstawowym narzędziem programowania w Internecie, może zawierać w sobie podprogram o działaniu podobnym do konia trojańskiego.

Szczegółowe omówienie zagadnienia można znaleźć w rozdziale 5.

Na rynku dostępnych jest szereg programów umożliwiających diagnostykę i skanowanie sieci pod względem bezpieczeństwa. Większość tego typu oprogramowania działa w systemie Linux i jest darmowa (rozprowadzana na licencji GNU lub GPL.

Można wymienić kilka grup popularnych programów:

- Oprogramowanie sieciowe: tcpdump, wireshark, hping, scapy!
- Skanery: nmap, amap, nikto, iWar, etc.
- Skanery podatności: Nessus (+pluginy), OpenVAS,
- Exploity (dostępne publicznie, czasem kodowane ad-hoc),
- Frameworki: Metasploit, Netifera, Inguma, FastTrack
- Środowiska: BackTarck, Operator, PHLACK, Auditor.

W dalszej częsci omówiono wybrane programy.

12.2 Skanowanie sieci, portów - Linux

W rozdziale omówiono oprogramowanie do skanowania sieci. Skanowanie sieci jest podstawową techniką zbierania informacji o sieci oraz komputerach i usługach świadczonych w sieciach. Skanowanie sieci umożliwia:

- wykrywanie aktywnych hosty,
- wykrywanie rodzaju systemu operacyjnego hosta,
- wykrywanie usług (numery otwartych portów),
- testowanie poszczególnych usług.

Roodzaje skanowania portów Wyróżnia się kilka rodzajów skanowania portów. Niektóre rodzaje pozostawiają ślad w logach systemowych serwerów.

- połączenie TCP (TCP connect scan) - najbardziej podstawowa forma skanowania TCP; polega na połączeniu z wybranym portem i przeprowadzeniu pełnego trójstronnego powitania (SYN, SYN/ACK i ACK); jeżeli port nasłuchuje połączenie powiedzie się, w przeciwnym razie port nie jest dostępny; metoda ta jest łatwa do wykrycia ponieważ w logach celu znajdować się będzie wiele informacji o błędach spowodowanych przez połączenia z usługami, które są następnie od razu przerywane; W celu połączenia TCP nie potrzebne są uprawnienia root'a.
- TCP SYN - ta technika jest często nazywana skanowaniem półotwartym (*ang. half-open scanning*) ponieważ nie jest nawiązywane pełne połączenie TCP, lecz do wybranego portu przesyłany jest pakiet SYN tak jak w przypadku prawdziwego połączenia i następuje oczekiwanie na odpowiedź; Jeśli port odpowie sygnałem SYN/ACK to oznacza, że port nasłuchuje; natomiast odpowiedź RST/ACK oznacza zazwyczaj, że port nie

nasłuchuje; Komputer przeprowadzający skanowanie przesyła następnie sygnał RST/ACK, dzięki czemu połączenie nie jest nawiązane i może nie zostać odnotowane w logach celu. Do zbudowania pakietu SYN niezbędne są uprawnienia root'a.

- TCP FIN - polega na przesłaniu do wybranego portu pakietu FIN, cel powinien odpowiedzieć pakietem RST dla wszystkich zamkniętych portów.
- TCP Xmas Tree - polega na przesłaniu do wybranego portu pakietów FIN, URG i PUSH; cel powinien odpowiedzieć pakietem RST dla wszystkich zamkniętych portów.
- TCP Null - technika ta wyłącza wszystkie flagi; cel powinien odpowiedzieć pakietem RST dla wszystkich zamkniętych portów.
- TCP ACK - technika używana do kontroli działania zapory ogniowej; pozwala na określenie czy zapora ogniowa celu to tylko prosty filtr pakietów, dopuszczający jedynie nawiązane połączenia (połączenia z ustawionym bitem ACK), czy też może jest to zaawansowana zapora przeprowadzająca rozbudowane filtrowanie pakietów.
- UDP - technika wykorzystywana do ustalenia które porty UDP (*ang. User Datagram Protokol*) są otwarte na hoście; polega na przesłaniu pakietu UDP do wybranego portu. Jeśli wybrany port odpowie komunikatem *ICMP port unrechable*, to oznacza że jest on zamknięty; w przeciwnym razie można wnioskować, że port jest otwarty lub Firewall zablokował komunikację.

12.2.1 nmap

Nmap jest jednym z najbardziej rozpowszechnionych programów do skanowania sieci. Posiada duże możliwości i wiele opcji. Z programem rozprowadzana jest szczegółowa dokumentacja. Program działa przede wszystkim w środowisku Unix/Linux. Jest uruchamiany z linii komendy.

Nmap poza informacjami na temat uruchomionych usług, ich wersji oraz systemu operacyjnego nie pozwala na dokładniejsze zbadanie zdalnej aplikacji. Największy poziom szczegółowości można uzyskać za pomocą opcji *-sV*, np.:

```
nmap aiva.pl -P0 -sV -p 80

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-07 14:55 CEST
Nmap scan report for aiva.pl (192.168.2.101)
Host is up (0.0013s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
MAC Address: 00:08:C7:1E:92:8D (Hewlett-Packard Company)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.07 seconds
```

W przypadku testowanego serwera apache2 istnieje możliwość wyłączenia przedstawiania się w sieci, za pomocą parametru *ServerSignature Off.* ustawionym w głównym pliku konfiguracyjnym */etc/apache2/httpd.conf.*

Poniżej omówiono różne rodzaje skanowania za pomocą programu nmap.

Skanowanie typu TCP CONNECT Skanowanie typu *TCP CONNECT* - to najbardziej podstawowa technika. Polega na przeprowadzeniu pełnego połączenia TCP z danym portem. Podczas uzgadniania połączenia (SYN, SYN/ACK i ACK) żaden komputer pracujący w sieci nie może ignorować pakietów TCP/SYN. Jeśli więc dany port jest otwarty i otrzyma od pakiet TCP z ustawioną flagą SYN, odpowie pakietem SYN/ACK. Jeśli jest zamknięty odpowie RST/ACK. Metoda ta jest łatwa do wykrycia, gdyż nawiązywane jest próba faktycznego połączeń z usługami. W logach serwera, z którym następuje połączenie zostaną zapisane odpowiednie informacje o połączeniu. W celu przeprowadzenia skanowania TCP CONNECT za pomocą nmapa należy użyć opcji *-sT*:

```
nmap -sT adres_ip
```

Skanowanie typu TCP SYN Skanowanie TCP SYN polega na wysłaniu pakietu z ustawioną flagą SYN. Pełne połączenie nie jest jednak nawiązywane. Zdalny host odpowie SYN/ACK (port otwarty), natomiast intruz nigdy nie wyśle ACK. W logach typowych zapór ogniowych (firewall) nie będzie śladów połączenia. W celu wykonania tege typu skanowania należy użyć opcji *-sS*:

```
nmap -sS adres_ip
```

Skanowanie typu TCP FIN Skanowanie typu TCP FIN polega na przesłaniu do zdalnego portu pakietu z flagą FIN (kończy uzgadnianie połączenia). Zdalny host powinien odpowiedzieć pakietem RST jeśli port jest zamknięty. Jest to skanowanie ukryte, które można przeprowadzić z użyciem opcji *-sF*:

```
nmap -sF adres_ip
```

Skanowanie typu TCP ACK Skanowanie typu TCP ACK jest skanowanie metodą ukrytą. Jest stosunkowa. Polega na wysłaniu od razu pakietu z flagą ACK (z pominięciem wymaganych SYN i SYN/ACK). W tym przypadku wartość ACK jest sfałszowana, gdyż połączenia nigdy nie zostało nawiązane. Port zamknięty odpowie flagą RST, natomiast port otwarty wcale nie odpowie. W celu przeprowadzenia tego typu skanowania należy użyć flagi *-sA*:

```
nmap -sA adres_ip
```

Skanowanie typu TCP NULL Skanowanie TCP NULL polega na wysłaniu do zdalnego hosta pakietów bez żadnej flagi (SYN, SYN/ACKm FIN). Port otwarty nie odpowie, natomiast port zamknięty odpowie pakietem z flagą RST. Skanowanie tego typu wykonywane jest z flagą *-sN*:

```
nmap -sN adres_ip
```

Przykład skanowania Poniżej przedstawiono przykładowe skanowanie portów serwera za pomocą polecenia nmap.

```
nmap -sF aiva.pl

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-07 17:51 CEST
Nmap scan report for aiva.pl (192.168.2.101)
Host is up (0.0010s latency).
Not shown: 978 closed ports
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
88/tcp   open|filtered kerberos-sec
110/tcp  open|filtered pop3
135/tcp  open|filtered msrpc
139/tcp  open|filtered netbios-ssn
143/tcp  open|filtered imap
389/tcp  open|filtered ldap
443/tcp  open|filtered https
445/tcp  open|filtered microsoft-ds
464/tcp  open|filtered kpasswd5
465/tcp  open|filtered smtps
636/tcp  open|filtered ldapssl
749/tcp  open|filtered kerberos-adm
993/tcp  open|filtered imaps
995/tcp  open|filtered pop3s
1024/tcp open|filtered kdm
3268/tcp open|filtered globalcatLDAP
3269/tcp open|filtered globalcatLDAPssl
3389/tcp open|filtered ms-wbt-server
MAC Address: 00:08:C7:1E:92:8D (Hewlett-Packard Company)

Nmap done: 1 IP address (1 host up) scanned in 96.44 seconds
```

Wykrywanie systemu operacyjnego Program nmap pozwala na zdalne wykrycie systemu operacyjnego. Służy do tego opcja *-O*. Przykładowy wynik działania takiego skanu przedstawiono poniżej.

```
nmap -O aiva.pl

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-07 10:29 CEST
Nmap scan report for aiva.pl (192.168.2.101)
Host is up (0.0019s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
143/tcp  open  imap
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
465/tcp  open  smtps
636/tcp  open  ldapssl
749/tcp  open  kerberos-adm
993/tcp  open  imaps
995/tcp  open  pop3s
1024/tcp open  kdm
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:08:C7:1E:92:8D (Hewlett-Packard Company)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
```

```
OS details: Linux 3.11 - 3.14
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.86 seconds
```

12.2.2 Wykrywanie prób skanowania

Istnieją metody wykrywania skanowania. Można to zrealizować za pomocą modyfikacji reguł *iptables*.

Wykrywanie skanowanie typu TCP SYN Poniższa modyfikacja reguł umożliwia wykrywanie prób skanowania typu TCP SYN i zapisanie odpowiedniej informacji w logu.

```
iptables -A INPUT -m conntrack -cstate NEW -p tcp -tcp-flags
  SYN,RST,ACK,FIN,URG,PSH SYN -j LOG -log-level info -log-prefix "LOG:␣
      ↪ skanowanie␣TCP␣SYN"
```

Opcja *conntrack* oznacza, że śledzone są połączenia przychodzące.

Wykrywanie skanowanie typu TCP FIN Dla odmiany logowanie skanów typu TCP FIN np. wymaga analogicznej regułki:

```
iptables -A INPUT -m conntrack -cstate NEW -p tcp
 -tcp-flags SYN,RST,ACK,FIN,URG,PSH FIN -j LOG -log-level info -log-prefix
"LOG:␣skanowanie␣TCP␣FIN"
```

Połączenia typu TCP FIN można blokować, jeżeli serwer nie udostępnia żadnych usług, Odpowiednia reguła wygląda następująco:

```
iptables -A INPUT -m conntrack -cstate NEW -p tcp -tcp-flags SYN,RST,ACK,FIN,
    ↪ URG,PSH SYN -j DROP
```

Wykrywanie skanowanie typu TCP NULL Skanowanie pakietów typu TCP NULL jest wykonywane za pomocą opcji INVALID, która poinformuje iptables, że pakiet nie należy do żadnego prawidłowo nawiązanego połączenia:

```
iptables -A INPUT -m conntrack -cstate INVALID -p tcp -tcp-flags
     ! SYN,RST,ACK,FIN,URG,PSH SYN,RST,ACK,FIN,URG,PSH -j LOG -log-level info
-log-prefix "LOG:␣skanowanie␣TCP␣NULL!"
```

12.2.3 netperfmeter

Oprogramowanie służy do sprawdzania szybkości transmisji portów. Instalację oprogramowania można przeprowadzić za pomocą komendy:

```
apt-get install netperfmeter
```

Przykład użycia programu dla interfejsu eth1 serwera przedstawiono poniżej.

```
netperfmeter -runtime=5 192.168.0.111

Network Performance Meter - Version 1.0
----------------------------------------

Active Mode:
```

```
- Measurement ID  = e268cd05
- Remote Address  = 192.168.0.111:9000
- Control Address = 192.168.0.111:9001 - connecting
```

12.2.4 netdiscover

Program służy do rekonesansu sieci, pierwotnie stworzony do zbierania informacji w sieciach bezprzewodowych. Program przeszukuje sieci w poszukiwaniu hostów przez wysyłanie do nich zapytań ARP. Instalację oprogramowania można przeprowadzić za pomocą komendy:

```
apt-get install netdiscover
```

Przykład pracy programu przedstawiono poniżej. Program skanuje adresy w sieci lokalnej (*-r 192.168.2.0/24*), podaje adres MAC oraz inne informacje.

```
netdiscover -r 192.168.2.0/24

Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
_____________________________________________________________________________
IP            At MAC Address      Count  Len   MAC Vendor
-----------------------------------------------------------------------------
192.168.2.100   f8:d2:13:96:46:99    01    060   Unknown vendor
```

12.2.5 netstat

Program służy m.in. do wyświetlania połączeń sieciowych, tablic trasowania, statystyk interfejsu sieciowego, połączeń maskaradowych. Program obsługuje IPv4 i IPv6. Instalację oprogramowania można przeprowadzić za pomocą komendy:

```
apt-get install netdiscover
```

Przykład użycia programu podano poniżej. Opcja -r umożliwia wyświetlenie tablic trasowania (routingu).

```
netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         192.168.2.101   0.0.0.0         UG        0 0          0 wlan0
192.168.2.0     *               255.255.255.0   U         0 0          0 wlan0
```

Program posiada wiele opcji. Umożliwia szczegółową analizę pracy połączeń sieciowych (opcja *-i*) jak pokazano na wydruku poniżej.

```
netstat  -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500 0  58475251    261      0 0      89573052     23      0      0
     ↪ BMRU
eth1       1500 0  89980150      0      1 0      58904556      0      0      0
     ↪ BMRU
lo        65536 0    906419      0      0 0        906419      0      0      0
     ↪ LRU
tun0       1500 0         0      0      0 0             0      0      0      0
     ↪ MOPRU
```

12.2.6 netcat

Prosty i szeroko używany program do skanowania portów używany przez inne programy.

```
apt-get install netcat
```

Przykład skanowania portów 1-1023 serwera localhost.

```
nc -zv localhost 1-1023
localhost [192.168.2.101] 995 (pop3s) open
localhost [192.168.2.101] 993 (imaps) open
localhost [192.168.2.101] 636 (ldaps) open
localhost [192.168.2.101] 465 (ssmtp) open
localhost [192.168.2.101] 464 (kpasswd) open
localhost [192.168.2.101] 445 (microsoft-ds) open
localhost [192.168.2.101] 443 (https) open
localhost [192.168.2.101] 389 (ldap) open
localhost [192.168.2.101] 143 (imap2) open
localhost [192.168.2.101] 139 (netbios-ssn) open
localhost [192.168.2.101] 135 (loc-srv) open
localhost [192.168.2.101] 110 (pop3) open
localhost [192.168.2.101] 88 (kerberos) open
localhost [192.168.2.101] 80 (http) open
localhost [192.168.2.101] 53 (domain) open
localhost [192.168.2.101] 25 (smtp) open
localhost [192.168.2.101] 22 (ssh) open
```

Obecnie dostępna jest wersja programu obsługująca protokół IPv6 (*netcat6*).

12.2.7 wireshark

Wireshark jest programem typu sniffer, który umożliwia przechwytywanie i zgrywanie pakietów danych, a także ich dekodowanie. Posiada szereg wtyczek, dzięki którym może rozpoznawać i analizować różne protokoły komunikacyjne. Głównie wykorzystywany jest przez administratorów sieci, służby specjalne oraz hackerów do śledzenia pakietów. Program posiada graficzny interfejs użytkownika, co jest jego wielką zaletą. Instalację oprogramowania można wykonać komendą:

```
apt-get install wireshark
```

Na rys. 12.1 przedstawiono różne aspekty działania programu Wireshark.

Rys. 12.1: Wireshark.

12.3 Firewall

Firewall to zapora pomiędzy siecią wewnętrzną organizacji a dowolną siecią zewnętrzną (Internet, WAN Wide Area Network) albo pomiędzy działami firmy sieci lokalnej (Intranet, LAN Local Area Network)

Firewalle to oprogramowaniem instalowane na komputerze, który ma oddzielać sieć wewnętrzną od zewnętrznej.

Zadaniem ściany ogniowej jest chronić sieć wewnętrzną przed dostępem osób niepowołanych z sieci zewnętrznej.

Firewall filtruje przychodzące i wychodzące dane, zapewnia dostęp do określonych usług internetowych i odrzuca usługi nie dopuszczone przez administratora. Zapisuje także zdarzenia związane z ruchem w sieci i alarmuje podczas prób włamania do systemu.

W systemie Linux zadania ściany ognia realizuje program iptables. Poniżej przedstawiono przykładowy plik tworzący reguły filtrowania pomiędzy dwoma interfejsami sieciowymi i włączający *ang. masquarade*.

```
#!/bin/sh
#

# echo "/etc/init.d/firewall is OFF"
# exit 0

# czyszczenie starych regul
iptables -F
iptables -X
iptables -t nat -X
iptables -t nat -F
iptables -t mangle -F
iptables -t mangle -X


# ustawienie domyslnej polityki
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Always accept loopback traffic
iptables -A INPUT -i lo -j ACCEPT

# Allow established connections, and those not coming from the outside
iptables -A INPUT   -j ACCEPT -m state --state ESTABLISHED,RELATED
iptables -A FORWARD -j ACCEPT -m state --state ESTABLISHED,RELATED
iptables -A OUTPUT  -j ACCEPT -m state --state ESTABLISHED,RELATED

# ethZ1 interface eth1 - internet eth0 - LAN
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
# Don't forward from the outside to the inside.
iptables -A FORWARD -i eth1 -o eth1 -j REJECT

# dodane 20160907 - ochrona przed spamem 1msg na polaczenie, 6pol/minute
iptables -A INPUT -p tcp --dport 25 -m state --state NEW -m recent --set
iptables -A INPUT -p tcp --dport 25 -m state --state NEW -m recent --update
         --seconds 60 --hitcount 6 -j DROP

# PLAY modem
# iptables -t nat -A POSTROUTING -o wwan0 -j MASQUERADE
# Don't forward from the outside to the inside.
# iptables -A FORWARD -i wwan0 -o wwan0 -j REJECT

#iptables -A FORWARD -i eth0 -s 192.168.0.0/24 -j ACCEPT

# Masquerade.
# iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -d 0.0.0.0/0 -j MASQUERADE


# wlaczenie w kernelu forwardowania
echo 1 > /proc/sys/net/ipv4/ip_forward
```

12.4 Tor - sieć anonimowa

Tor (*ang. The Onion Route*) to wirtualna sieć komputerowa implementująca trasowanie cebulowe drugiej generacji. Sieć zapobiega analizie ruchu sieciowego i w konsekwencji zapewnia użytkownikom prawie anonimowy dostęp do zasobów Internetu. Podobnie jak sieci Freenet, GNUnet czy MUTE, Tor może być wyko-

rzystywany w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych.

Tor chroni tożsamość użytkowników oraz ich działalność w sieci przed analizą ruchu. Operatorzy utrzymują wirtualną sieć złożoną z ruterów cebulowych, zapewniającą anonimowość zarówno w sensie ukrycia lokalizacji użytkownika, jak też możliwości udostępniania anonimowych ukrytych usług.

Wykorzystuje kryptografię, wielowarstwowo szyfrując przesyłane komunikaty (*trasowanie cebulowe*), zapewniając w ten sposób poufność przesyłania danych pomiędzy ruterami. Użytkownik musi mieć uruchomiony na swoim komputerze program, który łączy się z serwerem pośredniczącym sieci Tor. Takie serwery, zwane węzłami, może uruchomić u siebie każdy, kto chce wspomóc rozwój Tora. Oprogramowanie łączące się z internetem może korzystać z Tora poprzez interfejs SOCKS.

Tor nie oferuje całkowitej anonimowości i przy założeniu dostępu do odpowiednio dużych środków technicznych możliwe jest wytropienie danego użytkownika tej sieci. Tor nie może i nie próbuje chronić przed monitorowaniem ruchu na granicach sieci, tzn. pakietów wchodzących i opuszczających sieć. Na przykład rząd Stanów Zjednoczonych ma możliwość monitorowania dowolnego szerokopasmowego połączenia z Internetem dzięki urządzeniom wprowadzonym na podstawie Communications Assistance for Law Enforcement Act (CALEA) i dlatego może kontrolować oba punkty końcowe połączeń Tora, wykonywanych na terytorium USA. O ile Tor chroni przed analizą ruchu, nie może zapobiec potwierdzeniu komunikacji.

Wycieki zapytań DNS Podobnie jak w przypadku wielu innych systemów do anonimowego surfowania po internecie, część aplikacji nadal wykonuje bezpośrednie zapytania do serwerów Od wersji 0.2.0.1-alpha, Tor ma wbudowany własny resolver DNS, który przekierowuje zapytania przez sieć Tor, co powinno rozwiązać problem wycieków DNS, jak też umożliwić aplikacjom nieposługującym się protokołem SOCKS korzystanie z ukrytych usług.

Analiza ruchu Jak wszystkie współczesne sieci anonimowe z niewielkimi opóźnieniami (*ang. low latency*), Tor jest podatny na analizę ruchu przez adwersarzy, którzy mogą obserwować oba końce połączenia użytkownika[16].

Podsłuchiwanie przez węzły wyjściowe We wrześniu 2007 r. ujawniono, że monitorując założone przez siebie węzły wyjściowe sieci Tor można przechwycić nazwy użytkowników i hasła do dużej liczby kont pocztowych. Tor nie może i nie szyfruje danych przesyłanych pomiędzy węzłem wyjściowym a serwerem docelowym, dlatego każdy węzeł wyjściowy ma potencjalną możliwość przechwycenia dowolnych danych, które przezeń są przesyłane, a nie są zabezpieczone poprzez na przykład szyfrowanie SSL.

Bibliografia

[1] Brandm, Sheila (editor): *Trusted computer system evaluation criteria*. Department of defense standard, Dec 1985, ISBN 978-0788143250. 43

[2] CSC: *The Green Books*. Department of Trade and Industry Commercial Computer Security Centre, Great Britain, 1989.

[3] *Comp*, 2017. http://www.comp.com.pl/.

[4] *Enigma systemy ochrony informacji sp. z o.o.*, 2017. http://www.enigma.com.pl/.

[5] *Techlab 2000 r& d company*, 2017. http://www.tl2000.pl/.

[6] *Google public dns/security*. Google developers Web page. https://developers.google.com/speed/public-dns/docs/security. 83

[7] ITISEC: *Information Technology Security Evaluation Criteria*. Department of Trade and Industry Commercial Computer Security Centre, Harmonised Criteria of France, Germany, Netherlands, UK, 1991. 43

[8] Liderman, K.: *Podstawowe twierdzenie bezpieczeństwa*. Biuletyn Wojskowej Akademii Technicznej, 60(4):315–329, 2011.

[9] Liderman, K. (editor): *Bezpieczeństwo informacyjne*. Wydawnictwo Naukowe PWN, 2013.

[10] *Pem*, 2016. https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail.

[11] Plaskura, P.: *System operacyjny Linux*. AIVA, Piotrków Trybunalski, 2016, ISBN 978-83-937245-2-9. http://epub.aiva.pl/?isbn=978-83-937245-2-9. 86

[12] Schneier, B.: *Kryptografia dla praktyków: protokoły, algorytmy i programy źródłowe w języku C*. Wydawnictwa Naukowo-Techniczne, 2002, ISBN 83-204-2678-2. 107

[13] Stallings, W. (editor): *Kryptografia i bezpieczeństwo sieci komputerowych*. Helion, 2012.

[14] *X.509*, 2016.

Spis tablic

Spis rysunków

Słownik

3DES algorytm szyfrowania symetrycznego polegający na trzykrotnym użyciu algorytmu DES: szyfrowanie 1 kluczem, deszyfrowanie 2 kluczem, szyfrowanie 3 kluczem. https://pl.wikipedia.org/wiki/3DES . 108, 112, 120, 122

ABI Administrator bezpieczeństwa informacji . 12

ACL *ang. Access Control List* - listy kontroli dostępu w systemach komputerowych, które przypisują odpowiednim obiektom prawa dostępu. Więcej informacji pod adresem http://en.wikipedia.org/wiki/Access_control_lista. . 86, 182

AES *ang. Advanced Encryption Standard* - symetryczny szyfr blokowy przyjęty przez NIST jako standard FIPS-197 w wyniku konkursu ogłoszonego w roku 1997, który wygrał algorytm nazywany roboczo Rijndael. . 100, 101, 122, 126, 182, 193, 194

ARP Adress Resolution Protocol (ARP) to protokół sieciowy umożliwiający mapowanie logicznych adresów warstwy sieciowej na fizyczne adresy warstwy łącza danych. Protokół ten nie ogranicza się tylko do konwersji adresów IP na adres MAC stosowany w sieciach Ethernet. Jest także wykorzystywany do odpytywania o adresy fizyczne stosowane w technologiach Token ring oraz FDDI. . 169

CA Centrum Certyfikacji Kluczy (*ang. Certification Authority*). Trzecia strona zaufana w systemie PKI potwierdzająca autentyczność certyfikatów kluczy użytkowników systemu. CA wystawia certyfikaty, generuje listy CRL i certyfikuje inne CA. . 119, 134–136, 138, 179

certyfikat Certyfikat cyfrowy to elektroniczne zaświadczenie, przyporządkowujące dane służące do weryfikacji podpisu elektronicznego do określonej osoby, potwierdzające jej tożsamość. Pojęcie certyfikatu jest zgodne z odpowiednią Dyrektywą Unii Europejskiej. Fizycznie jest to ciąg bajtów zapisanych w odpowiednim formacie - najpopularniejszy jest standard X.509. . 95

CLI *ang. Command-Line Interface* - interfejs z linią komendy. . 48

cookie *ang. Cookie* lub HTTP Cookie - mały fragment tekstu, który serwis internetowy wysyła do przeglądarki i który przeglądarka wysyła z powrotem do serwera. Pliki cookie zapamiętywane są po stronie klienta i często wykorzystywane są do śledzenia użytkownika. . 95

CRL lista certyfikatów unieważnionych generowana przez CA. . 153, 158

dane osobowe Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. . 40

DDos DDoS (*ang. distributed denial of service* - rozproszona odmowa usługi) - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów . Zobacz https://pl.wikipedia.org/wiki/DDoS. . 83, 84

DES *ang. Data Encryption Standard* - blokowy algorytm symetryczny zaprojektowany w 1975 roku przez firmę IBM, wykorzystujący do szyfrowania 56*b* klucz szyfrujący. . 100, 108, 125

DHCP *ang. Dynamic Host Configuration Protocol* Protokół dynamicznego konfigurowania hostów - protokół komunikacyjny umożliwiający hostom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski podsieci. . 197

DNS System nazw domen. Usługa serwera wymagana do tłumaczenia nazw na numery IP i odwrotnie. Zobacz http://www.dns.pl.. 20, 86, 88, 197

Dos Rodzaj ataku na system najczęściej serwerowy polegający na niedostępności usługi poprzez zarzucenie serwera zapytaniami. Zobacz http://pl.wikipedia.org/wiki/DoS. . 81

DSA *ang. Digital Signature Algorithm* - algorytm asymetryczny stworzony przez NIST. Algorytm został opatentowany przez NIST, ale można go używać za darmo, także w zastosowaniach komercyjnych. DSA jest zaimplementowany między innymi w OpenSSL, OpenSSH i GnuPG. . 120

EMDC *ang. Extended Message Authentication Code* - rozszerzony skrót MDC. . 110, 111

firewall (ściana przeciwogniowa) - jeden ze sposobów zabezpieczania sieci i systemów informatycznych przed atakami, przez np. filtrowanie pakietów. Chroni sprzęt i oprogramowanie w sieci wewnętrznej LAN przed dostępem z zewnątrz. Umożliwia także monitorowanie ruchu. . 53, 57, 85, 87, 166

GID *ang. Group ID* - identyfikator grupy - numer przypisywany grupie w momencie tworzenia grupy. . 48

GIODO Generalny Inspektor Ochrony Danych Osobowych . 12

GNU *ang. GNU's Not Unix* to projekt systemu operacyjnego podobnego do Unix'a, który wykorzystuje wyłącznie wolne oprogramowanie rozprowadzane na licencji GNU GPL. . 163

GPL GNU General Public Licence - licencja oprogramowania otwartego. Licencja gwarantuje użytkownikowi końcowemu prawo do używania, studiowania budowy, kopiowania (udostępniania) i modyfikacji oprogramowania. Oprogramowania takie nazywane jest w języku angielskim *ang. free software*. Oprogramowanie wykorzystujące programy na licencji GPL musi także być dystrybuowane na licencji GPL. Zobacz http://en.wikipedia.org/wiki/GNU_General_Public_License. . 163, 180

GUI *ang. Graphical User Interface* - graficzny interfejs użytkownika. . 48

HMAC HMAC (*ang. keyed-Hash Message Authentication Code*) - kod MAC z wmieszanym kluczem Kod MAC z wmieszanym kluczem tajnym za-

pewniający zarówno ochronę integralności jak i autentyczności danych. Zobacz http://tools.ietf.org/html/rfc2104. . 115

HTTP *ang. Hypertext Transfer Protocol* - protokół przesyłania dokumentów hipertekstowych w sieci WWW. Obecnie obowiązuje standard RFC 2616.. 20, 181

HTTPS Protokół HTTP z szyfrowaniem kanału komunikacyjnego.. 20

IBM *ang. International Business Machines Corporation* - jeden z najstarszych koncernów informatycznych na świecie. . 126

IDEA *ang. International Data Encryption Algorithm* - szyfr blokowy, wykorzystujący 128*b* klucz szyfrujący. . 100, 108, 122

IP *ang. Internet Protocol* - numer komputera w sieci. Obecnie stosowane są dwie wersje protokołu IP: v4 i v6. W wersji 4 numer ma długość 32 bitów, natomiast w wersji 6 - 128 bitów.. 81, 86, 179

ISDN ISDN (ang. Integrated Services Digital Network, sieć cyfrowa z integracją usług) - technologia sieci telekomunikacyjnych mająca na celu wykorzystanie infrastruktury publicznej sieci telefonicznej (wcześniej analogowej) do bezpośredniego udostępnienia usług cyfrowych użytkownikom końcowym (bez pośrednictwa urządzeń analogowych). . 156

Java Obiektowy język programowania stworzony w firmie Sun Microsystems. Java jest językiem tworzenia programów źródłowych kompilowanych do kodu bajtowego - postaci wykonywanej przez maszynę wirtualną. Składnia języka jest podobna do składni C++. . 163

klucz prywatny *ang. private key, secret key* - SK - klucz znany tylko temu użytkownikowi sieci, któremu jest przypisany. Przy użyciu kluczy prywatnych możliwe jest generowanie podpisów cyfrowych (elektronicznych). . 107

klucz publiczny *ang. public key* - PK jest udostępniany wszystkim użytkownikom sieci . 107

Linux Rodzina darmowych uniksopodobnych systemów operacyjnych opartych na jądrze Linux. . 87, 163

MAC (*ang. Media Access Control*) MAC to unikalny 48-bitowy (6B) adres karty sieciowej, najczęściej zapisywany heksadecymalnie. Adres podzielony jest na dwie równe części - początkowe 24b to identyfikator producenta, końcowe 24b to identyfikator egzemplarza karty. Starsze karty ethernetowe nie miały możliwości zmiany adresu MAC, natomiast w najnowszych istnieje taka możliwość. Adres MAC wykorzystywany jest do zapewnienia bezpieczeństwa w sieciach komputerowych oraz w licencjonowaniu oprogramowania. . 179, 193

MAC *ang. Message Authentication Code* - uwierzytelnienia wiadomości przez dołączenie do wiadomości ciągu bitów zwanego znacznikiem. . 109, 110

MainFrame to tzw. komputery głównego szeregu. Charakteryzują się dużą niezawodnością. Przeznaczone są do wykonywania dużej liczby operacji wejścia/wyjścia. Przeznaczone są głównie do obsługi dużych baz danych (pliki rzędu xTB). Nie posiada tak dużej mocy obliczeniowej jak superkomputer.. 49

MD4 MD4 to algorytm liczenia skrótu. Obecnie nie powinien być używany. . 100

MD5 MD5 to algorytm liczenia skrótu. Obecnie nie powinien być używany. . 100, 119, 120, 138, 182

MDC *ang. Modification Detection Code* - znacznik integralności danych - zobacz message digest . 110, 180

message digest *ang. message digest* - skrót z wiadomości. Najczęściej używane algorytmy: MD5, SHA-1, SHA-2. . 182

MPDU *ang. Media access control protocol data unit* - tecnika podnosząca niezawodność transmisji w sieci bezprzewodowej przez zmniejszenie liczby kolizji. . 195

NIST *ang. National Institute of Standards and Technology*. . 100, 115–117, 119, 126, 179

NSA *ang. National Security Agency*. . 115

NTFS NTFS (*ang. New Technology File System*) standardowym system plików systemu Windows NT i jego następców. Posiada rozbudowany system praw dostępu (listy kontroli dostępu - ACL, mechanizmy szyfrowania systemu plików i dziennika operacji dyskowych (*ang. journal*). . 57, 182

PGP *ang. Pretty Good Privacy*. System szyfrowania i deszyfrowania wiadomości podpisanych cyfrowo. Umożliwia weryfikację autentyczność nadawcy (pod warunkiem, że ten także korzysta z PGP) i zarządzanie kluczami. Weryfikacja kluczy opiera się o sieć zaufania (*ang. web of trust*). Poziom autentyczności danego klucza jest determinowany przez sumę podpisów, złożonych przez różne osoby znające posiadacza klucza. . 138

PID (*ang. Process ID*) identyfikator procesu - liczba całkowita przypisywana procesowi w momencie uruchomienia. . 48

PIN *ang. Personal Identification Number* . 37

pishing Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. . 95

PKI Infrastruktura Klucza Publicznego (*ang. Public Key Infrastructure*) - system umożliwiający bezpieczną wymianę informacji (kryptografia z kluczem asymetrycznym). Zapewnia autentyczność i niezaprzeczalność. Zobacz http://pl.wikipedia.org/wiki/Infrastruktura_klucza_publicznego. . 13, 107, 133–136, 141, 149, 153, 179, 183, 184

RA *ang. Registration Authority* - urząd rejestracji, punkt rejestracji - zbiera wnioski o wydanie certyfikatu, weryfikuje tożsamość subskrybentów. . 134

RC6 blokowy algorytm symetryczny opracowany przez Rivest'a, Shamir'a, Adleman'a. Informacje można znaleźć pod adresem: http://www.rsa.com/ (RSA Security). Algorytm został opatentowany: U.S. Patent 5,724,428 i U.S. Patent 5,835,600. . 126

Rijndael nazwa robocza algorytmu AES. . 101, 125

RSA Algorytm asymetrycznym RSA , opublikowanym w 1978 roku. Jako jeden z nielicznych algorytmó asymetrycznych oparł się próbom ataku i stał

się standardem, używanym powszechnie m.in. do generacji podpisów cyfrowych. . 108, 111, 120

S/KEY protokół uwierzytelniania wykorzystujący hasła jednorazowe oraz funkcje jednokierunkowe zaproponowany przez Lesliego Lamporta w 1981 roku. . 37

sekret W kryptografii oznacza klucz szyfrujący. . 99

SHA *ang. Secure Hash Algorithm* - bezpieczny algorytm liczenia skrótu. Opublikowano kilka wersji SHA-0 (160*bit*), SHA-1 (160*bit*), SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512). Obecnie używane jest algorytm SHA-1. Ze względów bezpieczeństwa należy przejść na algorytm SHA-2. . 100, 120

SHA-1 *ang. Secure Hash Algorithm* - funkcja skrótu, która tworzy skrót o długości 160*b*. . 182

SHA-2 zestaw kryptograficznych funkcji skrótu (SHA-224, SHA-256, SHA-384, SHA-512), generujących skróty o różnych długościach 224..512*b*. . 182

sniffer Program lub urządzenie, którego zadaniem jest przechwytywanie i ewentualnie analizowanie danych przepływających w sieci. Analizator odbiera wszystkie ramki z sieci, także te nieadresowane bezpośrednio do niego. Wywmaga to przełączenie karty sieciowej w tryb mieszany (*ang. promiscuous*). . 170

spam Niechciane lub niepotrzebne wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam za pośrednictwem poczty elektronicznej. . 84, 86

SSID *ang. Service Set Identifier* - jest unikalny identyfikator sieci WI-FI. . 193

SSL *ang. Secure Socket Layer* jest protokołem do zabezpieczania kryptograficznego kanału komunikacyjnego w architekturze klient-serwer. Wymaga odpowiedniego certyfikatu klucza szyfrującego (kryptografia asymetryczna) do ustanowienia połączenia szyfrowanego. Po ustanowieniu połączenia generowany jest klucz sesyjny (symetryczny) i dalsze szyfrowanie odbywa się tym kluczem. Ma to na celu redukcję nakładów obliczeniowych związanych z wykorzystaniem kluczy asymetrycznych (klucze te wykorzystywane są tylko na etapie. SSL jest obecnie szeroko stosowany w praktyce. Następcą jest TLS. . 119, 183

system calls wywołania systemowe. Funkcje jądra (kernel'a) do komunikacji ze sprzętem. W systemie Unix/Linux jest ich około 300. Im mniej tym system jest bardziej bezpieczny. . 48

TCP *ang. Transmission Control Protocol* . 164, 165

The Orange Book Pomarańczowa Księga - dokument definiujący poziomy bezpieczeństwa komputerowego systemu operacyjnego. Tekst dostępny jest pod adresem: http://www.dynamoo.com/orange/. . 43, 44, 47

TLS *ang. Transport Layer Security* to protokół kryptograficzny wykorzystywany w bezpiecznej komunikacji internecie (RFC6176). Wykorzystuje certyfikaty X.509 w celu identyfikacji drugiej strony, z którą odbywa się komunikacja. Wykorzystywana jest tutaj kryptografia asymetryczna i system PKI. Poprzednikiem TLS jest SSL. . 183

UDP *ang. User Datagram Protocol* . 165

UID *ang. User ID* - identyfikator użytkownika - numer przypisywany użytkownikowi na etapie zakładania konta. . 48

V.34 Standard w komunikacji rekomendowany przez ITU-T, charakteryzujący się pełną transmisją dwukierunkową pomiędzy dwoma modemami wdzwanianymi (połączenie wdzwaniane, *ang. dial-up*) przy przepustowości łącza do $28.8 kbit/s$. . 157

vi Podstawowy edytor administratora systemu Unix. W wielu komercyjnych systemach Unix edycja konfiguracji możliwa jest tylko za pomocą edytora vi.. 49

X.509 Zbiór standardów sieciowych opisujących usługi katalogowe w sieci. Standard definiujący certyfikaty kluczy publicznych, sposób unieważniania certyfikatów oraz zestaw atrybutu wykorzystywany do budowy systemu PKI. . 119, 179

Dodatek A

Zadania

Zadanie 1 Bezpieczeństwo systemów informatycznych

Co zrobić, aby podnieść bezpieczeństwo pracy w systemie Windows 7/8/10 (wymień co najmniej 5 działań, które należy wykonać)? Jakie znasz rodzaje kont użytkowników - do czego służą? Co to jest i do czego służy filtr kontroli rodzicielskiej? Jak można wykorzystać filtr kontroli rodzicielskiej do podniesienia bezpieczeństwa pracy? Co to jest lokalizacja sieci? Jakie znasz lokalizacje sieci? Jakie konsekwencje pociąga za sobą włączenie lokalizacji sieci (np.sieć publiczna)? Co to jest usługa OneDrive? Jakie mogą być konsekwencje używania usługi OneDrive? Do czego służy oprogramowanie Sysinternals?

Zadanie 2 Przeglądarki WWW - pytania

Jak podnieść bezpieczeństwo pracy przeglądarki internetowej?

Zadanie 3 Kryptografia

Wymień podstawowe usługi kryptografii i wyjaśnij co oznaczają.

Zadanie 4 Kryptografia symetryczna

Narysuj sposób szyfrowania w kryptografii symetrycznej *informacji* pomiędzy nadawcą i odbiorcą. Jaka jest główna zaleta i główna wada kryptografii symetrycznej?

Zadanie 5 Kryptografia asymetryczna

Narysuj sposób szyfrowania w kryptografii asymetrycznej *informacji* pomiędzy nadawcą i odbiorcą. Jaka jest główna zaleta i główna wada kryptografii symetrycznej? Co to jest klucz prywatny i publiczny? Jaka jest zależność pomiędzy kluczami?

Zadanie 6 Klucze

Co to jest klucz prywatny i publiczny? Jaka jest zależność pomiędzy kluczami? Jakie są konsekwencje utraty klucza prywatnego?

Zadanie 7 Funkcja skrótu

Co to jest funkcja skrótu i do czego służy? Jakie znasz algorytmy obliczania funkcji skrótu? Które z tych algorytmów nie mogą lub nie powinny być stosowane i dlaczego? Co to jest kolizja i co powoduje?

Zadanie 8 Podpis elektroniczny

Co to jest podpis elektroniczny? Do czego stosuje się podpis elektroniczny? Wymień znane Ci systemy podpisu elektronicznego?

Zadanie 9 Certyfikat klucza

Co to jest certyfikat klucza szyfrującego? Do czego służy i jakie informacje zawiera? Kto wystawia certyfikaty? Czy certyfikat klucza można unieważnić? Co się wtedy stanie? W jaki sposób certyfikaty i klucze są dystrybuowane? Jakie znasz rodzaje certyfikatów? Co to są certyfikaty zakładkowe?

Zadanie 10 Polityka bezpieczeństwa

Co to jest Polityka Bezpieczeństwa? Co zawiera, a czego nie zawiera? Napisz własną Politykę Bezpieczeństwa dla wybranej organizacji/firmy.

Zadanie 11 Zabezpieczanie przed utratą danych

Jakie znasz metody zabezpieczania systemów komputerowych przed utratą danych? Wymień co najmniej dwa i scharakteryzuj. Podaj wady i zalety każdego ze sposobów.

Zadanie 12 Backup

Co to jest *backup*? W jaki realizuje się *backup*? Wymień rodzaje *backupu*

Zadanie 13 Mirroring

Co to jest *mirroring*? Gdzie jest stosowany i w jakim celu?

Zadanie 14 Ataki na systemy komputerwe

Wymień znane Ci ataki na systemy komputerowe (w tym serwery sieciowe)? Omów jeden wybrany.

Zadanie 15 Ochrona elektromagnetyczna

Co to jest obudowa tempestowa komputera?

Dodatek B

Router CellPipe 7130

Na wydruku B.1 przedstawiono zawartość pliku *password.html* pobranego z routera. Plik nie jest w żaden sposób zabezpieczony. Do pobrania pliku wystarczy zalogowanie się na konto użytkownika *user*. Analiza kodu umożliwia prześledzenie sposobu działania uwierzytelnienia na routerze i jest pomocna dla hackerów. W kodzie zapisane zostały hasła użytkownika *user* (linia 14) oraz administratora *admin* (linia 12).

Wydruk B.1: Plik password.html pobrany z routera CellPipe7130.

```
1  <html>
2  <head>
3  <meta http-equiv="Content-Type" content="text/html; charset=
       ↪ ISO-8859-1" />
4  <link rel="stylesheet" href='stylemain.css' type='text/css'>
5  <link rel="stylesheet" href='colors.css' type='text/css'>
6  <script language="javascript" src="util.js"></script>
7  <script language="javascript" src="lang_en.js"></script>
8
9  <script language="javascript">
10 <!-- hide
11
12 pwdAdmin = 'xxxxxxxxxx';
13 pwdSupport = 'supportadmin';
14 pwdUser = 'xxxxxxxxxxxxxx';
15 curUser = 'user';
16
17 var AccountCfgObjectItems = 'Username}-{Password}-{|,|';
18 var AccountCfgObjectRows = numOfRow(AccountCfgObjectItems);
19 var obj2_userArray = getColFromList(AccountCfgObjectItems, '
       ↪ Username');
20 var obj2_password = getColFromList(AccountCfgObjectItems, '
       ↪ Password');
21
22 var eleObj = new Array( "id1", "id2", "id3", "id4", "id5","
       ↪ id6","id7");
23 var elelength = eleObj.length;
24
25 function fillAccountCfgObjectItems(){
```

```
26  var i;
27
28  if (curUser == 'admin')
29  {
30      document.writeln("<option value= admin>admin");
31      document.writeln("<option value= user>user");
32      for(i=0; i < AccountCfgObjectRows; i++)
33      {
34          document.writeln("<option value="+obj2_userArray[i]+"
                ↪ >"+obj2_userArray[i]);
35      }
36  }
37  else
38  {
39      document.writeln("<option value="+  curUser + ">" +
            ↪ curUser);
40  }
41 }
42
43 function frmLoad() {
44    with ( document.forms[0] ) {
45    FillCell(eleObj, WEB_PASSWORD);
46    }
47 }
48
49 function btnApply() {
50  var loc = 'password.cgi?';
51
52  with ( document.forms[0] ) {
53      var idx = userName.selectedIndex;
54      switch ( idx ) {
55          case 0:
56              alert(getWebElement( WEB_PASSWORD, elelength ));
57              return;
58        default:
59          if (userName.value == 'admin')
60          {
61              if ( pwdOld.value == pwdAdmin )
62                  break;
63              else
64              {
65                  alert(getWebElement( WEB_PASSWORD, elelength +
                        ↪ 1));
66                  return;
67              }
68          }
69          else if (userName.value == 'user')
70          {
71              if ( pwdOld.value == pwdUser )
72                  break;
73              else
74              {
75                  alert(getWebElement( WEB_PASSWORD, elelength +
                        ↪ 3));
```

```
76                  return;
77              }
78          }
79          else
80          {
81              for(i=0; i < AccountCfgObjectRows; i++)
82              {
83                  if (obj2_userArray[i] == userName.value)
84                  {
85                      if (pwdOld.value == obj2_password[i])
86                          break;
87                      else
88                      {
89                          alert(getWebElement( WEB_PASSWORD,
                                ↪ elelength + 3));
90                          return;
91                      }
92                  }
93              }
94          }
95
96          /* case 1:
97              if ( pwdOld.value == pwdAdmin )
98                  break;
99              else {
100                 alert(getWebElement( WEB_PASSWORD, elelength +
                        ↪ 1));
101                 return;
102             }
103          case 2:
104             if ( pwdOld.value == pwdSupport )
105                 break;
106             else {
107                 alert(getWebElement( WEB_PASSWORD, elelength +
                        ↪ 2));
108                 return;
109             }
110         case 2:
111             if ( pwdOld.value == pwdUser )
112                 break;
113             else {
114                 alert(getWebElement( WEB_PASSWORD, elelength +
                        ↪ 3));
115                 return;
116             }*/
117     }
118
119     if ( pwdNew.value != pwdCfm.value ) {
120         alert(getWebElement( WEB_PASSWORD, elelength + 4));
121         return;
122     }
123
124     var str = new String();
125     str = pwdNew.value;
```

```
126     if ( str.length > 16 ) {
127         alert(getWebElement( WEB_PASSWORD, elelength + 5));
128         return;
129     }
130     if ( str.indexOf(' ') != -1 ) {
131         alert(getWebElement( WEB_PASSWORD, elelength + 6));
132         return;
133     }
134 
135     switch ( idx ) {
136         case 0:
137             break;
138         default:
139             if (userName.value == 'admin')
140             {
141                 loc += 'adminPassword=' + encodeUrl(pwdNew.
                        ↪ value);
142                 break;
143             }
144             else if (userName.value == 'user')
145             {
146                 loc +='usrPassword='+encodeUrl(pwdNew.value);
147                 break;
148             }
149             else
150             {
151                 loc +='otherUserName='+userName.value
152                     +'&otherPassword='+encodeUrl(pwdNew.value);
153                 break;
154             }
155 
156       /* case 1:
157             loc +='adminPassword='+encodeUrl(pwdNew.value);
158             break;
159         case 2:
160             loc +='usrPassword='+encodeUrl(pwdNew.value);
161             break;
162         default:
163             loc +='otherUserName='+userName.value
164                 +'&otherPassword='+encodeUrl(pwdNew.value) ;
165             break; */
166     }
167 
168     var code = 'location="'␣+␣loc␣+␣'" ';
169     eval(code);
170 }
171 }
172 
173 function addClick() {
174     var loc = 'passwordadd.html';
175     var code = 'location=\"'␣+␣loc␣+␣'\" ';
176     eval(code);
177 }
178 
```

```
179 function removeClick(rml) {
180     var lst = '';
181 
182     lst = document.forms[0].userName.value;
183 
184     if(lst == 1 || lst == 2 || lst == 3)
185     {
186         alert(getWebElement( WEB_PASSWORD, elelength + 7));
187         return;
188     }
189 
190     var loc = 'password.cmd?action=remove_user&rmLst=' + lst;
191     var code = 'location=\" '␣+␣loc␣+␣'\" ';
192     eval(code);
193 }
194 // done hiding -->
195 </script>
196  </head>
197  <body onLoad='frmLoad()'>
198   <blockquote>
199    <form>
200       <b id="id1" class="tdTitle"></b><br><br>
201       <span id="id2"></span><br><br>
202       <span id="id3"></span><br><br>
203       <table border="0" cellpadding="0" cellspacing="0">
204          <tr>
205             <td id="id4" width="120" class="tdItem"></td>
206             <td><select name='userName'  style="width:146px"
                    ↪  size="1">
207                <option value="0">
208                <!-- <option value="1">admin -->
209                <!-- <option value="2">support -->
210                <!-- <option value="3">user -->
211                <script language='javascript'>
212                <!--hide
213                    fillAccountCfgObjectItems();
214                //-->
215                </script>
216             </select></td>
217          </tr>
218          <tr>
219             <td id="id5" class="tdItem"></td>
220             <td><input name='pwdOld' type="password"
221              size="20" maxlength="16"></td>
222          </tr>
223          <tr>
224             <td id="id6" class="tdItem"></td>
225             <td><input name='pwdNew' type="password" size="
                    ↪ 20"
226              maxlength="16"></td>
227          </tr>
228          <tr>
229             <td id="id7" class="tdItem"></td>
230             <td><input name='pwdCfm' type='password' size="
```

```
                    ↪ 20"
231                maxlength="16"></td>
232             </tr>
233          </table>
234          <br>
235          <center>
236          <input class='buttonX' type='button' onClick='addClick
                 ↪ ()' id='addBtn'>
237          <script language="javascript">
238          if (curUser == 'admin')
239             document.writeln("<input␣class='buttonX'␣type='
                    ↪ button'
240 ␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣onClick='removeClick()'␣id='removeBtn'>");
241          </script>
242          <script language="javascript">
243          <!-- hide
244          if ('0' == '1')
245             document.writeln("<a␣href='javascript:btnApply()'>
246 ␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣<img␣src='pic/apply_p.jpg'␣border='0'></a>");
247           else
248             document.writeln("<input␣class='buttonX'␣type='
                    ↪ button'
249 ␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣onClick='btnApply()'␣␣id='saveapplyBtn'>");
250          // done hiding -->
251          </script>
252          </center>
253       </form>
254     </blockquote>
255   </body>
256 </html>
```

Dodatek C

Konfiguracja routerów

Nieprawidłowa konfiguracja routerów jest od wielu lat jednym z najsłabszych elementów w sieciach komputerowych. Może powodować lub umożliwiać opisane w pracy oszustwa lub włamania. Poniżej przedstawiono sposób ustawienia szeregu opcji routera, które podnoszą bezpieczeństwo oraz te, które zwiększają wydajność. Poniżej przedstawiono zalecenia dotyczące prawidłowej konfiguracji routerów.

SSID - identyfikator sieci Wi-Fi SSID *Service Set Identifier - network name* jest unikalnym identyfikatorem sieci WI-FI. Duże i małe litery są rozróżniane.

Zalecane ustawienie: unikalna nazwa

Wybrana nazwa sieci nie może być taka sama jak nazwa sieci w zasięgu routera. Niektóre routery posiadają skonfigurowany domyślny SSID, np.: *linksys*, *netgear*, *NETGEAR*, *dlink*, *wireless*, *2wire*, and *default*.

Sieci ukryte Sieci ukryte nie emitują swojego identyfikatora sieci (SSID). Czasami takie sieci nazywane są nieprawidłowo *zamkniętymi*.

Zalecane ustawienie: wyłączyć (Disabled)

Dla urządzeń sieciowych trudniej jest odnaleźć sieci ukryte, co skutkuje dłuższymi czasami potrzebnymi na potrzebnymi na podłączenie się i trudnościami z automatycznym łączeniem się. Ukrywanie SSID nie zabezpiecza sieci, gdyż można go uzyskać innymi metodami.

Filtrowanie lub ograniczanie z wykorzystaniem MAC Technika umożliwia ograniczenie dostępu do routera WI-FI dla urządzeń o ustawionym adresie MAC.

Zalecane ustawienie: wyłączyć (Disabled)

Włączenie opcji umożliwia ustawienie adresów MAC urządzeń, które mogą łączyć się z routerem. Urządzenia o adresie MAC spoza listy nie będą łączyły się z routerem. Jednak obecne adres MAC urządzenia można łatwo zmienić, więc ten sposób zabezpieczania sieci może okazać się nieskuteczny.

Bezpieczeństwo Bezpieczeństwo sieci WI-FI jest w głównej mierze zapewnione dzięki prawidłowo ustawionemu mechanizmowi uwierzytelniania i szyfrowania używanemu przez router.

Logowanie umożliwia kontrolę dostępu do sieci, natomiast szyfrowanie zabezpiecza transmisję w sieci bezprzewodowej. Nowoczesne routery wyposażone są w szyfrowanie algorytmem AES - opcja WPA2 Personal.

Zalecane ustawienie: WPA2 Personal (AES)

Obecnie WPA2 Personal jest najsilniejszym mechanizmem zabezpieczania w sieciach WI-FI. Wymagane jest jednak tzw. silne hasło - o dużej długości (min. 8znaków) i odpowiednim skomplikowaniu. Jest to związane ze specyfiką algorytmu AES.

W przypadku konieczności dołączenia do sieci starszych urządzeń, które nie obsługują WPA2 Perspnal (AES), dobrym rozwiązaniem jest ustawienie trybu *WPA/WPA2 Mode* (czasami opcja nazywa się *WPA Mixed Mode*). W takim przypadku nowe urządzenia wykorzystywać będą silniejszy algorytm kryptograficzny (WPA2), a starsze słabszy (WPA).

Jeżeli router nie wspiera WPA2/WPA to w następnej kolejności najlepszym rozwiązaniem jest WPA Personal (TKIP).

Używanie jeszcze starszego mechanizmu WEP jest niezalecane ze względu na kompatybilność, szybkość i bezpieczeństwo. WEP nie gwarantuje odpowiedniego poziomu bezpieczeństwa.

Zarówno WPA TKIP jak i WEP są niezalecane. Uniemożliwiają pełne wykorzystanie szybkości i innych cech protokołu 802.11n. Należy je stosować tylko tam gdzie jest to absolutnie konieczne.

2.4 GHz Radio Mode Opcja określa, która wersja protokołu 802.11a/b/g/n będzie wykorzystywana na częstotliwości $2.4GHz$. Nowy standard (802.11n) umożliwia największe prędkości transmisji danych, starsze standardy zapewniają jednak kompatybilność ze starszym sprzętem.

Zalecane ustawienie: 802.11b/g/n

Zalecane jest ustawienie możliwości transmisji w różnych standardach. Urządzenie samo dobierze najszybszy tryb transmisji. Ustawienie tylko wybranych standardów może powodować interferencję z innymi routerami lub powodować niemożność połączenia się starszych urządzeń.

5 GHz Radio Mode Opcja określa, która wersja protokołu 802.11a/b/g/n będzie wykorzystywana na częstotliwości $5GHz$. Nowy standard (802.11n) umożliwia największe prędkości transmisji danych, starsze standardy zapewniają jednak kompatybilność ze starszym sprzętem.

Zalecane ustawienie: 802.11a/n

Routery wspierające 802.11n powinny być ustawione w trybie 802.11a/n dla uzyskania maksymalnej szybkości i kompatybilności. Zależy to jednak od konkretnego routera. Urządzenia samo dobierze najszybszy standard transmisji. Ustawienie tylko wybranych standardów może powodować interferencję z innymi routerami lub powodować niemożność połączenia się starszych urządzeń.

Kanał transmisji Opcja umożliwia ustawienie kanału komunikacyjnego, na którym odbywa się transmisja. Ustawienie automatycznego doboru kanału umożliwia wybór najlepszego kanału transmisji.

Zalecane ustawienie: Auto

Możliwe jest ręczne ustawienie kanału, jednak ustawienie kanału już wykorzystywanego powoduje interferencje i zakłócenia w działaniu sieci. Przed ręcz-

nym ustawieniem kanału należy zbadać, które kanały są wolne jednym z dostępnych programów (np.:InSSIDer, LinSSID). W jednym obszarze mogą nadawać (nie zakłócając się) sieci korzystające z czterech częstotliwości:

1. kanały: 1, 6, 11
2. kanały: 2, 7, 12
3. kanały: 3, 8, 13
4. kanały: 1, 5, 9, 13

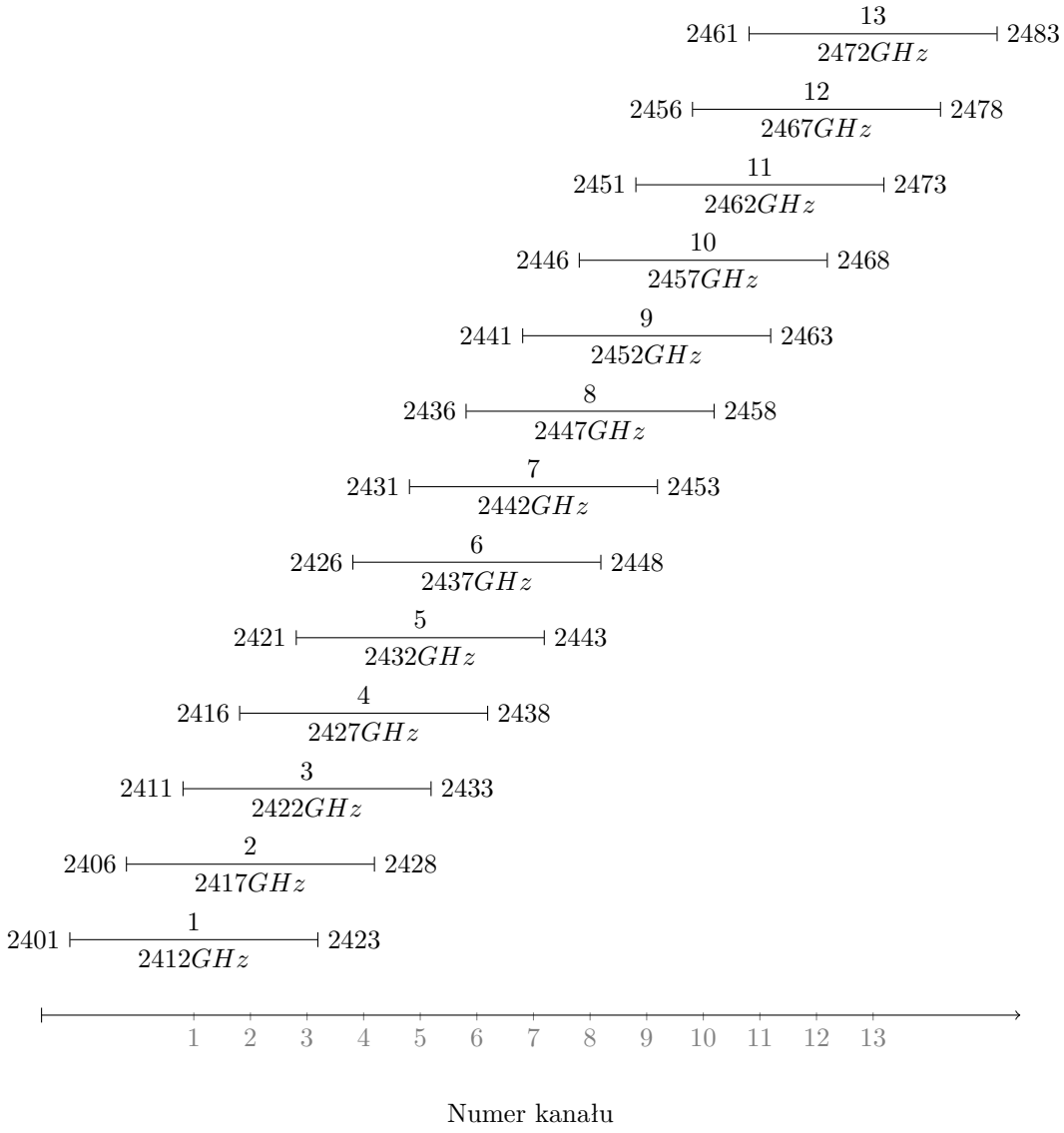
Nieprawidłowa praca	Przyczyna	Rozwiązanie
Zrywanie połączeń i niska prędkość łącza radiowego	Niska wartość parametru SNR	Przeszkody w I strefie Fresnela. Źle obliczony bilans energetyczny łącza, źle dobrany sprzęt. Zła polaryzacja anten. Źle ustawione anteny. Wysoki poziom zakłóceń interferencyjnych, szumy.
Niski transfer ze stacji bazowej, przy łączu radiowym pracującym z prędkością maksymalną	Częste kolizje	Włączyć klientom mechanizm RTS/CTS

RTS/CTS Mechanizm zagwarantowania poprawności transmisji (RTS/CTS - *ang. request to send / clear to send*), nawet gdy występują tzw. ukryte stacje. Stacja, która wygrała rywalizację o dostęp do kanału nie transmituje swojej ramki MPDU bezpośrednio lecz wysyła ramkę RTS (*ang. Request To Send*). Stacja odbiorcza odpowiada wysłaniem ramki CTS (*ang. Clear To Send*), co gwarantuje, że wszystkie stacje w zasięgu zarówno stacji nadającej jak i odbierającej zostaną powiadomione o tym, że będzie transmitowana ramka i na czas tej transmisji pozostaną nieaktywne. Technika wnosi pewną nadmiarowość transmitowanych danych i jest tym bardziej efektywna, im transmitowane ramki MPDU są dłuższe.

Szerokość kanału dla częstotliwości 2.4 GHz Szerokość kanału (*ang. 2.4 GHz channel width*) opisuje szerokość pasma częstotliwości używanych do transmisji. Szerokość pasma $40MHz$ traktowane jest jako szeroki kanał, natomiast $20MHz$ jako kanał wąski. Kanał szeroki $40MHz$ może powodować problemy z wydajnością i niezawodnością sieci, ze względu na większą podatność na interferencje i kolizje z innymi urządzeniami (Bluetooth, telefony komórkowe, inne routery), a także mniejszy poziom emitowanego sygnału. Węższy kanał np. $20MHz$ oferuje większą moc sygnału (większy zasięg) przy mniejszej szybkość transmisji.

Zalecane ustawienie: $20MHz$

-



Rys. C.1: Rozkład kanałów w paśmie 2.4GHz

Szerokość kanału dla częstotliwości 5 GHz Szerokość kanału używanego do transmisji danych w paśmie $5GHz$ jest mniejszy problemem niż w paśmie $2.4GHz$. Szerokie kanały ($40MHz, 80MHz$) narażone są na interferencje i kolizje z innymi urządzeniami. Kanał wąski to $20MHz$.

Zalecane ustawienie: dla 802.11n i $5GHz$ szerokość kanału $20MHz$ i $40MHz$. Dla 802.11ac i $5GHz$ szerokość kanału: $20MHz$, $40MHz$ i 80 MHz.

DHCP Automatyczny konfiguracja hosta (DHCP) po włączaniu do sieci. Umożliwia m.in. dynamiczny przydział adresów IP umożliwia przydział adresów IP po włączeniu do sieci. W sieci może istnieć tylko 1 serwer DHCP

Zalecane ustawienie: Jeden serwer DHCP na sieć

Istnieje możliwość skonfigurowania DHCP jako usługi serwera. Atak na sieci komputerowe związany jest z podmianą prawidłowych adresów serwerów DNS. W związku z tym na komputerach należy czasami ustawiać adresy serwerów DNS jako adresy stałe, np. DNS Google: 8.8.8.8 i 8.8.4.4 .

NAT Translacja adresów z sieci Internet do sieci lokalnej umożliwia korzystanie użytkownikom sieci lokalnej w sieci Internet.

Zalecane ustawienie: włączyć na routerze (Enabled)

Tylko jedno urządzenie w sieci może dostarczać usługi NAT. W przypadku uruchomienia usługi na więcej niż jednym urządzeniu będą występowały problemy z różnymi usługami, np.: z dostępem do Internetu, Voice Over IP (VoIP), VPN.

WMM (Wi-Fi Multimedia) WNM wprowadza priorytety transmisji dla czterech kategorii ruchu: głosu, wideo, video, ...

Zalecane ustawienie: włączyć (Enabled)

Wszystkie 802.11n i 802.11ac punkty dostępowe powinny mieć domyślnie włączoną opcję WMM. Wyłączenie WMM może powodować problemy dla całego sieci.

Natężenia pola W celu zapewnienia prawidłowej transmisji wartość odbieranego sygnału powinna być na poziomie $-56dB/mW$. Graniczna wartość prawidłowego odbioru to $-62dB/mW$.

IT Security

W pracy przedstawiono wybrane zagadnienia bezpieczeństwa systemów informatycznych. Omówiono wybrane algorytmy kryptograficzne, system PKI, oprogramowanie złośliwe, zagadnienia skanowania sieci. Przedstawiono sprzęt kryptograficzny produkowany w Polsce oraz obowiązujące regulacje prawne. Praca przeznaczona jest dla osób zainteresowanych tematyką, w tym dla studentów kierunku Bezpieczeństwo Narodowe jako uzupełnienie zagadnień wykładowych.

Autor od wielu lat zajmuje się systemami operacyjnymi Unix, w szczególności systemem Linux. Poza omawianą tematyką główne obszary zainteresowań autora obejmują: techniki symulacji układów elektronicznych oraz mikrosystemów, języki behawioralnego opisu sprzętu, systemy zarządzania tokiem kształcenia, platformy e-learningowe, techniki programowania obiektowego odporne na błędy. Autor zaimplementował w praktyce szeregu systemów, m.in.: symulatora mikrosystemów *Dero*, platformy zarządzania i monitorowania procesem dydaktycznym *Quela*, systemu różniczkowania symbolicznego *Deriv*.

ISBN 978-83-937245-3-6