Wykład ten powstał przy współpracy z mgr inż. Andrzejem Mazurkiem, zajmującym się mechanizmami uwierzytelniania i certyfikacji w systemach informatycznych

1. Bezpieczeństwo danych i systemów

System operacyjny jest składnikiem systemu komputerowego. Ten zaś wchodzi w skład większego organizmu jakim jest *system informatyczny*. Pod pojęciem systemu informatycznego rozumiemy zespół elementów sprzętowych i programowych służący do gromadzenia, przetwarzania i przesyłania danych. Dane gromadzone przez system informatyczny modelują najczęściej określony fragment rzeczywistości i podlegają określonym regułom przetwarzania. Problem bezpieczeństwa i ochrony danych (informacji) przechowywanych przez systemy informatyczne nabiera coraz większego znaczenia. Liczba osób korzystających z systemów informatycznych ciągle rośnie, a ostatnie lata przynoszą ciągły, dynamiczny rozwój usług internetowych, usług teleinformatycznych, handlu elektronicznego i bankowości elektronicznej. Łatwo sobie wyobrazić jakie skutki dla funkcjonowania przedsiębiorstwa mogą wiązać się z utratą lub niekontrolowaną zmianą danych elektronicznych.

(1.1) Zagrożenia

Zagrożenia dla danych przechowywanych w systemach teleinformatycznych są bardzo różnorodne. Należą do nich zarówno działania mogące spowodować zniszczenie, uszkodzenie lub zmianę danych w systemie jak również zmierzające do odczytania (skradzenia) ich przez osoby nieuprawnione.

Zbiory danych należące do użytkownika podłączonego do systemu otwartego (a więc udostępnionego w sieci publicznej) mogą zostać zniszczone np. w wyniku działania wirusów lub odczytane przez hakera. Mogą też zostać zniekształcone lub zniszczone w czasie transmisji np. w wyniku awarii lub też celowego działania innych osób. W ich wyniku może nastąpić zarówno utrata danych, przechwycenie przez osoby nieupoważnione jak również naruszenie integralności i spójności systemu (bazy danych), do którego dane te zostały przesłane. Przedstawimy teraz kilka zagrożeń, które są związana z atakami na systemy informatyczne dokonywanymi z zewnątrz.

Dane w systemie informatycznym są bezpieczne jeśli spełnione są następujące dwa warunki:

- zapewniona jest ochrona poufności i integralności, czyli dane są chronione przed nieupoważnionym odczytem i modyfikacją
- zapewniona jest dostępność i spójność danych, czyli dane są dostępne dla osoby uprawnionej i są wiarygodne

Problem bezpieczeństwa systemu informatycznego należy rozpatrywać w dwu zasadniczych kategoriach:

- ochrony systemu (*ang. protection*) oraz
- bezpieczeństwa systemu (*ang. security*).

NASTĘPNA

2. Ochrona

Ochrona jest problemem wewnętrznym systemu informatycznego i dotyczy mechanizmów służących do kontrolowania dostępu programów, procesów lub użytkowników do zasobów zdefiniowanych w systemie komputerowym.

(2.1) Cele ochrony

Pierwsze systemy komputerowe wyposażone były w bardzo słabe mechanizmy ochrony. Wraz z pojawieniem się systemów wieloprogramowych problem ochrony zaczął nabierać istotnego znaczenia i stał się bardziej intensywnym obiektem zainteresowań konstruktorów systemów.

Prawidłowa ochrona w systemie dostarcza odpowiednich mechanizmów, które mogą posłużyć do realizacji określonej polityki wykorzystania zasobów systemu.

Do mechanizmów tych należą między innymi:

- bezpieczne dzielenie wspólnej przestrzeni nazw logicznych, np. katalogów plików;
- bezpieczne dzielenie wspólnej przestrzeni obiektów fizycznych, np. pamięci.

Dzięki zastosowaniu ochrony można zwiększyć niezawodność systemu, podnieść wykrywalność błędów, zapobiegać zamierzonym próbom naruszenia praw dostępu przez użytkowników systemu itd.

Podstawowym celem stosowania ochrony jest zapewnienie, aby każdy wykonywany proces korzystał tylko i wyłącznie z zasobów mu przyznanych i to w sposób określony przez politykę ochrony.

(2.2) Domenowy model ochrony

W celu realizacji mechanizmów ochrony zbudowano model systemu komputerowego, w którym wykorzystuje się pojęcie domeny ochrony.

Domena ochrony jest zbiorem obiektów i rodzajów operacji, które można wykonać dla danego obiektu.

Obiektem może być segment pamięci, procesor, drukarka, dysk, plik, program itd. W zależności od rodzaju z danym obiektem związane są określone operacje. Na przykład z plikiem związane są takie operacje jak: otwarcie pliku, zamknięcie pliku, odczyt z pliku, zapis do pliku.

W modelu domenowym korzysta się również z pojęcia prawa dostępu. Prawo dostępu jest to zbiór operacji, które można wykonać na określonym obiekcie.

Ważną zasadą w skutecznej realizacji ochrony systemu komputerowego jest zasada wiedzy koniecznej.

Zasada wiedzy koniecznej (*ang. need-toknow*) mówi, że każdy proces ma w systemie dostęp tylko do tych zasobów, którą są mu niezbędnie potrzebne do zakończenia zadania i do których otrzymał prawo dostępu.

Oznacza to, że proces otrzymuje tylko tyle swobody do działania w systemie ile jest mu niezbędnie potrzebne. Można dzięki temu ograniczyć zakres ewentualnych uszkodzeń.

Domena ochrony może być traktowana w różny sposób. Może to być na przykład użytkownik systemu, proces lub procedura.

Przykładem systemu wykorzystującego model domeny ochrony jest system operacyjny Unix, w którym domena jest związana z użytkownikiem.

NASTĘPNA

3. Bezpieczeństwo

Bezpieczeństwo jest zagadnieniem szerszym niż ochrona systemu. Bezpieczeństwo systemu polega na zapewnieniu nienaruszalności systemu przez czynniki zewnętrzne. Uważamy, że system jest bezpieczny jeśli jest chroniony przed zagrożeniem ze strony środowiska, na przykład przed próbami naruszenia poufności danych.

(3.1) Polityka bezpieczeństwa

Bezpieczeństwo systemu zależy w dużej mierze od przyjętej polityki bezpieczeństwa. Nawet najlepsze zabezpieczenia nie uchronią przed kradzieżą lub zniszczeniem danych, jeśli polityka bezpieczeństwa pozwala na swobodny dostęp do konsoli administratora.

Polityka bezpieczeństwa, rozumiana jako zbiór wszystkich działań przyjętych w celu osiągnięcia wysokiego poziomu bezpieczeństwa systemu informatycznego, jest więc sprawą bardzo istotną i złożoną.

Podstawowymi mechanizmami stosowanymi w celu zapewnienia bezpieczeństwa w systemie jest dokonywanie identyfikacji, uwierzytelniania oraz autoryzacji użytkowników systemu.

Identyfikacja

Identyfikacja polega na stwierdzeniu tożsamości użytkownika lub innego obiektu zamierzającego skorzystać z zasobów systemu. Najczęściej każdy użytkownik systemu ma przypisany unikalny w obrębie systemu identyfikator lub numer. Dzięki stosowaniu identyfikatorów system wie z jakim użytkownikiem ma do czynienia. Może również dokonywać rejestracji działań wykonanych przez tego użytkownika i na tej podstawie przedstawiać raporty lub dokonywać rozliczeń.

Uwierzytelnianie

Sama identyfikacja nie może jednak zapewnić bezpieczeństwa systemu. Identyfikatory użytkowników są najczęściej tworzone na podstawie dostępnego algorytmu i są wobec tego znane lub łatwe do odgadnięcia. Z tego powodu poza procesem identyfikacji przeprowadzany jest proces uwierzytelniania.

Uwierzytelnianie polega na sprawdzeniu, że obiekt, który zgłasza żądanie dostępu do systemu jest tym za kogo się podaje.

Hasła

Najczęstszym sposobem uwierzytelniania użytkowników systemu jest wymaganie podania

hasła. Długość i rodzaj hasła są oczywiście zależne od systemu (np. niektóre systemy przyjmują hasła o długości do8 znaków lub nie rozróżniają wielkich i małych liter) i od przyjętej polityki bezpieczeństwa, ale warto jest przestrzegać następujących ogólnych zasad:

1. hasło powinno być dostatecznie długie;
2. hasło nie powinno być słowem słownikowym (np. imieniem członka rodziny, psa, datą urodzenia itd.);
3. hasło powinno składać się ze znaków alfanumerycznych czyli zawierać zarówno litery jak i cyfry. Jeśli to możliwe należy stosować kombinacje dużych i małych liter;
4. nie należy zapisywać hasła w łatwo dostępnym miejscu, a już na pewne nie należy umieszczać go na obudowie komputera (!)

Ze względu na swoją naturalność i prostotę systemy identyfikacji opierające swoje działanie na hasłach są wciąż najczęściej stosowane w dzisiejszych systemach komputerowych. Stosowanie haseł w celu określenia tożsamości posiada jednak wiele wad. Najważniejsze z nich to:

- komputer musi przechowywać hasła użytkowników;
- hasło może zostać przechwycone w czasie przesyłania go do komputera;
- użytkownicy zapominają swoje hasła;
- użytkownicy wybierają hasła, które łatwo odgadnąć;
- użytkownicy ujawniają swoje hasła innym osobom.

Przedmioty

Oprócz lub obok uwierzytelniania za pomocą hasła stosuje się też uwierzytelnianie za pomocą specjalnych identyfikatorów (kart chipowych). lub tokenów. Takie systemy również mają swoje wady. Przedmioty używane do identyfikacji w rzeczywistości nie potwierdzają tożsamości danej osoby, lecz przedmiotu. Każdy, kto zdobędzie taki przedmiot będzie mógł podszywać się pod jego właściciela. Z tego też powodu takie systemy są uzupełnieniem systemów opartych na hasłach.

Indywidualne cechy użytkownika

Do uwierzytelniania stosowane są też metody biometryczne wykorzystujące fakt unikatowości pewnych cech fizycznych człowieka – takich jak linie papilarne, czy rysunek tęczówki oka lub też

cech behawioralnych takich jak sposób mówienia, czy pisania.

Typowym przykładem uwierzytelniania na podstawie cech fizycznych użytkownika jest skanowanie linii papilarnych. Rozpoznawanie tej cechy dowiodło już swoją skuteczność, wiarygodność i wygodę. Skanowanie obrazu odcisku palca zabiera mało czasu i wysiłków użytkownika oraz jest jedną z najmniej inwazyjnych metod biometrycznych. Weryfikacja odcisku linii papilarnych jest również stosunkowo szybka.

W chwili obecnej weryfikacja użytkowników za pomocą ich cech fizycznych lub behawioralnych osiąga coraz większą popularność. Technika ta jest używana razem z weryfikacją opartą na haśle. Taki dwustopniowy proces uwierzytelniania zapewnia wyższy poziom bezpieczeństwa, niż każda z tych metod oddzielnie.

Autoryzacja

Po przeprowadzeniu identyfikacji i uwierzytelnienia obiektu system przydziela danemu obiektowi określone praw dostępu do obiektów systemu informatycznego.

(3.2) Zagrożenia bezpieczeństwa

Zagrożenia bezpieczeństwa systemu można podzielić na dwie zasadnicze grupy. Pierwsza grupa, to zagrożenia wynikające ze świadomego działania człowieka. Druga, to nieświadome działania użytkowników, awarie sprzętu, zaniki zasilania oraz oddziaływanie czynników zewnętrznych (pożary, powodzie, katastrofy).

Użytkownicy

Najczęstszym zagrożeniem dla systemu informatycznego jest działanie czynnika ludzkiego, a w tym użytkowników systemu. Z badań wynika, że większość naruszeń bezpieczeństwa systemu jest wynikiem działań wewnątrz tego systemu (organizacji). Do najistotniejszych zagrożeń wewnętrznych należy zaliczyć:

- sabotaż wewnętrzny;
- kradzież informacji;
- kradzież usług;
- błędy użytkowników;
- niedbalstwo;
- nieprawidłowe stosowanie procedur polityki bezpieczeństwa.

Ataki na system

Atak na system przeprowadzany jest najczęściej poprzez przechwycenie lub odgadnięcie danych uprawnionego użytkownika.

Do najczęstszych metod ataku należą:

- **Zmiana oryginalnego programu** rejestrującego użytkowników do systemu (tzw. koń trojański). Program taki przechwytuje dane wprowadzane przez użytkownika i przesyła je do osoby atakującej. Następnie przekazuje sterowanie prawdziwemu programowi rejestrującemu. Przed rejestracją do systemu Windows 2000 niezbędne jest naciśniecie kombinacji klawiszy Ctr+Alt+Delete. Powoduje to wygenerowanie odpowiedniego przerwania przez system, które uniemożliwia zastosowanie tego typu ataku.
- **Podsłuch połączenia sieciowego** (ang. *sniffing*) jest popularnym rodzajem ataku, który często prowadzi do utraty tajności danych. Prowadzi on do utraty tajności kilku rodzajów informacji, niezbędnych do utrzymania minimum bezpieczeństwa chronionej sieci. Informacje te obejmują między innymi: hasła, identyfikatory kont oraz dane prywatne. Podsłuch jest atakiem biernym (nie czyni więc bezpośrednich szkód w systemie), ale bardzo niebezpiecznym, ponieważ najczęściej stanowi wstęp przed zastosowaniem innych metod. Najważniejszym narzędziem w walce z podsłuchem połączenia sieciowego jest podział sieci komputerowej na osobne fragmenty (segmenty), czyli tak zwana segmentacja sieci. W idealnej sytuacji każda maszyna powinna należeć do osobnego segmentu, a jej interfejs nie powinien mieć dostępu do danych dla niego nie przeznaczonych. W praktyce stosuje się też często koncepcję tak zwanych zaufanych systemów (segmentów). Pod tym pojęciem rozumie się system, w którym wszystkie maszyny w danym segmencie są bezpieczne. W celu osiągnięcia takiego stanu komputery oraz połączenia pomiędzy nimi muszą posiadać wystarczającą ochronę fizyczną (zamki w drzwiach, strażnicy, zabezpieczenia przed emisją ujawniającą), aby mieć pewność, że włamywacz nie będzie mógł zainstalować w tym segmencie urządzenia podsłuchującego. Przy transmisji danych należy stosować bezpieczne protokoły oraz szyfrowanie. Należy także unikać przesyłania haseł w formie jawnej.

- **Łamanie haseł**. Najczęściej stosowanymi metodami ataku w celu uzyskania nieautoryzowanego dostępu są tzw. metody korzystające z haseł. Polegają one na podjęciu próby przeniknięcia do systemu poprzez podanie identyfikatora użytkownika i hasła. Atakujący może próbować wielu haseł, aż do momentu podania właściwego. Szybko zorientowano się, że nie jest trudno napisać program generujący rozmaite hasła. Obecnie istnieje wiele tego typu programów, które skutecznie działają na różnych platformach systemowych. Używają one zbiorów słów (słowników), dlatego też ataki tego typu znane są jako metody słownikowe. Programy takie mogą również próbować wszystkich możliwych kombinacji haseł – jest to wtedy tak zwany atak brutalny lub wyczerpujący. Skutecznym sposobem obrony przed atakami na hasła jest stosowanie podstawowych lub zaawansowanych

sposobów tworzenia haseł, systemowe blokowanie konta użytkownika po określonej liczbie błędnych wprowadzeń hasła, stosowanie sprawdzonych mechanizmów powiadamiania o próbach nieautoryzowanego dostępu oraz szyfrowanie plików zawierających hasła.

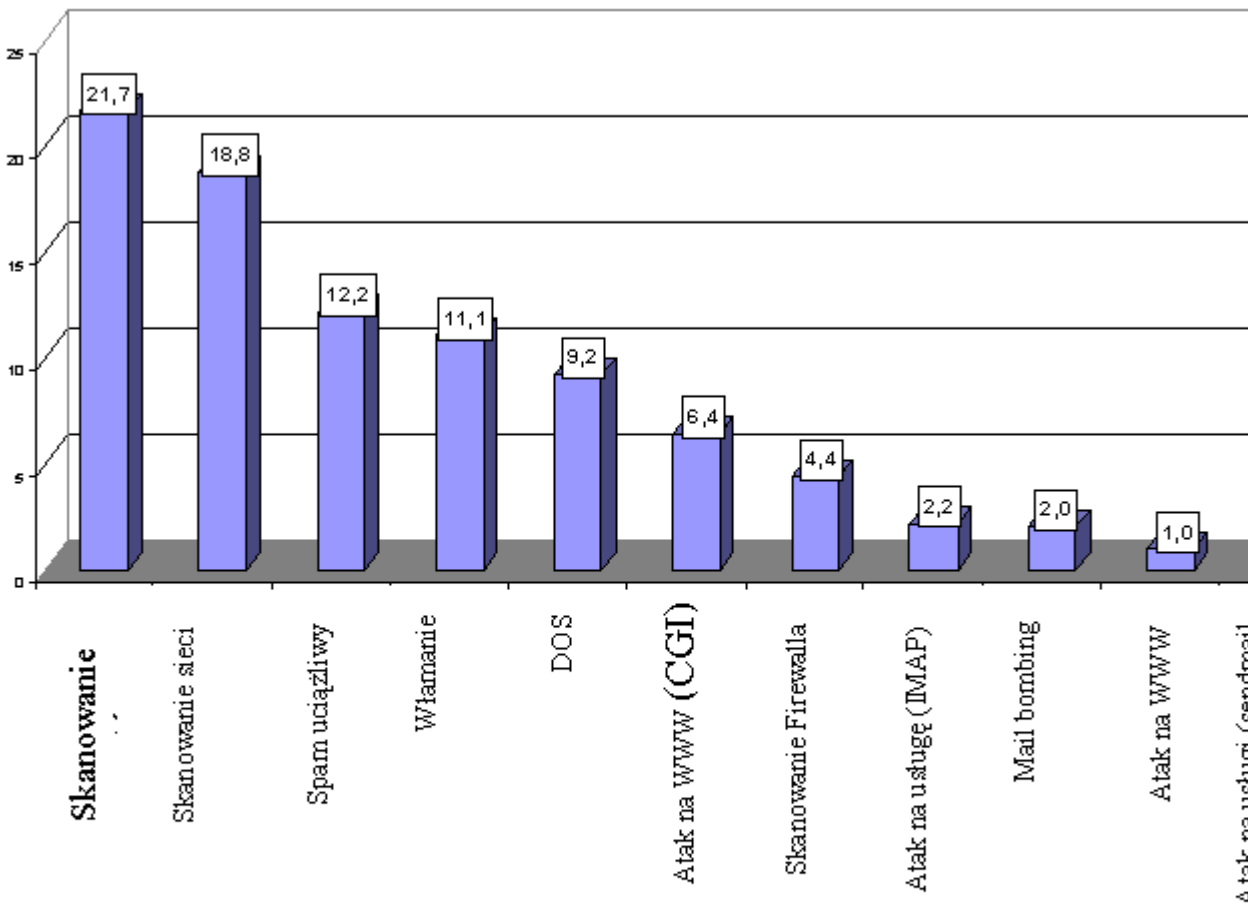
- **Podszywanie się** (ang. *spoofing*) pod inną maszynę z sieci może wystąpić na każdej z warstw protokołu TCP/IP (spoofing adresu sprzętowego, spoofing ARP, spoofing routingu IP, spoofing nazw DNS, spoofing połączeń TCP). Komputery wymieniające między sobą informacje przekazują nawzajem dane o sobie. Osoba niepowołana może wysłać do komputera-odbiorcy fałszywe informacje o swoim komputerze, które świadczą, że jest on bezpiecznym komputerem głównym znajdującym się wewnątrz sieci lub poza nią. Podczas ataku tego typu pakiety wysyłane przez intruza mają dostęp do systemu, do którego się on włamuje i do usług tego systemu.

- **Zablokowanie usługi – DOS** (ang. *Denial of Service*) jest to przerwanie dostarczania usługi spowodowane zniszczeniem systemu lub jego chwilową niedostępnością. Zagrożenie to dotyczy konkretnych usług realizowanych przez system, takich jak WWW, FTP czy poczta elektroniczna. Przykładowe przyczyny odmowy usługi to między innymi zniszczenie twardego dysku lub zajęcie całej dostępnej pamięci. Możliwe jest zaprogramowanie tego rodzaju ataków w skomplikowany sposób, co może doprowadzić do awarii działania całej sieci. Ataki DOS najczęściej są atakami zewnętrznymi, odbywającymi się z zewnątrz sieci lokalnej na przykład z Internetu, uzyskując dostęp poprzez lukę w systemie zabezpieczeń. Często atakujący za pomocą techniki spoofingu ukrywa swój prawdziwy adres internetowy tak, że zlokalizowanie go często staje się niemożliwe.

Wirusy komputerowe

Wirusy należą do grupy programów powodujących zakłócenie pracy systemu informatycznego. Pod pojęciem wirus komputerowy rozumie się program, który potrafi się rozmnażać i dopisywać w postaci ukrytej do innych programów lub w sektorach rozruchowych dysków. Najlepszym sposobem ochrony przed wirusami komputerowymi jest stosowanie programów antywirusowych. Powszechną grupę wśród wirusów stanowią makrowirusy, czyli wirusy tworzone za pomocą języków makropoleceń dostępnych na przykład w edytorach tekstów takich jak MS Word.

Oprócz wirusów można spotkać również programy nazywane *bakteriami*. Są to samodzielne programy powielające się. Ich działanie polega na zużywaniu zasobów systemu (pamięć operacyjna, przestrzeń dyskowa), co szybko powoduje „zatkanie” się systemu. Podobnie zachowują się robaki. Są to programy, które również wykorzystują zasoby systemu, z tą jednak różnicą, że atakują one całe sieci komputerowe a nie pojedynczy system. Często wirusy i bakterie są środkiem do realizacji ataku DOS.



Rysunek 1. *Ataki na system*

Awarie sprzętu

Przyczyną utraty danych może być też awaria sprzętu. Wiele systemów nie może pozwolić sobie na utratę danych lub przestoje spowodowane awarią sprzętu. Aby osiągnąć odpowiednią niezawodność stosuje się następujące metody:

- wykonywanie stałych kopii zapasowych.
  Kopie zapasowe powinno wykonywać się codziennie. Jest to jedna z prostszych i mniej kosztowych metod zapewnienia bezpieczeństwa danych. Powinna być stosowana nawet przez pojedynczego użytkownika – w tym również przez Ciebie drogi Czytelniku. Jednak wykonywanie kopii bezpieczeństwa nie rozwiązuje całkowicie problemu awaryjności sprzętu, gdyż pozwala na odzyskanie danych aktualnych w momencie wykonania ostatniej kopii.

- macierze RAID
  Stanowią one zestaw kilku dysków magnetycznych traktowanych przez system operacyjny jak jeden dysk logiczny. Istnieje wiele rozwiązań tego typu różniących się szybkością działania, możliwością i szybkością odtwarzania danych oraz kosztami eksploatacji.
- zasilacze awaryjne
  przed zanikiem napięcia zasilającego można uchronić stosując specjalne akumulatorowe zasilacze awaryjne (UPS) lub generatory prądotwórcze. Urządzenia takie pozwalają na normalną pracę systemu od kilku minut do kilku godzin. Praca zasilaczy awaryjnych jest nadzorowana przez system operacyjny.

NASTĘPNA

4. Kryptografia

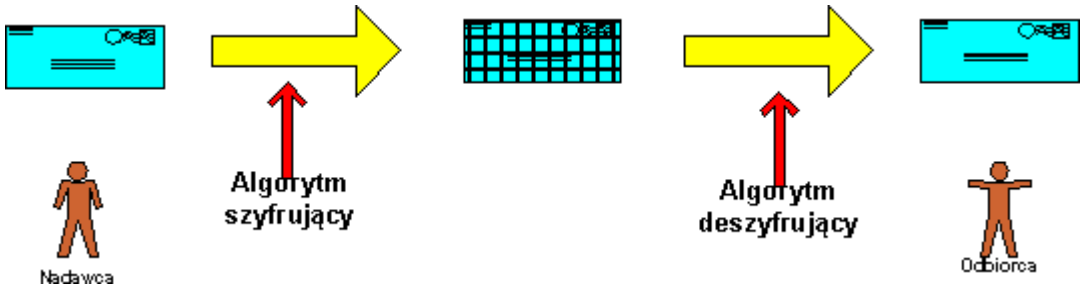
Kryptografia dostarcza narzędzia dzięki którym można, stosując metody matematyczne, zabezpieczać zarówno dane gromadzone w lokalnych magazynach informacji jak i dane przesyłane przez sieć.

Szyfrowanie informacji ma szczególne znaczenie, jeśli korzystamy z systemów otwartych takich jak na przykład Internet. Rozwój bezpiecznych metod kryptograficznych w znaczący sposób przyczynił się do rozwoju handlu elektronicznego i bankowości elektronicznej.

(4.1) Szyfrowanie

Szyfrowanie jest metodą powszechnie stosowaną do ochrony informacji. Choć metody szyfrowania zmieniały się na przestrzeni wieków, to ogólny mechanizm wygląda ciągle tak samo. Można go przedstawić w następujący sposób:

1. Tekst jawny zostaje poddany obróbce zgodnie z algorytmem szyfrowania, czyli podlega kodowaniu. W wyniku tej operacji otrzymuje się tekst, który można co prawda czytać (w sensie odczytu znaków), ale nie można poznać jego sensu.
2. Tekst zaszyfrowany przesyłany jest do odbiorcy normalnymi, niechronionymi kanałami.
3. Po odebraniu tekstu zaszyfrowanego, odbiorca stosując algorytm deszyfracji dekoduje go do postaci czytelnej.



Rysunek 2. Proces szyfrowania i deszyfrowania

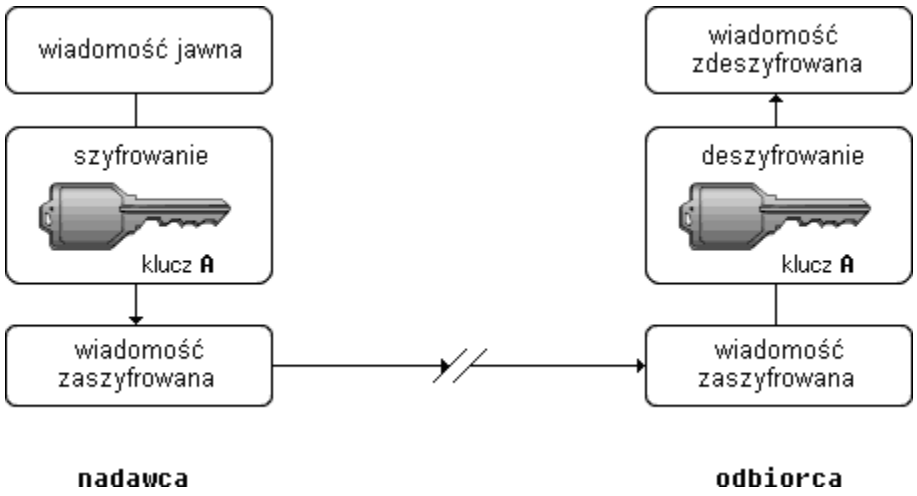
Aby można było stosować opisaną powyżej metodę do bezpiecznego przesyłania informacji, to odczytanie tekstu zaszyfrowanego bez znajomości algorytmu deszyfrującego powinno być bardzo trudne lub niemożliwe. Istnieje wiele metod spełniających te wymaganie. Najpopularniejsze z nich i najczęściej stosowane to szyfrowanie z kluczem tajnym i szyfrowanie z kluczem publicznym.

(4.2) Szyfrowanie z kluczem prywatnym

W szyfrowaniu z kluczem prywatnym (tajnym) zarówno odbiorca jak i nadawca posługują się tajnym kluczem służącym do szyfrowania i deszyfrowania wiadomości. Z tego powodu tego typu postępowanie nosi również nazwę szyfrowania symetrycznego.

Aby można było stosować tę metodę komunikacji muszą być dostępne następujące elementy:

- ogólny algorytm szyfrowania *E*;
- ogólny algorytm deszyfrowania *D*;
- tajny klucz (lub klucze) służący do szyfrowania i deszyfrowania informacji.



Rysunek 3. Szyfrowanie z kluczem prywatnym (symetryczne)

Klucze prywatne są powszechnie stosowane przez protokoły bezpieczeństwa, jako klucze sesji w poufnej komunikacji w trybie on-line. Na przykład protokół IPSec wykorzystuje symetryczne klucze sesji ze standardowymi algorytmami stosowanymi do szyfrowania i deszyfrowania poufnej komunikacji między stronami. Dla każdej poufnej sesji komunikacji używane są inne klucze.

Szyfrowanie symetryczne jest też powszechnie stosowane przez technologie zapewniające masowe szyfrowanie trwałych danych, takich jak wiadomości e-mail czy pliki typu dokument. Protokół S/MIME stosuje klucze symetryczne do szyfrowania wiadomości poufnej poczty, a system szyfrowania plików EFS w Windows 2000/XP używa symetrycznych kluczy do szyfrowania plików.

Powszechnie wykorzystywanym, symetrycznym algorytmem szyfrującym jest algorytm DES (*ang. data-encryption standard*), który w ogólnych założeniach wygląda następująco:

Jeśli przez E_k oznaczymy algorytm szyfrowania z kluczem k, a przez D_k – algorytm deszyfrowania z tym kluczem, to wówczas dla każdej wiadomości m muszą być spełnione następujące warunki:

1) $D_k(E_k(m))=m$ – oznacza to, że po zaszyfrowaniu wiadomości ($E_k(m)$) przesłaniu jej, a następnie odszyfrowaniu ($D_k(E_k(m))$) nie zgubimy informacji, czyli że proces szyfrowania i deszyfrowania nie zniekształca wiadomości;

2) Obliczenie E_k i D_k jest efektywne, czyli daje się wykonać w rozsądnym czasie przy zastosowaniu dostępnym zasobów obliczeniowych;

3) Bezpieczeństwo systemu zależy tylko od tajności klucza k, a nie od tajności algorytmów E i D - – oznacza to, że algorytmy szyfrowania (E) i deszyfrowania (D) mogą być ujawnione, a chronić należy jedynie wartość klucza k.

Szczegółowy opis działania algorytmu DES wykracza poza zakres tego wykładu.

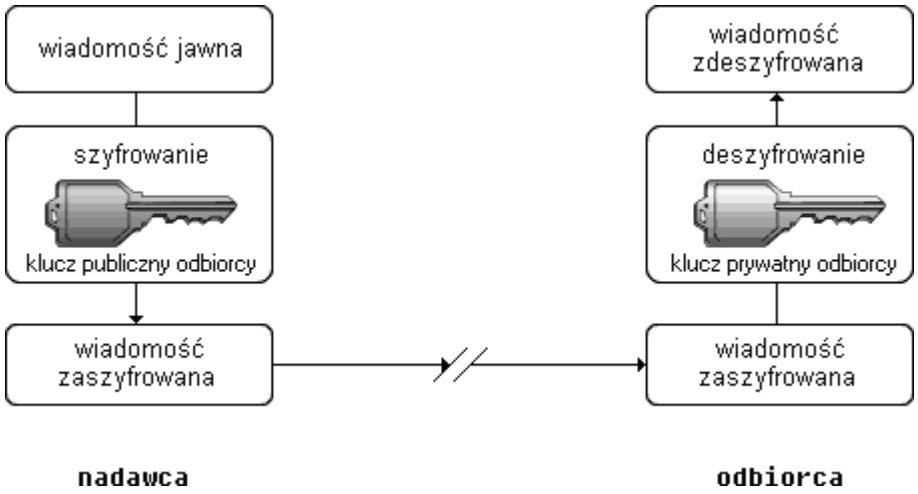
Gwałtowny wzrost mocy obliczeniowej komputerów doprowadził do tego, że obecnie algorytm DES można złamać w ciągu zaledwie kilku godzin. Dlatego opracowany został algorytm 3-DES (Triple DES), w którym zwiększone bezpieczeństwo uzyskano poprzez zastosowanie dwóch lub trzech kluczy. Dzięki zastosowaniu 3-DES czas potrzebny na złamanie szyfru znacząco się wydłuża – na dzień dzisiejszy liczony jest w milionach lat.

Problemem w szyfrowaniu symetrycznym jest przekazywanie kluczy. Aby zapewnić bezpieczeństwo informacji klucz taki musi pozostać tajny. Nie może więc być bezpośrednio przesłany przez sieć telekomunikacyjną, gdyż byłby narażony na łatwe przechwycenie.

Problem ten rozwiązano poprzez szyfrowanie z wykorzystaniem różnych kluczy do szyfrowania i deszyfrowania. Ten sposób szyfrowania nosi nazwę szyfrowania asymetrycznego (lub publicznego). Polega on na zastosowaniu dwu kluczy: jednego do szyfrowania wiadomości, a drugiego do deszyfrowania.

(4.3) Szyfrowanie z kluczem publicznym

W szyfrowaniu z kluczem publicznym każdy użytkownik dysponuje dwoma kluczami. Jeden z nich to klucz jawny służący do szyfrowania wiadomości. Drugi to klucz tajny, znany tylko odbiorcy wiadomości. Służy on do odszyfrowania wiadomości.



Rysunek 4. Szyfrowanie asymetryczne

Dwaj użytkownicy mogą się skutecznie porozumiewać znając swoje klucze jawne.

Zasada działania algorytmu szyfrowania opartego na kluczach prywatnych bazuje na własnościach matematycznych dużych liczb. Polega ona na tym, że mnożenie dwu nawet dużych, specjalnie dobranych liczb jest łatwe. Trudne jest natomiast wykonanie rozkładu liczby na czynniki (o ile liczba jest odpowiednio duża i dobrze dobrana). Oznacza to, że odszyfrowanie wiadomości bez znajomości klucza tajnego wymaga ogromnych mocy obliczeniowych (a co za tym idzie czasu) lub jest niewykonalne.

Najbardziej popularnym algorytmem z kluczem publicznym jest algorytm RSA opracowanym przez Ronalda Rivesta, Adi Shamira i Leonarda Adlemana. Bazuje on na trudności rozłożenia dużej liczby na czynniki pierwsze. Wykorzystuje funkcję Eulera Totient $\phi(n)$ zdefiniowaną jako ilość liczb naturalnych mniejszych od n i względnie pierwszych z n. Liczby m i n są względnie pierwszymi, jeśli nie mają wspólnych podzielników innych niż 1. Funkcja $\phi(n)$ zawsze przyjmuje wartość mniejszą niż n. Euler odkrył, że każda liczba k, względnie pierwsza z n podniesiona do potęgi $\phi(n)$ modulo n daje w wyniku 1:

$$k^{\phi(n)} \bmod n = 1$$

(a mod b oznacza resztę z dzielenia liczby a przez b. Na przykład 10 mod 3 =1; 4 mod 2 = 0)

W RSA wykorzystuje się jeszcze jedną własność. Jeżeli k i l są losowymi liczbami naturalnymi będącymi odwrotnościami modulo $\phi(n)$ oraz A jest dowolną liczbą względnie pierwszą z n to:

$$(A^k)^l \bmod n = (A^l)^k \bmod n = A.$$

Jeśli A jest częścią wiadomości wówczas szyfrowania dokonujemy za pomocą funkcji

$$S = A^k \bmod n \ ,$$

zaś deszyfrowania za pomocą funkcji

$$A = S^l \bmod n \ .$$

Wyboru kluczy szyfrujących dokonuje się w następujący sposób:

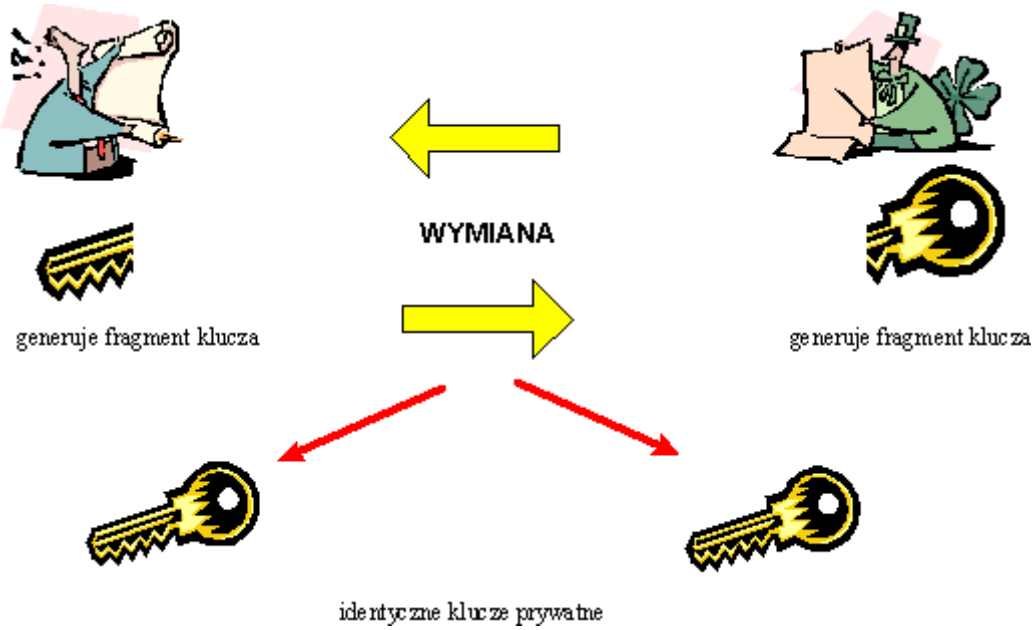
- losuje się dwie duże liczby pierwsze *p*, *q*;
- oblicza się *n* = *pq,* oraz wyznacza funkcję $\phi(n)$;
- losowo wybiera się liczbę *e* z przedziału *(1,* $\phi(n)$ *)*, względnie pierwszą z $\phi(n)$;
- wyznacza się liczbę *d* odwrotną do $e \bmod \phi(n)$, czyli $d = e^{-1} \bmod \phi(n)$;
- kluczami szyfrującymi są *k* = *(n, e)* oraz *l* = *(n, d)*.

Dysponując kluczami szyfrujemy wiadomość *A*.

W algorytmie RSA liczby *n* oraz *k* lub *l* można wyjawiać bez poważnego narażenia bezpieczeństwa. Do złamania szyfru potrzebna jest funkcja $\phi(n)$ zaś do jej znalezienia musimy rozłożyć *n* na czynniki pierwsze, co jest zadaniem bardzo trudnym. W praktyce stosuje się klucze o długości 512–1024 bitów. W 1999 roku rozkład na czynniki pierwsze liczby 512-bitowej zajął trzystu szybkim stacjom około siedmiu miesięcy. Dlatego klucze o takiej długości nie stanowią obecnie dobrego zabezpieczenia.

W praktyce często stosuje się połączenie metody szyfrowania symetrycznego i asymetrycznego. Ponieważ szyfracja i deszyfracja wiadomości przy użycia klucza prywatnego jest dużo szybsza niż przy stosowaniu klucza publicznego, więc przy komunikacji dwu stron stosuje się następującą metodę. Klucze prywatne nadawcy i odbiorcy przekazuje się stosując metodę szyfrowania z kluczem publicznym. Klucz taki może więc być bezpiecznie przekazany przez publiczną sieć telekomunikacyjną. Następnie wiadomości mogą być już przekazywane przy zastosowaniu szyfrowania metodą klucza prywatnego.

Każdy z rozmówców generuje fragment klucza prywatnego i przed przesłaniem do partnera szyfruje go stosując metodę szyfrowania z kluczem publicznym.



Rysunek 5. Wymiana kluczy prywatnych

NASTĘPNA

5. Bezpieczenstwo w systemie Windows 2000

W systemie Windows 2000 stosowany jest system Kerberos oraz dodatkowe mechanizmy zabezpieczające na poziomie protokołu IP oraz szyfrowanie plików z kluczem publicznym.

System Kerberos został opracowany w Massechusetts Institute of Technology w latach osiemdziesiątych XX wieku. Został on zaimplementowany w wielu systemach uniksowych i internetowych.

Kerberos jest dwukierunkowym mechanizmem uwierzytelniania z udziałem zaufanej trzeciej strony. Protokół ten przyjmuje założenie, że transakcje zachodzące między klientami i serwerami mają miejsce w sieci otwartej, czyli w środowisku, gdzie większość klientów i serwerów nie jest fizycznie zabezpieczona, a przesyłane pakiety sieciowe mogą być z łatwością monitorowane i modyfikowane. Kerberos zaprojektowany jest dla środowiska przypominającego dzisiejszą sieć Internet, w której niepowołane osoby z łatwością mogą podszywać się pod klienta lub pod serwer oraz mogą przechwycić lub przekształcić dane przesłane w ramach połączenia między legalnymi klientami i serwerami.

Kerberos stosuje do utajniania informacji algorytm szyfrowania symetrycznego DES (algorytm z kluczem tajnym), który jest najlepiej znanym i najszerzej stosowanym w świecie algorytmem kryptograficznym. Podczas używania systemu DES, należy zwrócić uwagę na kilka czynników, które mają wpływ na bezpieczeństwo szyfrowanych danych. Należy często zmieniać klucze kryptograficzne, aby uniknąć ataku przez przedłużoną analizę danych oraz nadawca i odbiorca komunikacji muszą znaleźć bezpieczną metodę przekazywania sobie nawzajem kluczy DES. Kerberos zapewnia mechanizmy gwarantujące bezpieczną wymianę kluczy oraz pozwala na ograniczanie czasu ich ważności, przez co wymusza ich częste zmiany.

W systemie Kerberos wyróżnić można cztery podstawowe jednostki:

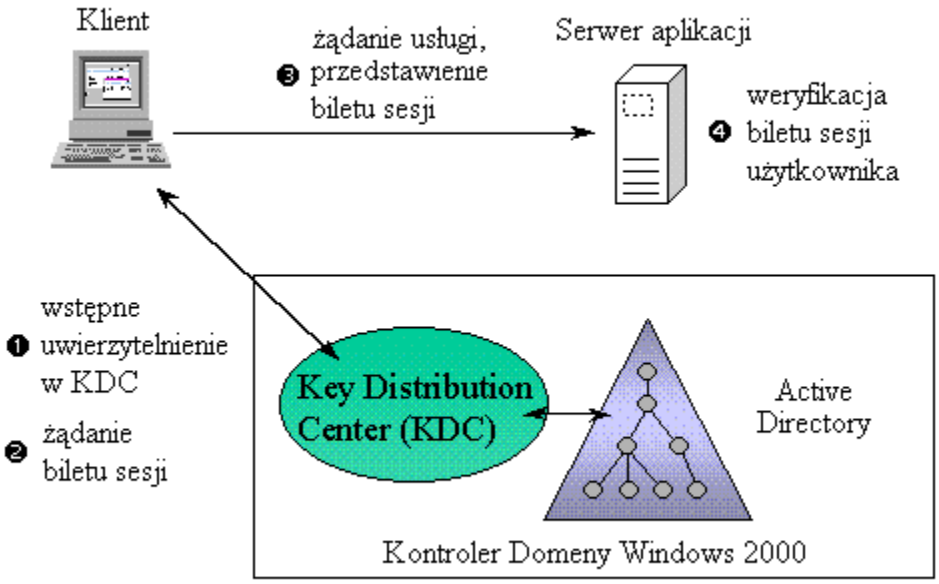
- klient – stacja robocza;
- serwer uwierzytelniający AS (ang. *Autentication Server*);
- serwer przyznawania biletów TGS (ang. *Ticket Granting Server*);
- serwer aplikacji AP (ang. *Application Server*).

Procedura uwierzytelniania wymaga wymiany informacji trzech typów (tzw. transakcji). Pierwsza wymiana zachodzi między klientem i serwerem uwierzytelniającym AS. Zadaniem tej wymiany jest sprawdzenie przez serwer AS autentyczności użytkownika. Uwierzytelniony użytkownik otrzymuje informację potrzebną do zainicjowania wymiany z serwerem przyznawania biletów TGS. Druga wymiana zachodzi między klientem i serwerem TGS. W jej wyniku użytkownik otrzymuje bilet uprawniający do dostępu do określonego serwera usług AP. Trzecia wymiana zachodzi między klientem i serwerem AP. Użytkownik za pomocą biletu otrzymanego od serwera

TG może udowodnić serwerowi AP, że jest legalnym użytkownikiem

Kerberos jest podstawowym elementem bezpieczeństwa w systemie NT 2000.

W systemie Windows 2000 usługa uwierzytelniania (AS) oraz usługa przydzielania biletów (TGS) zaimplementowane są jako jedna usługa KDC (ang. *Key Distribution Center*). Usługa KDC znajduje się na każdym kontrolerze domeny (czyli komputerze, który zarządza grupą komputerów tworzących tak zwaną domenę) i korzysta z usługi Active Directory (centralna baza kontrolera domeny) jako bazy danych przechowujących konta podmiotów zabezpieczeń wraz z dodatkowymi informacjami.



Rysunek 6. Kerberos w Windows 2000

Podstawowym elementem systemu Kerberos jest żeton. Jest to rodzaj certyfikatu, który jest wydawany przez usługę Kerberosa jako potwierdzenie, że wyrażono zgodę na ustanowienie sesji.

Kiedy komputer PC chce uzyskać dostęp do informacji przechowywanych na serwerze w obrębie tej samej domeny, musi przejść przez proces weryfikacji tożsamości w sieci. W praktyce ta weryfikacja tożsamości może zostać podzielona na sekwencję zdarzeń zachodzących pomiędzy klientem a KDC.

Kerberos stosuje komunikaty do dostarczenia każdemu z komponentów systemu Kerberos koniecznych informacji dotyczących tego co zaszło podczas procesu weryfikacji tożsamości. Jak już powiedziałem, wiele z tych komunikatów jest szyfrowanych i zawiera znaczniki czasu, które zapobiegają możliwości przechwycenia pakietu za pomocą tradycyjnych urządzeń przechwytujących i powtórnemu wykorzystaniu go w późniejszym czasie, bez zauważenia czegokolwiek podejrzanego przez mechanizm zabezpieczeń.

Poniżej opisana została typowa sekwencja czynności realizowanych podczas weryfikacji tożsamości klienta na określonym serwerze (lub usłudze):

1, Klient przesyła do KDC zwyczajny komunikat tekstowy, prosząc o żeton umożliwiający wymianę informacji z KDC. Komunikat przesyłany przez klienta zawiera nazwę użytkownika, nazwę serwera KDC lub usługi oraz znacznik czasu.

2. KDC przesyła klientowi zaszyfrowaną odpowiedź. Ten komunikat jest szyfrowany za pomocą hasła klienta i zawiera klucz sesji opatrzony znacznikiem czasu, który będzie wykorzystywany przy wymianie informacji z KDC, oraz żeton TGT, który klient może wykorzystać do uzyskania kolejnych żetonów umożliwiających korzystanie z wybranych usług w obszarze dziedziny KOC.

3. Klient przesyła KDC zaszyfrowany komunikat, w którym prosi o prawo do komunikowania się z wybranym serwerem lub usługą. Klient szyfruje ten komunikat za pomocą klucza sesji otrzymanego od KDC. Komunikat zawiera nazwę serwera lub usługi, z której klient chce korzystać, znacznik czasu oraz żeton TGT. Gdy KDC otrzymuje komunikat, może mieć pewność, że pochodzi on od właściwego klienta, gdyż komunikat jest deszyfrowany za pomocą jego klucza sesji. Następnie KDC tworzy wspólny klucz sesji, który jest wykorzystywany zarówno przez klienta, jak i przez serwer. KDC tworzy także specjalny żeton dla serwera, który zawiera klucz sesji, nazwę klienta, adres jego karty sieciowej, okres ważności żetonu oraz znacznik czasu.

4. KDC przesyła klientowi komunikat zawierający zaszyfrowany wspólny klucz sesji oraz zaszyfrowany żeton. Wspólny klucz sesji jest szyfrowany za pomocą klucza sesji posiadanego przez klienta, natomiast żeton -za pomocą klucza sesji posiadanego przez serwer.

5. Klient przesyła do serwera komunikat informujący, że ma prawo do komunikowania się z nim. (To, czy kolejne prośby serwera zostaną wykonane, zależy oczywiście od systemu bezpieczeństwa serwera). Komunikat zawiera zaszyfrowany żeton, który klient otrzymał od KDC, oraz czasowy identyfikacyjny znacznik czasu zaszyfrowany za pomocą wspólnego klucza sesji. Serwer deszyfruje nadesłany żeton za pomocą swojego własnego hasła. Żeton ten zawiera kopię wspólnego klucza sesji oraz kilka innych bardzo istotnych informacji dotyczących klienta. Serwer używa wspólnego klucza sesji do odszyfrowania identyfikacyjnego znacznika czasu, aby określić, kiedy klient wysłał komunikat. jeśli komunikat został wysłany w okresie ważności żetonu oraz jeśli wszystkie inne warunki zostaną poprawnie spełnione, to serwer zaakceptuje prośbę klienta.

6. Po zatwierdzeniu klienta serwer przesyła zaszyfrowany komunikat, informując klienta o udzieleniu zezwolenia na komunikację. Ten komunikat zawiera identyfikacyjny znacznik czasu, który klient przesłał na serwer w kroku 5. Identyfikacyjny znacznik czasu zaszyfrowany jest za pomocą wspólnego klucza sesji.

NASTĘPNA

Podsumowanie

Współczesne systemy informatyczne podlegają wielu zagrożeniom zarówno wewnętrznym jak i zewnętrznym. Konieczne stało się więc zaimplementowanie mechanizmów ochronnym, pozwalających w skuteczny sposób zabezpieczyć system i gromadzone w nim informacje przed celowym lub przypadkowych uszkodzeniem, utratą bądź kradzieżą danych. Większość systemów operacyjnych dostarcza odpowiednich mechanizmów do realizacji polityki ochrony. Polityka ta jest równie ważna jak stosowane zabezpieczenia systemów. Należy więc ściśle przestrzegać ustalonych zasad. Podstawowe reguły bezpieczeństwa dotyczą wszystkich systemów od pojedynczego domowego stanowiska aż po wielkie systemy korporacyjne. Oczywiście poziom zabezpieczeń jest w każdym wypadku inny , ale nawet w swoim domowym komputerze warto jest dbać o wykonywanie kopii zapasowych i ochronę antywirusową.

Wraz z rozwojem Internetu i usług sieciowych wzrasta również konieczność bezpiecznego przesyłania danych. Dzięki rozwojowi kryptografii i technik matematycznych możliwe jest dziś bezpieczne komunikowanie się w sieci publicznej. najpopularniejszymi metodami stosowanymi w tego rodzaju wymianie danych jest szyfrowanie wiadomości z kluczem publicznym lub prywatnym oraz wykorzystanie certyfikatów i podpisów elektronicznych.

Dodatek

Dodatek zawiera materiał nieobowiązkowy. Dotyczy on standardów i klas bezpieczeństwa systemów zalecanych przez światowe organizacje. Polecamy go osobom szczególnie zainteresowanym sprawom bezpieczeństwa systemów.

Normy w zakresie bezpieczeństwa systemów

Fakt istnienia zróżnicowanego sprzętu i oprogramowania pochodzącego od różnych producentów wskazuje na potrzebę opracowania międzynarodowych norm pozwalających na ocenę systemu informatycznego pod względem bezpieczeństwa. Aby móc określić poziomy (klasy) bezpieczeństwa w sposób zunifikowany nakreślono wspólne kryteria, a standardy przedstawione poniżej powinny stanowić ramy polityki bezpieczeństwa systemu informacyjnego.

„Pomarańczowa księga"

W 1983 roku Departament Obrony USA oficjalnie ogłosił „Kryteria oceny zaufania systemów komputerowych" TCSEC (ang. *Trusted Computer System Evaluation Criteria*) znane także pod nazwą „Pomarańczowej księgi" (ang. *Orange Book*).

„Pomarańczowa księga" definiuje cztery poziomy bezpieczeństwa – od D do A, które podzielone są na klasy oznaczone liczbowo tak, że bezpieczeństwo klasy w ramach poziomu rośnie wraz ze zwiększaniem się numeru. Każdy poziom i klasa charakteryzowane są przez cztery elementy:

- polityka bezpieczeństwa (ang. *security policy*);
- identyfikacja, kontrola i sprawdzanie podmiotu (ang. *accountability*);
- ubezpieczenie eksploatacyjne i okres trwałości ubezpieczenia (ang. *assurance*);
- opis sposobu zabezpieczania systemów (ang. *documentation*).

Poziom D

Klasa Dl bezpieczeństwa jest najniższą w systemie certyfikacyjnym Departamentu Obrony USA. Nie zapewnia ona ochrony ani plikom, ani użytkownikom. Przykładem takiego systemu jest system operacyjny taki jak Microsoft Windows 95/98.

Poziom C

Klasy poziomu C świadczą o tym, że system zapewnia bezpieczeństwo uznaniowe, polegające na przyznawaniu praw do danych tylko tym pracownikom, którzy muszą mieć do nich dostęp. Zabezpieczenia takie umożliwiają śledzenie operacji wykonywanych przez użytkowników. Istnieją

dwie klasy poziomu C - C1 i C2.

Klasa Cl

Sprawdzona instalacja – TCB (ang. *Trusted Computing Base*) systemu klasy Cl spełnia wymagania dotyczące zapewnienia bezpieczeństwa uznaniowego izolując użytkowników i dane. System klasy Cl zawiera niezawodny mechanizm kontrolowania, który umożliwia nakładanie ograniczeń na indywidualnych użytkowników. Pozwala on na zabezpieczanie swoich prywatnych danych oraz informacji dotyczących wykonywanych zadań przed przypadkowym odczytaniem lub zniszczeniem przez innych użytkowników. Wszystkie informacje są zabezpieczone w taki sam sposób, a żaden dokument w tym systemie nie jest chroniony efektywniej niż inne. System NetWare 3.11 i wersje wcześniejsze są przykładami klasy Cl. Należy pamiętać, że wszystkie komputery przyłączone do sieci są klasy D1, ponieważ są fizycznie narażone na atak. Oto minimalne wymagania dla systemu klasy Cl:

- określony i kontrolowany dostęp nazwanych użytkowników do nazwanych obiektów;
- system identyfikacyjny i sprawdzający hasła, decydujący o przyznaniu użytkownikom dostępu do informacji w sieci komputerowej.

Klasa C2

System klasy C2 umożliwia sprawowanie pełniejszej kontroli niż ma to miejsce w wypadku klasy Cl. Użytkownicy systemu klasy C2 są osobiście odpowiedzialni za wykonywane przez siebie operacje sieciowe. Ta odpowiedzialność wymuszana jest poprzez zastosowanie procedury logowania, wykrywane zdarzeń związanych z bezpieczeństwem oraz izolowanie poszczególnych zasobów sieciowych. Systemy zaliczone do klasy C2 muszą, oprócz wymagań klasy Cl, spełniać także kilka dodatkowych:

- możliwość decydowania o dostępie grup i indywidualnych użytkowników;
- mechanizm kontrolowania dostępu ogranicza replikację praw dostępu;
- uznaniowy mechanizm kontrolowania dostępu domyślnie lub na podstawie jawnego żądania użytkownika uniemożliwia nieautoryzowany dostęp do obiektów;
- mechanizm kontrolowania dostępu może dopuszczać lub ograniczać dostęp użytkowników do określonych obiektów;
- system identyfikowania może rozpoznać każdego użytkownika, który się loguje do sieci;
- system operacyjny wykonuje wszystkie operacje zlecane przez poszczególnych użytkowników

zgodnie z nadanymi im prawami;

- system może śledzić dostęp do obiektów w sieci.

Poziom B

W „Pomarańczowej księdze” podzielono poziom B na trzy klasy: Bl, B2 i B3. Musi on zapewniać obowiązkowe zabezpieczenia, czym różni się od poziomu C i oznacza,
że poziom wejściowy takiego systemu musi działać na podstawie pewnych zasad. Innymi słowy, każdemu obiektowi jest przyporządkowana ocena poziomu bezpieczeństwa, a system nie zezwoli użytkownikowi na zapisanie obiektu bez takiej oceny.

Klasa Bl

System klasy B1 musi spełniać wszystkie wymagania klasy C2, a ponadto wymaga się nieoficjalnego zapewnienia o istnieniu w systemie modelu zasad bezpieczeństwa oraz modelu obowiązkowej kontroli dostępu obejmujących użytkowników i obiekty. Oprócz tego system ten musi spełniać poniższe wymagania:

- system musi umożliwiać stosowanie „etykiet” oznaczających ważność wszystkich kontrolowanych obiektów. Można na przykład oznaczyć dane dotyczące sprzedaży etykietą „ważne”, a prognozy zawierające informacje bankowe etykietą „niezwykle ważne”;

- system kontroluje dostęp do danych na podstawie etykiet, którymi je opatrzono;

- przed umieszczeniem w systemie importowanych obiektów, zostaną one opatrzone etykietami. System nie zezwoli na posługiwanie się nieoznaczonymi obiektami;

- podczas tworzenia systemu, dodawania nowych kanałów komunikowania się
lub nowych urządzeń wejścia–wyjścia, administrator musi oznaczyć je jako jedno lub wielopoziomowe. Oznaczenia tego nie można zmienić automatycznie – operację taką trzeba wykonać ręcznie;

- urządzenia wielopoziomowe nie modyfikują oznaczenia stopnia ważności danych przesyłanych z sieci;

- urządzenia jednopoziomowe nie zachowują takiego oznaczenia przesyłanych danych;

- operacja wysyłania danych wyjściowych do użytkownika, w formie nietrwałej
lub trwałej , musi tworzyć etykietę oznaczającą ważność tych danych;

- system musi korzystać z haseł i identyfikować użytkownika w celu określenia jego praw dostępu. Ponadto na podstawie praw użytkownika system musi podejmować decyzję

o przyznaniu mu dostępu do obiektów;

- system musi rejestrować próby uzyskania nieautoryzowanego dostępu.

Klasa B2

Systemy klasy B2 muszą spełniać wszystkie wymagania klasy Bl, a ponadto administrator zabezpieczeń jest zobowiązany oprzeć sprawdzoną instalację systemu na jasno zdefiniowanym i udokumentowanym modelu zasad bezpieczeństwa. Model ten w systemie klasy B2 musi rozbudować mechanizmy uznaniowego i obowiązkowego kontrolowania dostępu obecne w Bl, tak aby obejmowały one wszystkich użytkowników oraz obiekty. System taki rozwiązuje niejawne problemy i jest podzielony na elementy kluczowe dla bezpieczeństwa oraz elementy, które nie są dla niego kluczowe. Jest on stosunkowo odporny na ataki. System klasy B2 musi spełniać również poniższe wymagania:

- system natychmiast powiadamia każdego użytkownika o zmianach wprowadzonych w systemie bezpieczeństwa, które jego dotyczą;

- podczas początkowego logowania się i w trakcie uwiarygodniania system korzysta z pewnego kanału komunikacyjnego łączącego go z użytkownikiem. Jedynie użytkownik może rozpocząć wymienianie informacji za pośrednictwem tego kanału;

- twórca systemu przeprowadzi dokładne poszukiwania ukrytych kanałów umożliwiających przesyłanie informacji i określi maksymalną przepustowość każdego z nich;

- sprawdzona instalacja systemu pozwala na korzystanie z oddzielnych funkcji operatora i administratora;

- w projektowaniu systemu musi wziąć udział osoba, której obowiązkiem będzie informowanie odpowiednich władz o wszelkich zmianach wprowadzonych do projektu systemu oraz uzyskanie ich aprobaty.

Klasa B3

System klasy B3 musi spełniać wszystkie wymagania klasy B2, a ponadto jego twórcy muszą pamiętać o zapewnianiu dostępu tylko tym osobom, którym nadano odpowiednie prawa, a także o uodpornieniu systemu na wszelkie próby wdarcia się do niego. Musi być on także wystarczająco zwarty, aby można go było poddać analizom i testom. Ze sprawdzonej instalacji systemu należy usunąć cały kod, który nie jest kluczowy z punktu widzenia zasad bezpieczeństwa, natomiast projektanci powinni zapewnić małą złożoność systemu, co łatwi jego analizowanie. Należy także wyznaczyć administratora zabezpieczeń, wyposażyć go w mechanizmy kontrolne oraz procedury uruchamiania systemu po awarii. System klasy B3 jest bardzo odporny na ataki. Poniżej przedstawiono minimalne wymagania, które powinien on spełniać:

- oprócz dostępnej w systemie klasy B2 możliwości kontrolowania dostępu do obiektów i indywidualnych użytkowników, musi zapewnić również możliwość tworzenia czytelnej dla człowieka listy bezpieczeństwa, na której znajdują się wszyscy użytkownicy sieci wraz z prawami dostępu do wszystkich obiektów systemu;

- wszystkie obiekty korzystają z listy użytkowników, którzy nie mają dostępu do konkretnego obiektu;

- system potwierdza tożsamość użytkownika przed wykonaniem jakichkolwiek operacji;

- system identyfikuje użytkownika nie tylko wewnętrznie, ale również za pomocą zewnętrznych protokołów bezpieczeństwa i nie przyzna dostępu użytkownikom, którzy nie spełnią wymagań tych protokołów, nawet jeśli spełnią oni inne wymagania systemu. Ponadto taka próba uzyskania dostępu zostanie zarejestrowana;

- projektanci systemu muszą odizolować pewne kanały komunikacyjne od innych;

- sprawdzona instalacja systemu rejestruje wszelkie operacje wykonywane przez użytkowników na nazwanych obiektach. Ponadto każda próba wykonania operacji spowoduje zarejestrowanie informacji o niej w celach kontrolnych;

- sprawdzona instalacja systemu rozdziela poszczególne funkcje administratora zabezpieczeń;

- system musi uruchamiać się po awarii bez obniżenia poziomu bezpieczeństwa.

Poziom A

Najwyższym poziomem bezpieczeństwa przywidzianym w „Pomarańczowej księdze" jest poziom A, który posiada obecnie tylko jedną klasę. Jest ona przyznawana systemom korzystającym z metod weryfikacji. Metody te gwarantują, że obowiązkowe i uznaniowe mechanizmy kontrolne zastosowane w systemie efektywnie chronią poufne oraz ważne dane gromadzone lub przetwarzane w systemie. Uzyskanie poziomu A przez konkretny system wymaga przedstawienia obszernej dokumentacji świadczącej o spełnieniu wszelkich wymagań.

Klasa Al

Systemy klasy Al nie różnią się funkcjonalnie od klasy B3, dlatego nie wymaga się tu żadnych dodatkowych funkcji lub zasad bezpieczeństwa. Projektanci systemu klasy Al muszą przeprowadzić analizę jego specyfikacji, a następnie procedury weryfikujące zgodność z założeniami tej specyfikacji. System klasy Al musi spełniać poniższe wymagania:

- administrator zabezpieczeń systemu musi otrzymać od autorów systemu oficjalny model zasad bezpieczeństwa, który jasno opisuje wszelkie jego zasady. Musi on także zawierać matematyczny dowód zgodny z założeniami i zasadami bezpieczeństwa;

- wszystkie części systemu klasy Al muszą mieć administratora zabezpieczeń;
- administrator zabezpieczeń instaluje system klasy Al, dokumentuje każdą wykonaną operację i wykazuje, że system jest zgodny z zasadami bezpieczeństwa i oficjalnym modelem.

Do podstawowych zarzutów kierowanych pod adresem twórców „Pomarańczowej księgi" należy zaliczyć fakt, że przy opracowywaniu uwzględniono bezpieczeństwo przechowywania (poufność) danych, a mniejszą uwagę zwrócono na integralność danych i niezawodność systemu. Z badań jakie przeprowadzono wynika,
że większość firm zadowala poziom bezpieczeństwa klasy C2.

W 1987 roku opublikowano zmodyfikowany dokument (ang. *Trusted Network Interpretation of TCSEC*) znany pod nazwą „Czerwona księga" (ang. *Red Book*). Dodatkowo w 1991 roku opracowano kolejną modyfikację (ang. *Trusted Database Interpretation*), który uwzględniał potrzebę oceny systemów aplikacyjnych nie mieszczących się w pojedynczej klasie bezpieczeństwa widzianej z poziomu systemu operacyjnego.

Kryteria ITSEC

Standard ITSEC (ang. *Information Technology Security Evaluation Criteria*) został opracowany wspólnie przez kilka państw na podstawie wcześniejszych standardów o zasięgu krajowym: TCSEC ze Stanów Zjednoczonych, ZSIEC z 1989 roku z Niemiec, GESG2 i DTIEC z Anglii oraz SCSSI z Francji.

ITSEC definiuje 10 klas funkcjonalności systemu, z których 5 ma odpowiedniki w „Pomarańczowej księdze" (F-C1, F-C2, F-B1, F-B2, F-B3). Dodatkowo utworzono
5 klas o podwyższonych wymaganiach:

- F-IN – wysokie wymagania związane z integralnością danych i programów;
- F-AV – wysokie wymagania związane z dostępnością systemu lub jego funkcji;
- F-DI – wysokie wymagania co do integralności w czasie transmisji;
- F-DC – wysokie wymagania co do poufności w czasie transmisji;
- F-DX – wysokie wymagania co do poufności i integralności w czasie transmisji.

ITSEC definiuje także trzy poziomy odporności (podstawowy, średni i wysoki) na bezpośredni atak oraz siedem poziomów zaufania (od E0 do E6) co do poprawności implementacji funkcji i mechanizmów bezpieczeństwa. Na każdy wyższy poziom składają się tu wymagania niższego oraz pewne dodatkowe. Równorzędność poziomów klasyfikacyjnych według ITSEC, „Pomarańczowej księgi" oraz CCITSE przedstawia tabela 1.

Tabela 1. Kompatybilność standardów TCSEC, ITSEC i CCITSE

Lp.	TCSEC	ITSEC	CCITSE
1.	D	E0	EAL0

2.	C1	F-C1, E1	EAL1
3.	C2	F-C2, E2	EAL2
4.	B1	F-B1, E3	EAL3
5.	B2	F-B2, E4	EAL4
6.	B3	F-B3, E5	EAL5
7.	A1	F-B3, E6	EAL6

W celu ujednolicenia wymagań opracowany został standard jednolitych kryteriów oceny bezpieczeństwa technologii informatycznych CCITSE. Do prac nad nim powołano międzynarodową komisję standaryzacyjną CCIB, która współpracuje z ISO. Wersja 1.0 została opublikowana w styczniu 1996 roku, wersja 2.0 - w maju 1998 roku, natomiast ostateczna wersja dokumentu w postaci składającego się z trzech części standardu ISO/IEC 15408 jesienią 1999 roku.

Standard CCITSE (ang. *Common Criteria for Information Technology Security Evaluation*) definiuje kryteria, stanowiące podstawę do oceny właściwości bezpieczeństwa systemów informatycznych oraz dostarcza zbioru wymagań nakładanych na systemy. Wymagania funkcjonalne zostały podzielone na kilka klas, w których wyróżnia się rodziny funkcji.

Klasy wymagań funkcjonalnych

Do klas wymagań funkcjonalnych należą:

- audyt bezpieczeństwa (klasa PAU);
- komunikacja (klasa FCO);
- ochrona kryptograficzna (klasa FCS);
- ochrona zasobów użytkownika (klasa FDP);
- identyfikacja i uwierzytelnianie (klasa FIA);
- zarządzanie bezpieczeństwem (klasa FMT);
- prywatność (klasa FPR);
- ochrona funkcji i danych związanych z bezpieczeństwem (klasa FPT);
- dostępność zasobów (klasa FRU);
- kontrola ustanawiania sesji użytkownika (klasa FTA);

- bezpieczeństwo komunikacji między użytkownikiem a systemem bezpieczeństwa oraz między systemami bezpieczeństwa (klasa FTP).

W standardzie zdefiniowano także osiem poziomów pewności działania mechanizmów bezpieczeństwa, które są do pewnego stopnia zgodne z tymi definiowanymi w standardach TCSEC i ITSEC.

W 1987 r. Międzynarodowa Organizacja Standaryzacyjna (ISO) wspólnie z Międzynarodową Komisją Elektrotechniczną (IEC) utworzyły Połączony Komitet Techniczny nr 1 (JTC 1) w celu tworzenia norm w zakresie technologii informatycznych. Opracował on między innymi standardy dotyczące zasad bezpieczeństwa dla warstw modelu ISO OSI, technik kryptograficznych, zarządzania bezpieczeństwem i oceny bezpieczeństwa systemów informacyjnych oraz standardy w zakresie bezpieczeństwa bankowości. Zestawienie wyżej wymienionych norm zawiera dodatek B.

W Polskim Komitecie Normalizacyjnym opracowano polskie wersje standardów ISO/IEC, wśród których znajdują się normy dotyczące bezpieczeństwa.