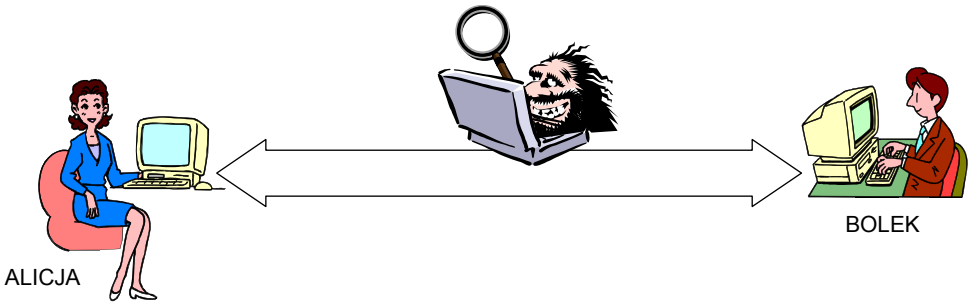
2. Podstawowe definicje i problemy

Klasy ataków

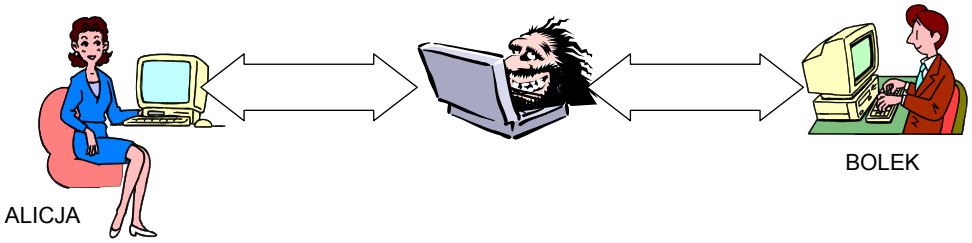
pasywne / aktywne

Pod względem interakcji atakującego z atakowanym systemem wyróżniamy ataki:

- pasywne – atakujący ma dostęp do danych (komunikacji) w systemie, mogąc je odczytać, lecz ich nie modyfikuje – przykład: podsłuch komunikacji pomiędzy legalnymi użytkownikami systemu.



- aktywne – atakujący pośredniczy w przetwarzaniu danych (komunikacji) w systemie, mogąc je nie tylko odczytać, lecz również sfałszować czy spreparować z premedytacją, tak by uzyskać zamierzony cel ataku – taki atak nazywa się popularnie „człowiek w środku” (ang. „*man in the middle*”).



lokalne / zdalne

Pod względem źródła rozpoczęcia ataku wyróżniamy ataki:

- lokalny – atakujący już ma dostęp do systemu (konto) i próbuje zwiększyć swe uprawnienia
- zdalny – atakujący nie posiada jeszcze żadnych uprawnień w systemie atakowanym

Ogólne formy ataku elektronicznego

Najczęściej spotykanymi formami ataku są:

- podszywanie (ang. *masquerading*) – atakujący (osoba, program) udaje inny podmiot, w domyśle zaufany systemowi atakowanemu, np. fałszywy serwer www podszywa się pod znaną witrynę internetową
- podsłuch (ang. *eavesdropping*) – pozyskanie danych składowanych, przetwarzanych lub transmitowanych w systemie – typowy przykład: przechwycenie niezabezpieczonego hasła klienta przesyłanego do serwera
- odtwarzanie (ang. *replaying*) – użycie ponowne przechwyconych wcześniej danych, np. hasła
- manipulacja (ang. *tampering*) – modyfikacja danych w celu zrekonfigurowania systemu lub wprowadzenia go do stanu, z którego atakujący może osiągnąć bezpośrednio lub pośrednio korzyść (np. zastosować skuteczny atak gotowym narzędziem)
- wykorzystanie luk w systemie (ang. *exploiting*) – posłużenie się wiedzą o znanej luce, błędzie w systemie lub gotowym narzędziem do wyeksploatowania takiej luki – bardzo częste w przypadku ataków zdalnych

Konkretne przypadki ataków ewoluują wraz z rynkiem informatycznym. Można np. przedstawić rys historyczny prawdopodobnie najbardziej typowych ataków przeprowadzanych w Internecie na przestrzeni ostatnich lat:

Ewolucja typowych ataków na przestrzeni lat

1993 r.	❍ wykorzystanie trywialnych haseł i znanych słabych punktów systemu ❍ analiza kodu źródłowego narzędzi systemowych w celu odkrycia nieznanych „dziur”
1995 r.	❍ ataki poprzez sniffery – przechwytywanie haseł ❍ wirusy, konie trojańskie ❍ ataki na sendmail ❍ ataki poprzez NFS i NIS
1998 r.	❍ IP spoofing, DNS spoofing ❍ ataki na routery, IP source routing, IP source porting
2000 r.	❍ IP hijacking, denial of service
2002 r.	❍ web-jacking (www hijacking), e-mail spamming ❍ dialery, malware (adware, spyware)
2005 r.	❍ web-phishing (*personal data fishing*),
	❍ spimming (ataki na komunikatory)

Podstawowe fazy ataku

W czasie przeprowadzania ataku pojawiają się zwykle mniej lub bardziej jawnie następujące ogólne fazy:

1. skanowanie (wyszukanie słabości, np. sondowanie usług)

2. wyznaczenie celu (np. niezabezpieczona usługa, znany exploit)
3. atak na system
4. modyfikacje systemu umożliwiające późniejszy powrót
5. usuwanie śladów
6. propagacja ataku

Podstawowe środki ostrożności

W celu zminimalizowania podatności na typowe ataki należy stosować elementarne zasady „higieny osobistej". Dotyczą one wszystkich komponentów systemu informatycznego, stanowisk komputerowych, infrastruktury sieciowej, usług aplikacyjnych.

Elementarna ochrona stacji roboczej

Do podstawowych środków ochrony stanowisk komputerowych można zaliczyć przykładowo:

- uniemożliwienie startowania systemu z nośników wymiennych
- ograniczenie wykorzystania przestrzeni lokalnych dysków twardych
- ograniczenie stosowania nośników wymiennych (stacji dyskietek, nagrywarek)
- rejestracja prób dostępu do systemu i ich limitowanie
  (kontrola, kto i kiedy korzystał z systemu)
- bezpieczne kasowanie poufnych danych
- uniemożliwienie usunięcia / wyłączenia zabezpieczeń, np. antywirusowych
- konsekwentna polityka haseł użytkowników

Elementarna ochrona sieci lokalnej

Do podstawowych środków ochrony infrastruktury sieciowej można zaliczyć przykładowo:

- dobór medium i topologii gwiazdy (okablowanie strukturalne)
- fizyczna ochrona pomieszczeń z węzłami sieci i serwerami
- zdefiniowanie listy stanowisk, z których dany użytkownik może uzyskać dostęp do systemu (adresy MAC lub IP)
- usuwanie nieużywanych kont użytkowników

Elementarna ochrona usług sieciowych

Procedura ochrony dostępu do usług sieciowych polega w ogólności na skrupulatnym przeprowadzeniu następującej sekwencji operacji:

1. usunięcie z systemu wszystkich usług zbędnych, najlepiej poprzez całkowite odinstalowanie, a co najmniej – dezaktywację

2. zastąpienie usług niezbędnych odpowiednikami o podwyższonym bezpieczeństwie (jeśli to możliwe i takie odpowiedniki są dostępne)

3. kontrola dostępu do pozostałych usług (np. poprzez zapory sieciowe *firewall*)

Złożoność problemu stosowania zabezpieczeń

Z realizacją zabezpieczeń związany jest szereg problemów, stawiających broniących od razu na pozycji gorszej niż atakującego. Dotyczą one m.in. asymetrii obrony i ataku, konieczności uwzględniania kontekstu całego otoczenia celu zabezpieczeń oraz trudności utrzymania poprawności zabezpieczeń (zarządzania i pielęgnacji).

- **asymetria**

  *Aby skutecznie zabezpieczyć system należy usunąć **wszystkie** słabości, aby skutecznie zaatakować – wystarczy znaleźć **jedną**.*

- **kontekst otoczenia systemu**

  Bezpieczeństwo powinno być rozważane w kontekście nie pojedynczego systemu informatycznego, ale całego otoczenia, w którym on się znajduje.

- **zarządzanie i pielęgnacja**

  Zabezpieczenie systemu nie jest pojedynczą operacją, ale ciągłym procesem.

Stosowanie mechanizmów bezpieczeństwa

W związku z w/w trudnościami realizacji zabezpieczeń istotne jest stosowanie kilku podstawowych reguł, w szczególności są to:

- zasada naturalnego styku z użytkownikiem
- zasada spójności poziomej i pionowej
- zasada minimalnego przywileju
- zasada domyślnej odmowy dostępu

Zasada naturalnego styku z użytkownikiem

Zabezpieczenie nie możne być postrzegane przez użytkowników jako nienaturalny element systemu, stanowiący utrudnienie w ich pracy. Jeśli wprowadzony zostanie nawet najbardziej wyrafinowany mechanizm bezpieczeństwa, którego jednak stosowanie będzie wymagało od użytkowników dodatkowo zbyt obciążających ich (czasochłonnych) operacji, to wkrótce wypracują oni sposób jego permanentnego obejścia i – w efekcie stanie się ów mechanizm bezużyteczny.

Zasada spójności poziomej i pionowej

Stosowanie zabezpieczeń w systemie musi zapewniać podstawowy warunek kompletności: spójność poziomą i pionową. Są one odpowiednikiem reguły „trwałości łańcucha”, która mówi, iż

cały łańcuch jest tak trwały, jak jego najsłabsze ogniwo. Spójność pozioma wymaga aby wszystkie, spośród potencjalnie wielu komponentów w danej warstwie systemu (jako dobry przykład modelu warstwowego można tu obrać model OSI obowiązujący w sieciach komputerowych), zostały zabezpieczone na jednakowym poziomie. W życiu codziennym spotykamy przykłady tej reguły – gdy zabezpieczamy okna pomieszczenia kratami, to wszystkie, a nie co drugie, gdy budujemy ogrodzenie, to do wysokości identycznie trudniej do sforsowania na całej jego długości. Gdy zabezpieczamy protokoły komunikacyjne danej warstwy modelu OSI, którymi posługuje się nasz system, to wszystkie niezbędne, a nie tylko jeden wybrany, choćby był on popularniejszy i częściej wykorzystywany od pozostałych.

Spójność pionowa mówi o konieczności zastosowania kompletnych zabezpieczeń „w pionie" – jak kraty w oknach na pierwszym piętrze, to i na parterze czy innej „dostępnej" z zewnątrz kondygnacji, analogicznie – jak jedna warstwa przez którą istnieje dostęp do systemu, to każda inna, w której niezależnie taki dostęp też jest możliwy.

Zasada minimalnego przywileju

Użytkownikom należy udzielać uprawnień w sposób zgodny z polityką bezpieczeństwa – tylko i wyłącznie takich, które są niezbędne do zrealizowania ich pracy. Zmianie zakresu obowiązków użytkownika powinna towarzyszyć zmiana zakresu uprawnień.

Zasada domyślnej odmowy dostępu

Jeśli na podstawie zdefiniowanych reguł postępowania mechanizmy obrony nie potrafią jawnie rozstrzygnąć, jaką decyzję podjąć wobec analizowanych operacji (np. nadchodzącego pakietu protokołu komunikacyjnego), to decyzją ostateczną powinna być odmowa dostępu (odrzucenie pakietu). Wiele urządzeń i protokołów jest jednak domyślnie konfigurowanych inaczej, czy to w celu wygody użytkownika, czy z założenia wynikającego z ich funkcji (por. routing).

Elementarne pojęcia

W celu przedstawienia problematyki ataku i obrony należy wprowadzić definicje niezbędnych pojęć. Dotyczyć one będą w szczególności użytkowników, ale także i innych komponentów systemu.

1. Identyfikacja (ang. *identification*)
    - możliwość rozróżnienia użytkowników, np. użytkownicy są identyfikowani w systemie operacyjnym za pomocą UID (*user identifier*)
2. Uwierzytelnianie (ang. *authentication*)
    - proces weryfikacji tożsamości użytkownika; najczęściej opiera się na tym:
        - co użytkownik wie (*proof by knowledge*), np. zna hasło
        - co użytkownik ma (*proof by possession*), np. elektroniczną kartę identyfikacyjną
3. Autoryzacja (ang. *authorization*)
    - proces przydzielania praw (dostępu do zasobów) użytkownikowi

4. Kontrola dostępu (ang. *access control*)
    - procedura nadzorowania przestrzegania praw (dostępu do zasobów)
5. Poufność (ang. *confidentiality*)
    - ochrona informacji przed nieautoryzowanym jej ujawnieniem
6. Nienaruszalność (integralność; ang. *data integrity*)
    - ochrona informacji przed nieautoryzowanym jej zmodyfikowaniem (ew. detekcja takiej modyfikacji)
7. Autentyczność (ang. *authenticity*)
    - pewność co do pochodzenia (autorstwa i treści) danych
8. Niezaprzeczalność (ang. *nonrepudiation*)
    - ochrona przed fałszywym zaprzeczeniem
        - przez nadawcę – faktu wysłania danych
        - przez odbiorcę – faktu otrzymania danych

Autoryzacja

Z procesem autoryzacji związane są kolejne pojęcia:

Zasób (obiekt)

- jest jednostką, do której dostęp podlega kontroli
- przykłady: programy, pliki, relacje bazy danych, czy całe bazy danych
- obiekty o wysokiej granulacji: poszczególne krotki bazy danych

Podmiot

- ma dostęp do zasobu
- przykłady: użytkownik, grupa użytkowników, terminal, komputer, aplikacja, proces

Prawa dostępu

- określają dopuszczalne sposoby wykorzystania zasobu przez podmiot

Filozofie przydziału uprawnień

W dowolnym modelu autoryzacji można stosować jedną z poniższych czterech możliwych filozofii:

1. Wszystko jest dozwolone.
2. Wszystko, co nie jest (jawnie) zabronione, jest dozwolone.

3. Wszystko, co nie jest (jawnie) dozwolone, jest zabronione.
4. Wszystko jest zabronione.

Z praktycznego punktu widzenia w grę wchodzić mogą środkowe dwie. Jak można zaobserwować, tylko trzecia jest zgodna z zasadą minimalnego przywileju i domyślnej odmowy dostępu.

Kontrola dostępu do danych

Wyróżnia się dwie ogólne metody kontroli dostępu do danych: uznaniową (DAC) i ścisłą. (MAC) Istnieją też ich różne warianty – jak np. kontrola oparta o role (RBAC) powszechnie spotykana np. systemach baz danych.

1. Uznaniowa kontrola dostępu (*Discretionary Access Control*)

Podstawowe własności tego podejścia są następujące:

- właściciel zasobu może decydować o jego atrybutach i uprawnieniach innych użytkowników systemu względem tego zasobu
- DAC oferuje użytkownikom dużą elastyczność i swobodę współdzielenia zasobów
- powszechnym zagrożeniem jest niefrasobliwość przydziału uprawnień (np. wynikająca z nieświadomości lub zaniedbań) i niewystarczająca ochrona zasobów
- najczęściej uprawnienia obejmują operacje odczytu i zapisu danych oraz uruchomienia programu

2. Ścisła kontrola dostępu (*Mandatory Access Control*)

Podstawowe własności tego podejścia są następujące:

- precyzyjne reguły dostępu automatycznie wymuszają uprawnienia
- nawet właściciel zasobu nie może dysponować prawami dostępu
- MAC pozwala łatwiej zrealizować (narzucić) silną politykę bezpieczeństwa i konsekwentnie stosować ją do całości zasobów

Ścisła kontrola dostępu operuje na tzw. poziomach zaufania wprowadzając **etykiety poziomu zaufania** (*sensitivity labels*) przydzielane w zależności np. od stopnia poufności. Mogą one być następjące:

ogólnie dostępne < do użytku wewn. < tylko dyrekcja < tylko zarząd

czy w innego typu instytucji:

jawne < poufne < tajne < ściśle tajne

Oprócz poziomu zaufania, każdy zasób posiada kategorię przynależności danych. Kategorie te nie są hierarchiczne i reprezentują jedynie rodzaj wykorzystania danych, np.:

FINANSOWE, OSOBOWE, KRYPTO, MILITARNE

W celu określenia uprawnień w systemach MAC są konstruowane **etykiety ochrony danych**. Składają się one z 2 parametrów: poziomu zaufania i kategorii informacji, np.

(tajne, {KRYPTO})
(ściśle tajne, {KRYPTO,MILITARNE})

Na zbiorze etykiet ochrony danych określona jest relacja wrażliwości:

(ściśle tajne, {KRYPTO,MILITARNE}) > (tajne, {KRYPTO})

Jest to relacja częściowego porządku, nie wszystkie etykiety do niej należą. Przykładowo może nie być określona relacja pomiędzy etykietą:

(ściśle tajne, {KRYPTO,MILITARNE})

a etykietą:

(tajne, {FINANSOWE,KRYPTO})

Wobec podmiotów i zasobów w systemie MAC narzucone są niezmienne reguły, które wymusza system. Podmiot nie może mianowicie czytać danych o wyższej etykiecie (*read-up*) niż swoja aktualna. Podmiot nie może również zapisywać danych o niższej etykiecie (*write-down*) niż swoja aktualna. Zbiór reguł przedstawia rysunek:

MAC 1:	Użytkownik może uruchomić tylko taki proces, który posiada etykietę nie wyższą od aktualnej etykiety użytkownika.
MAC 2:	Proces może czytać dane o etykiecie nie wyższej niż aktualna etykieta procesu.
MAC 3:	Proces może zapisać dane o etykiecie nie niższej niż aktualna etykieta procesu.

Reguły MAC

Klasy bezpieczeństwa systemów komputerowych

W historii dziedziny bezpieczeństwa systemów komputerowych od początku starano się stworzyć reguły klasyfikacji systemów. Opracowano standardy certyfikacji:

- Trusted Computer System Evaluation Criteria (TCSEC “Orange Book”) – USA http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html ; jest to standard opracowany w USA, ale stał się pierwszym powszechnym takim standardem w skali światowej. Owiązujący w latach 1983-2000 stał się podstawą opracowywania

podobnych norm w Europie i na świecie. Bardzo często nawet współcześnie znajduje się odwołania do certyfikatów tego standardu.

- Information Technology Security Evaluation Criteria (ITSEC) – EU http://www.cesg.gov.uk ; obowiązywał w 1991-1997. Powstał głównie z angielskiego CESG2/DTIEC, francuskiego SCSSI i niemieckiego ZSIEC.
- Common Criteria Assurance Levels (EAL) – aktualnie obowiązujący standard będący w istocie złączeniem ITSEC, TCSEC oraz CTCPEC (Kanada). Od 1996 powszechnie znany jako Common Criteria for Information Technology Security Evaluation (CC; http://www.commoncriteria.org). Od 1999 roku zaakceptowany jako międzynarodowa norma ISO15408 (EAL v.2).

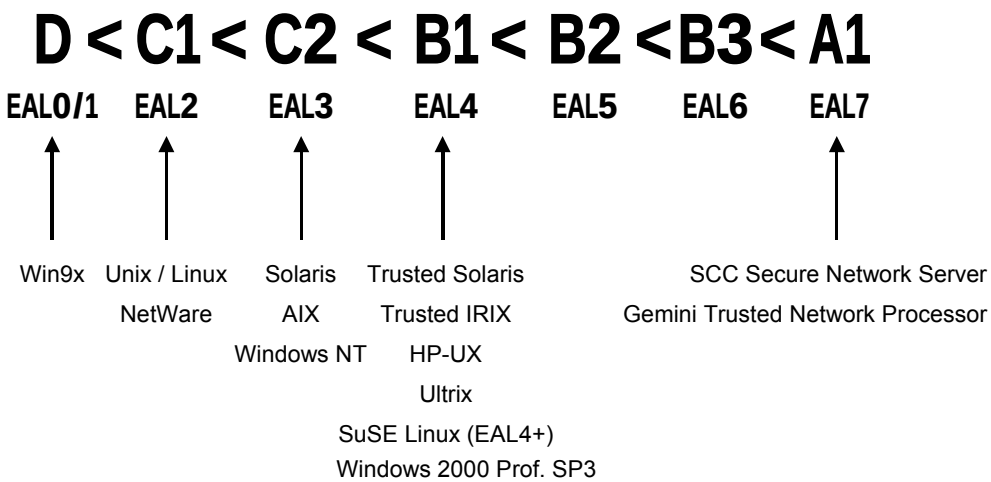
Poniżej zostaną przedstawione wymagania klas bezpieczeństwa systemów komputerowych wg oryginalnej propozycji TCSEC “Orange Book”. Schematyczne porównanie klas różnych standardów można znaleźć w tablece 1.

KLASA	WŁASNOŚCI
D	- minimalna ochrona (właściwie jej brak)
C1	- identyfikacja i uwierzytelnianie użytkowników, - hasła chronione - luźna kontrola dostępu na poziomie właściciela / grupy / pozostałych użytkowników - ochrona obszarów systemowych pamięci
C2	- kontrola dostępu na poziomie poszczególnych użytkowników - automatyczne czyszczenie przydzielanych obszarów pamięci - wymagana możliwość rejestracji dostępu do zasobów
B1	- etykietowane poziomy ochrony danych
B2	- ochrona strukturalna – jądro ochrony - weryfikacja autentyczności danych i procesów - informowanie użytkownika o dokonywanej przez jego proces zmianie poziomu bezpieczeństwa - wykrywanie zamaskowanych kanałów komunikacyjnych - ścisła rejestracja operacji
B3	- domeny ochronne - aktywna kontrola pracy systemu (security triggers) - bezpieczne przeładowanie systemu
A1	- formalne procedury analizy i weryfikacji projektu i implementacji systemu

Tabelka 1. Porównanie klas bezpieczeństwa systemów komputerowych

TCSEC	ITCES	CC / EAL
D	E0	EAL0
		EAL1
C1	E1, F-C1	EAL2
C2	E2, F-C2	EAL3
B1	E3, F-B1	EAL4
B2	E4, F-B2	EAL5
B3	E5, F-B3	EAL6
A1	E6, F-B3	EAL7

Popularne systemy operacyjne plasują się na różnych poziomach klas bezpieczeństwa. Trzeba zaznaczyć, iż uzyskanie certyfikatu danej klasy jest operacją formalną i odpłatną.



http://www.radium.ncsc.mil/tpep/
http://niap.nist.gov/cc-scheme/vpl/vpl_type.html