

Bezpieczeństwo systemów komputerowych

Podstawowe definicje i problemy

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

11 października 2011

Na podstawie materiałów Michała Szychowiaka
z <http://wazniak.mimuw.edu.pl>

Rodzaje ataków ze względu na interakcję

- ▶ **Pasywny** – agresor ma dostęp do danych (komunikacji), może je czytać, lecz ich nie modyfikuje. Typowym przykładem jest podsłuchiwanie komunikacji między legalnymi użytkownikami systemu.
- ▶ **Aktywny** – agresor modyfikuje przetwarzane lub przesyłane dane, może je nie tylko czytać, lecz również fałszować czy preparować z premedytacją, tak by uzyskać zamierzony cel ataku.
- ▶ **Intruz w środku** (ang. *man in the middle*) – wersja ataku aktywnego, w którym agresor pośredniczy w komunikacji i modyfikuje przesyłane dane.

Rodzaje ataków ze względu na źródło

- ▶ **Lokalny** – agresor ma już dostęp do systemu (konto) i próbuje zwiększyć swoje uprawnienia.
- ▶ **Zdalny** – agresor nie posiada jeszcze żadnych uprawnień w atakowanym systemie.

Ogólne formy ataku elektronicznego

- ▶ **Podszywanie** (ang. *masquerading*) – agresor udaje zaufany podmiot.
- ▶ **Podśluch** (ang. *eavesdropping*) – agresor uzyskuje dane składowane, przetwarzane lub transmitowane w systemie.
- ▶ **Odtwarzanie** (ang. *replaying*) – agresor ponownie używa przechwyconych wcześniej danych.
- ▶ **Manipulacja** (ang. *tampering*) – agresor modyfikuje dane w celu zrekonfigurowania systemu lub wprowadzenia go w stan, z którego może osiągnąć bezpośrednio lub pośrednio korzyść, np. zastosować skuteczny atak gotowym narzędziem.
- ▶ **Wykorzystywanie luk, penetrowanie** (ang. *exploiting, penetration*) – agresor posługuje się wiedzą o znanym błędzie w oprogramowaniu lub gotowym narzędziem wykorzystującym taki błąd.

Ewolucja ataków na przestrzeni lat

- ▶ Wykorzystanie trywialnych haseł i znanych luk w programach
- ▶ Analiza kodu źródłowego narzędzi systemowych w celu odkrycia luk
- ▶ Węszenie (ang. *sniff*), podsłuchiwanie haseł
- ▶ Wirusy, konie trojańskie
- ▶ Ataki na pocztę elektroniczną
- ▶ Ataki poprzez NFS (ang. *Network File System*) i NIS (ang. *Network Information Service*)
- ▶ Podszywanie się (ang. *spoofing*) pod adres IP lub pod DNS
- ▶ Ataki na routery
- ▶ Odmowa usługi, DoS (ang. *denial of service*)
- ▶ Przejmowanie stron www (ang. *page hijacking*)
- ▶ SPAM – Spiced Pork And ham
- ▶ Dialery, malware (adware, spyware)
- ▶ Łowienie w sieci (ang. *web-phishing, personal data fishing*)
- ▶ Ataki na komunikatory (ang. *spim, spimming*)

Podstawowe fazy ataku

- ▶ Skanowanie – szukanie słabości, np. sondowanie usług
- ▶ Wyznaczenie celu, np. niezabezpieczona usługa, znany exploit
- ▶ Atak na system
- ▶ Modyfikacja systemu umożliwiająca późniejszy powrót
- ▶ Usuwanie śladów
- ▶ 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

- ▶ Uniemożliwienie startowania systemu z nośników wymiennych
- ▶ Ograniczenie uprawnień do korzystania z przestrzeni lokalnych dysków twardych
- ▶ Ograniczenie stosowania nośników wymiennych (w tym również nagrywarek)
- ▶ Rejestracja prób dostępu do systemu i ich limitowanie (kontrola, kto i kiedy korzystał z systemu)
- ▶ Bezpieczne kasowanie poufnych danych
- ▶ Uniemożliwienie usunięcia lub wyłączenia zabezpieczeń, np. antywirusowych
- ▶ Konsekwentna polityka haseł użytkowników

Elementarna ochrona sieci lokalnej

- ▶ 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

- ▶ Usunięcie z systemu wszystkich usług zbędnych, najlepiej poprzez całkowite odinstalowanie, a co najmniej ich dezaktywację
- ▶ Zastąpienie niezbędnych usług ich odpowiednikami o podwyższonym bezpieczeństwie, jeśli to możliwe i takie odpowiedniki są dostępne
- ▶ Kontrola dostępu do pozostałych usług, np. za pomocą ściany (zapory) ogniowej (ang. *firewall*)

Złożoność problemu stosowania zabezpieczeń

- ▶ Broniący stoi na gorszej pozycji niż agresor.
- ▶ **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.

Zasada naturalnego styku z użytkownikiem

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

Zasada spójności poziomej i pionowej

- ▶ Cały łańcuch jest tak trwały, jak jego najsłabsze ogniwo.
- ▶ **Spójność pozioma** – wszystkie komponenty w danej warstwie systemu (np. w warstwie modelu OSI) powinny być zabezpieczone na jednakowym poziomie.
- ▶ 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 (odrzućcie pakietu).
- ▶ Wiele urządzeń i protokołów jest jednak domyślnie konfigurowanych inaczej, czy to w celu wygody użytkownika, czy z założenia wynikającego z ich funkcji, np. trasowanie (ang. *routing*).

Elementarne pojęcia

- ▶ **Identyfikacja** (ang. *identification*) – możliwość rozróżnienia użytkowników, np. użytkownicy w systemie operacyjnym są identyfikowani za pomocą UID (ang. *user identifier*).
- ▶ **Uwierzytelnianie** (ang. *authentication*) – proces weryfikacji tożsamości użytkownika. Najczęściej opiera się na tym:
 - ▶ co użytkownik wie (ang. *proof by knowledge*), np. zna hasło;
 - ▶ co użytkownik ma (ang. *proof by possession*), np. elektroniczną kartę identyfikacyjną.
- ▶ **Autoryzacja** (ang. *authorization*) – proces przydzielania użytkownikowi praw dostępu do zasobów
- ▶ **Kontrola dostępu** (ang. *access control*) – system składający się z urządzeń, oprogramowania i procedur organizacyjnych, mający na celu identyfikację podmiotu i nadzorowanie przestrzegania praw dostępu do zasobów

Elementarne pojęcia, cd.

- ▶ **Poufność** (ang. *confidentiality*) – ochrona informacji przed nieautoryzowanym jej ujawnieniem
- ▶ **Integralność (nienaruszalność)** (ang. *data integrity*) – ochrona informacji przed nieautoryzowanym jej zmodyfikowaniem (ewentualnie wykrywanie takiej modyfikacji)
- ▶ **Autentyczność** (ang. *authenticity*) – pewność co do pochodzenia (autorstwa i treści) danych
- ▶ **Niezaprzeczalność** (ang. *nonrepudiation*) – ochrona przed fałszywym zaprzeczeniem
 - ▶ przez nadawcę faktu wysłania danych
 - ▶ przez odbiorcę faktu otrzymania danych

Autoryzacja

- ▶ **Zasób (obiekt)** – jednostka, do której dostęp podlega kontroli, np. program, plik, relacja bazy danych, cała baza danych, ale też obiekty o wysokiej granulacji, np. poszczególne krotki bazy danych
- ▶ **Podmiot** – byt uzyskujący dostęp do zasobu, np. użytkownik, grupa użytkowników, terminal, komputer, aplikacja, proces.
- ▶ **Prawa dostępu** – dopuszczalne sposoby wykorzystani zasobu przez podmiot

Filozofie przydziału uprawnień

- ▶ Wszystko jest dozwolone.
- ▶ Wszystko, co nie jest (jawnie) zabronione, jest dozwolone.
- ▶ Wszystko, co nie jest (jawnie) dozwolone, jest zabronione.
- ▶ Wszystko jest zabronione.

Uznaniowa kontrola dostępu (ang. *discretionary access control*)

- ▶ Właściciel zasobu może decydować o jego atrybutach i uprawnieniach innych użytkowników względem tego zasobu.
- ▶ 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 uruchamiania programu, np. stosowane w systemach uniksowych atrybuty rwx.

Ścisła kontrola dostępu (ang. *mandatory access control*)

- ▶ Precyzyjne reguły dostępu automatycznie wymuszają uprawnienia.
- ▶ Nawet właściciel zasobu nie może dysponować prawami dostępu.
- ▶ Pozwala łatwiej zrealizować (narzucić) silną politykę bezpieczeństwa i konsekwentnie stosować ją do całości zasobów.

Kontrola oparta o role (ang. *role based access control*)

- ▶ Odmiana ścisłej kontroli dostępu.
- ▶ Powszechnie spotykana np. w systemach baz danych.

Ścisła kontrola dostępu, cd.

- ▶ **Poziomy zaufania**

ogólnie dostępne < do użytku wewnętrznego <
< tylko dyrekcja < tylko zarząd

albo

jawne < poufne < tajne < ściśle tajne

- ▶ **Kategorie informacji**

FINANSOWE OSOBOWE SZYFROWANE MILITARNE

- ▶ **Etykiety ochrony danych** składają się z poziomu zaufania i kategorii informacji, np.:

(tajne, {SZYFROWANE})

(ściśle tajne, {SZYFROWANE, MILITARNE})

Ścisła kontrola dostępu, cd.

- ▶ Na zbiorze etykiet ochrony danych określona jest relacja wrażliwości, np.:

$(\text{poufne}, \{\text{OSOBOWE}\}) < (\text{tajne}, \{\text{OSOBOWE}\})$

$(\text{tajne}, \{\text{SZYFROWANE}\}) <$

$< (\text{ściśle tajne}, \{\text{SZYFROWANE}, \text{MILITARNE}\})$

- ▶ Jest to relacja częściowego porządku. Przykładowo może nie być określona relacja pomiędzy etykietą

$(\text{ściśle tajne}, \{\text{SZYFROWANE}, \text{MILITARNE}\})$

a etykietą

$(\text{tajne}, \{\text{FINANSOWE}, \text{SZYFROWANE}\})$

Reguły ścisłej kontroli dostępu

- ▶ Użytkownik może uruchomić tylko proces, który posiada etykietę nie większą od jego aktualnej etykiety.
- ▶ Proces może czytać tylko dane o etykiecie nie większej od jego aktualnej etykiety.
- ▶ Proces może tworzyć tylko dane o etykiecie nie mniejszej od jego aktualnej etykiety.

Klasy bezpieczeństwa systemów komputerowych

- ▶ Trusted Computer System Evaluation Criteria (TCSEC Orange Book):
 - ▶ standard opracowany w USA;
 - ▶ pierwszy powszechny taki standard w skali światowej;
 - ▶ obowiązywał w latach 1985 – 2000;
 - ▶ stał się podstawą opracowania podobnych norm w Europie i na świecie;
 - ▶ bardzo często nawet współcześnie znajduje się odwołania do certyfikatów tego standardu.
- ▶ Information Technology Security Evaluation Criteria (ITSEC):
 - ▶ standard opracowany przez Unię Europejską;
 - ▶ obowiązywał w latach 1991 – 1997;
 - ▶ powstał głównie na podstawie angielskiego CESG2/DTIEC, francuskiego SCSSI i niemieckiego ZSIEC.

Klasy bezpieczeństwa systemów komputerowych, cd.

- ▶ Common Criteria Assurance Levels (EAL):
 - ▶ aktualnie obowiązujący standard;
 - ▶ będący w istocie złączeniem ITSEC, TCSEC oraz kanadyjskiego CTCPEC;
 - ▶ od 1996 powszechnie znany jako Common Criteria for Information Technology Security Evaluation (CCITSE);
 - ▶ *<http://www.commoncriteria.org>*;
 - ▶ od 1999 roku zaakceptowany jako międzynarodowa norma ISO 15408.
- ▶ Uzyskanie certyfikatu przynależności do klasy bezpieczeństwa jest operacją formalną i odpłatną.

Klasy TCSEC

- ▶ D:
 - ▶ minimalna ochrona (właściwie jej brak);
 - ▶ systemy poddane ocenie, ale nie spełniające wymagań wyższych klas.
- ▶ C1:
 - ▶ identyfikacja i uwierzytelnianie użytkowników;
 - ▶ użytkownicy i zasoby posiadają unikalne identyfikatory;
 - ▶ ochrona za pomocą haseł;
 - ▶ kontrola dostępu na poziomie: właściciel, grupa, pozostali użytkownicy;
 - ▶ ochrona systemowych obszarów pamięci.
- ▶ C2:
 - ▶ możliwość rozróżniania pojedynczych użytkowników;
 - ▶ automatyczne czyszczenie przydzielanych obszarów pamięci;
 - ▶ wymagana możliwość rejestracji dostępu do zasobu (ang. *audit*).

Klasy TCSEC

- ▶ B1:
 - ▶ etykietowane poziomy ochrony.
- ▶ B2:
 - ▶ precyzyjnie zdefiniowany i udokumentowany model bezpieczeństwa;
 - ▶ ochrona strukturalna – jądro ochrony;
 - ▶ weryfikacja autentyczności danych i procesów;
 - ▶ informowanie użytkownika o dokonywanej przez jego proces zmianie poziomu ochrony;
 - ▶ wykrywanie zamaskowanych kanałów komunikacyjnych;
 - ▶ ścisła rejestracja operacji.
- ▶ B3:
 - ▶ kontrola wszystkich przeprowadzanych przez użytkownika operacji;
 - ▶ domeny ochronne;
 - ▶ aktywna kontrola pracy systemu (ang. *security triggers*);
 - ▶ bezpieczne przeładowanie systemu.

Klasy TCSEC

- ▶ A1:
 - ▶ formalny opis systemu umożliwiający przeprowadzenie analizy poprawności implementacji;
 - ▶ formalne procedury analizy i weryfikacji projektu i implementacji systemu.

Poziomy pewności EAL

- ▶ EAL0:
 - ▶ brak pewności.
- ▶ EAL1:
 - ▶ produkt testowany funkcjonalnie;
 - ▶ analiza bezpieczeństwa wykorzystująca specyfikację funkcji i interfejsu w celu zrozumienia zachowania systemu;
 - ▶ niezależne testowanie funkcji bezpieczeństwa.
- ▶ EAL2:
 - ▶ produkt testowany strukturalnie;
 - ▶ analiza bezpieczeństwa wykorzystująca wysokopoziomowy opis projektu podsystemów;
 - ▶ dowody testowania przez producenta i wyszukiwania oczywistych słabych punktów.

Poziomy pewności EAL

▶ EAL3:

- ▶ produkt testowany metodycznie i sprawdzany;
- ▶ analiza bezpieczeństwa wykorzystująca metodę „szarej skrzynki”, tj. selektywne niezależne potwierdzanie wyników testów producenta;
- ▶ wymagania związane ze środowiskiem produkcji i zarządzaniem konfiguracją.

▶ EAL4:

- ▶ produkt metodycznie projektowany, testowany i sprawdzany;
- ▶ analiza bezpieczeństwa wykorzystująca niskopoziomowy projekt modułów systemu;
- ▶ niezależne wyszukiwanie luk w systemie;
- ▶ model życia, automatyczne zarządzanie konfiguracją.

Poziomy pewności EAL

► EAL5:

- produkt projektowany półformalnie i testowany;
- pełna analiza implementacji;
- pewność na podstawie modelu formalnego i półformalnej prezentacji specyfikacji funkcjonalnej i wysokopoziomowego opisu;
- poszukiwanie luk musi wykazać względną odporność na atak penetracyjny;
- analiza ukrytych kanałów;
- modularność projektu.

► EAL6:

- produkt z projektem półformalnie weryfikowanym i testowany;
- projektowanie modularne, warstwowe;
- poszukiwanie luk musi wykazać wysoką odporność na atak penetracyjny;
- systematyczna analiza ukrytych kanałów;
- zaostrome rygory środowiska produkcji i zarządzania konfiguracją.

Poziomy pewności EAL

► EAL7:

- produkt z projektem formalnie weryfikowanym i testowany;
- formalne podejście do specyfikowania, projektowania i dokumentowania systemu;
- kompletne niezależne testowanie i weryfikacja testów producenta;
- minimalizacja złożoności projektu.

Kompatybilność standardów bezpieczeństwa

| TCSEC | ITCES | CCITSE |
|-------|----------|--------------|
| 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 |

Przynależność popularnych systemów do klas bezpieczeństwa

| Klasa | System |
|---------|------------------------------|
| D EAL0 | Windows 9x |
| C1 EAL2 | Unix Linux NetWare |
| C2 EAL3 | Solaris AIX Windows NT |

Przynależność popularnych systemów do klas bezpieczeństwa, cd.

| Klasa | System |
|---------|--|
| B1 EAL4 | Trusted Solaris Trusted IRIX HP-UX Ultrix SuSE Linux (EAL4+) Windows 2000 Prof. SP3 |
| B2 EAL5 | |
| B3 EAL6 | |
| A1 EAL7 | SCC Secure Network Server Gemini Trusted Network Processor |