BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

dr inż. Michał Szychowiak

http://www.cs.put.poznan.pl/mszychowiak

Bezpieczeństwo

Co to jest bezpieczeństwo?

Def.: **System informatyczny** jest **bezpieczny**, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją.

Simson Garfinkel, Gene Spafford

Practical Unix and Internet Security

Możemy mówić, że system jest bezpieczny, jeśli np. zawsze można od niego oczekiwać, że wprowadzone dziś na stałe dane będą w nim jeszcze za tydzień, nie ulegną zniekształceniu i nie zostaną odczytane przez nikogo nieuprawnionego – ufamy, że system będzie przechowywał i chronił dane.

Szerszy kontekst

System wiarygodny =

- dyspozycyjny (*available*) = dostępny na bieżąco
- niezawodny (*reliable*) = odporny na awarie
- bezpieczny (*safe*) = bezpieczny dla otoczenia, przyjazny dla środowiska
- bezpieczny (*secure*) = zapewniający ochronę danych

Realne zagrożenia?

„... Rosyjscy hackerzy z powodzeniem przelewali pieniądze z kont banku CityCorp, kradnąc 400 tys. USD i nielegalnie przelewając ok. 11,6 mln USD..."

(*Wall Street Journal, August 21, 1995*)

Raport Instytutu Bezpieczeństwa Komputerowego (San Francisco) z 1998 r. szacuje, że 95% sieciowych wandali to nowicjusze posługujący się oferowanymi przez innych gotowymi programami, nie zdając sobie nawet sprawy z tego jak one działają. Straty przez nich spowodowane wyniosły w 1998 r. ok. 123 mln USD w samych Stanach.

Hacker?

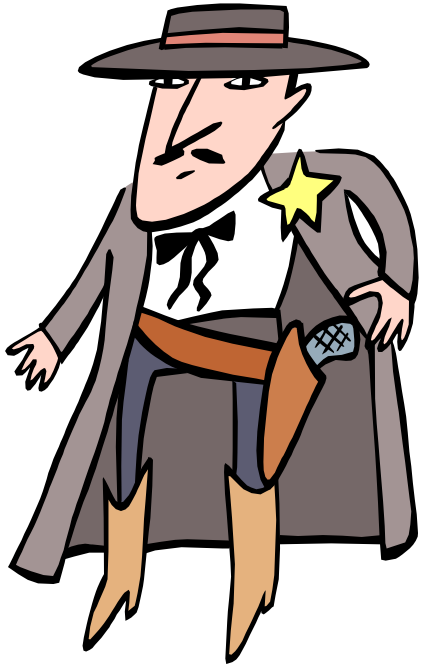
Def: **HACKER** 1. osoba, której sprawia przyjemność poznawanie szczegółowej wiedzy na temat systemów komputerowych i rozszerzanie tej umiejętności, w przeciwieństwie do większości użytkowników, którzy wolą uczyć się niezbędnego minimum; 2. osoba, która entuzjastycznie zajmuje się programowaniem i nie lubi teorii dotyczącej tej dziedziny.

Guy L. Steele et al.
The Hacker's Dictionnary

- powszechnie uznany przykład: Richard Stallman (Free Sotware Foundation, GNU)
- naruszenia bezpieczeństwa: cracker, intruz, włamywacz, napastnik, wandal, przestępca

Przestępstwa komputerowe

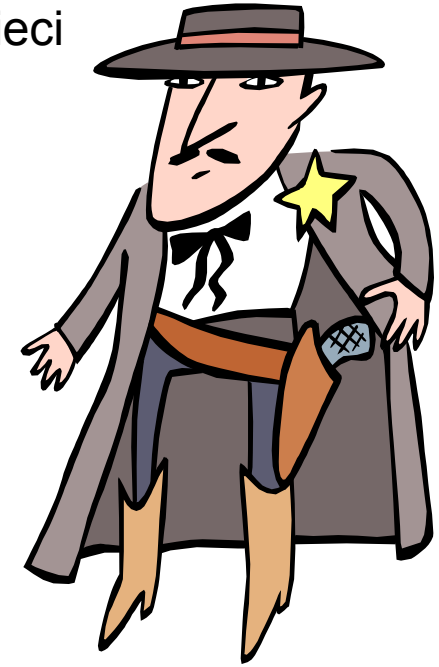
- włamanie do systemu komputerowego
- nieuprawnione pozyskanie informacji
- destrukcja danych i programów
- sabotaż (sparaliżowanie pracy) systemu
- piractwo komputerowe, kradzież oprogramowania
- oszustwo komputerowe i fałszerstwo komputerowe
- szpiegostwo komputerowe
- . . .



📖 Dorothy E. Robling Denning, "Wojna informacyjna i bezpieczeństwo informacji", WNT, 2002

Przestępstwa komputerowe

Praktycznie wszystkie przypadki naruszające bezpieczeństwo w sieci Internet wyczerpują znamiona przestępstw określonych w obowiązującym prawie RP.



W szczególności mają tu zastosowanie:

- artykuły 267-269 KK
- artykuł 287 Kodeksu Karnego

(http://www.gazeta-it.pl/prawo/przestepstwa_komputerowe.html)

Zazwyczaj przestępstwa te nie są ścigane z oskarżenia publicznego, lecz na wniosek pokrzywdzonego.

Bezpieczeństwo systemu informatycznego

Czynniki decydujące o znaczeniu problemu

- rola systemów informatycznych (szcz. sieci) dla funkcjonowania współczesnej cywilizacji
- trudności związane ze skonstruowaniem i eksploatacją systemu spełniającego wysokie wymagania w zakresie bezpieczeństwa (niedoskonałości technologii, konfiguracji i polityki bezpieczeństwa)
- elementarny konflikt interesów – pomiędzy użytecznością systemu a ryzykiem związanym z jego wykorzystaniem

Bezpieczeństwo systemu informatycznego

Truizmy

1. Nie istnieje coś takiego, jak absolutne bezpieczeństwo.
2. Złożoność jest najgorszym wrogiem bezpieczeństwa.
3. Bezpieczeństwo musi być rozpatrywane w relacji z ekonomią.
4. Zasoby mają większą wartość niż myślimy.
5. Napastnik nie pokonuje zabezpieczeń, on je obchodzi.
6. System dopóty nie jest bezpieczny, dopóki nie ma pewności że jest.
7. Wzrost poziomu bezpieczeństwa odbywa się kosztem wygody.
8. Nie należy pokładać zaufania w jednej linii obrony.

Komponenty systemu informatycznego

Elementarne składniki systemu informatycznego:

1. Stanowisko komputerowe i infrastruktura sieciowa
2. System operacyjny i usługi narzędziowe
3. Aplikacje użytkowe

Bezpieczeństwo w sieci

Sieć publiczna / globalna

Chcemy korzystać z globalnych usług:

- wysyłać pocztę do wybranej osoby
- współdzielić dane (pliki) poprzez sieć rozległą
- uzyskiwać informacje zgromadzone w sieci rozległej

Sami oferujemy usługi:

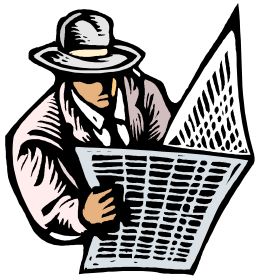
- udostępniamy serwis WWW poprzez sieć publiczną

Sieć lokalna

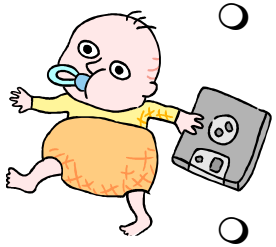
- zapewnienie zgodności przetwarzania z polityką bezpieczeństwa firmy
- bezpieczeństwo współdzielenia przetwarzanych danych

Bezpieczeństwo w sieci rozległej

Sieć publiczna – wielu różnych użytkowników:



- szpiedzy z obcych państw węszący za tajnymi informacjami
- dziennikarze łapczywie polujący na każdą sensację
- pracownicy z konkurencyjnych firm przyczajeni by podejrzeć nasze ruchy
- zwolnieni pracownicy naszej firmy czekający, by odpłacić za niełaskę



- rzesze nieodpowiedzialnych małolatów spędzających noce na próbach przełamania dla zabawy naszych zabezpieczeń (w tym tzw. *script kiddies*)
- pospolici złodzieje gotowi ukraść każdą informację, którą tylko da się sprzedać

Bezpieczeństwo w sieci rozległej

Zaciekła konkurencja:

- w 1997 r. CIWARS (Centre for Infrastructural Warfare Studies) odnotował 2 incydenty (w Brazylii i w Australii), w których zaatakowały się wzajemnie (SYN flood) konkurujące ze sobą firmy ISP

Anarchia itp.:

- w 1997 r. grupa Damage Inc. zastąpiła witrynę Urzędu Rady Ministrów stroną proklamującą utworzenie Hackrepubliki Polskiej i Centrum Dezinformacyjnego Rządu z odsyłaczami do `playboy.com`.

Terroryzm itp.:

- w 1998 r. w akcie protestu przeciwko próbom nuklearnym grupa Milw0rm zaatakowała systemy indyjskiego BARC (Bhabba Atomic Research Center)

Ocena ryzyka

1. Określenie zasobów = „Co chronić?”
2. Identyfikacja zagrożeń = „Przed czym chronić?”
3. Oszacowanie ryzyka = „Ile czasu, wysiłku i pieniędzy można poświęcić na należna ochronę” (analiza kosztów i zysku)

Strategia bezpieczeństwa

Strategia bezpieczeństwa

Formalny dokument

- polityka bezpieczeństwa

Etapy realizacji

1. zaprojektowanie
2. zaimplementowanie
3. zarządzanie (w tym okresowe audyty bezpieczeństwa)

Polityka bezpieczeństwa

Zakres

- definicja celu i misji polityki bezpieczeństwa
- standardy i wytyczne których przestrzegania wymagamy
- kluczowe zadania do wykonania
- zakresy odpowiedzialności

Specyfikacja środków

- ochrona fizyczna
- polityka proceduralno-kadrowa (odpowiedzialność personalna)
- mechanizmy techniczne

Normy i zalecenia zarządzania bezpieczeństwem

kanonem jest ISO/IEC Technical Report 13335 (PN-I-13335)

TR 13335-1	terminologia i modele
TR 13335-2	metodyka planowania i prowadzenia analizy ryzyka, specyfikacja wymagań stanowisk pracy związanych z bezpieczeństwem systemów informatycznych
TR 13335-3	techniki zarządzania bezpieczeństwem – zarządzanie ochroną informacji – zarządzanie konfiguracją systemów IT – zarządzanie zmianami
TR 13335-4	metodyka doboru zabezpieczeń
WD 13335-5	zabezpieczanie połączeń z sieciami zewnętrznymi

Normy i zalecenia (c.d.)

ale norm ISO dotyczących bezpieczeństwa jest wiele:

- ISO 2382-8:1986 Information processing systems – Vocabulary – Part 08: Control, integrity and security
- ISO 6551:1982 Petroleum liquids and gases – Fidelity and security of dynamic measurement – Cabled transmission of electric and/or electronic pulsed data
- ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
- ISO/IEC 7816-4:1995 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange
- ISO/IEC 9796:1991 Information technology – Security techniques – Digital signature scheme giving message recovery
- ISO/IEC 9797:1994 Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm
- ISO/IEC 9798-1:1991 Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model
- ISO/IEC 9798-2:1994 Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms
- ISO/IEC 9798-3:1993 Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm
- ISO/IEC 9798-4:1995 Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function
- ISO/IEC 10118-1:1994 Information technology – Security techniques – Hash-functions – Part 1: General
- ISO/IEC 10118-2:1994 Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm
- ISO/IEC 10164-7:1992 Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function
- ISO/IEC 10164-8:1993 Information technology – Open Systems Interconnection – Systems Management: Security audit trail function
- ISO/IEC DIS 10181-1 Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview
- ISO/IEC DIS 10181-2 Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework
- ISO/IEC DIS 10181-3 Information technology – Open Systems Interconnection – Security frameworks in open systems – Part 3: Access control
- ISO/IEC DIS 10181-4 Information technology – Open Systems Interconnection – Security frameworks in Open Systems – Part 4: Non-repudiation
- ISO/IEC DIS 10181-5 Information technology – Security frameworks in open systems – Part 5: Confidentiality
- ISO/IEC DIS 10181-6 Information technology – Security frameworks in open systems – Part 6: Integrity
- ISO/IEC DIS 10181-7 Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Security Audit Framework
- ISO/IEC 10736:1995 Information technology – Telecommunications and information exchange between systems – Transport layer security protocol

- ISO/IEC 10745:1995 Information technology – Open Systems Interconnection – Upper layers security model
- ISO 11166-1:1994 Banking – Key management by means of asymmetric algorithms – Part 1: Principles, procedures and formats
- ISO 11166-2:1994 Banking – Key management by means of asymmetric algorithms – Part 2: Approved algorithms using the RSA cryptosystem
- ISO 11442-1:1993 Technical product documentation – Handling of computer-based technical information – Part 1: Security requirements
- ISO/IEC 11577:1995 Information technology – Open Systems Interconnection – Network layer security protocol
- ISO/IEC DIS 11586-1 Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation
- ISO/IEC DIS 11586-2 Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) service specification
- ISO/IEC DIS 11586-3 Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) protocol specification
- ISO/IEC DIS 11586-4 Information technology – Open Systems Interconnection – Generic upper layers security: Protecting transfer syntax specification
- ISO/IEC DIS 11586-5 Information technology – Open Systems Interconnection – Generic Upper Layers Security: Security Exchange Service Element Protocol Implementation Conformance Statement (PICS)
- ISO/IEC DIS 11586-6 Information technology – Open Systems Interconnection – Generic Upper Layers Security: Protecting Transfer Syntax Implementation Conformance Statement (PICS)
- ISO/IEC DIS 11770-1 Information technology – Security techniques – Key management – Part 1: Framework
- ISO/IEC DIS 11770-2 Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques
- ISO/IEC DISP 12059-7 Information technology – International Standardized Profiles – OSI Management – Common information for management functions – Part 7: Security alarm reporting
- ISO/IEC DISP 12059-8 Information technology – International Standardized Profiles – OSI Management – Common information for management functions – Part 8: Security audit trail
- ISO/IEC DISP 12060-6 Information technology – International Standardized Profiles - OSI Management – Management functions – Part 6: Security management capabilities
- ISO/IEC DTR 13335-1 Information technology – Guidelines for the management of IT security – Part 1: Concepts and models for IT security
- ISO/IEC DTR 13335-2 Information technology – Guidelines for the management of IT security – Part 2: Planning and managing IT security (Future Technical Report)
- ISO/IEC DTR 13335-3 Information technology – Guidelines for the management of IT security – Part 3: Techniques for the management of IT security
- ISO/IEC TR 13594:1995 Information technology – Lower layers security
- ISO/IEC DIS 14980 Information technology – Code of practice for information security management

. . .

Określenie zasobów = „Co chronić?”

- sprzęt komputerowy
- infrastruktura sieciowa
- wydruki
- strategiczne dane
- kopie zapasowe
- wersje instalacyjne oprogramowania
- dane osobowe
- dane audytu
- zdrowie pracowników
- prywatność pracowników
- zdolności produkcyjne
- wizerunek publiczny i reputacja

Identyfikacja zagrożeń = „Przed czym chronić?”

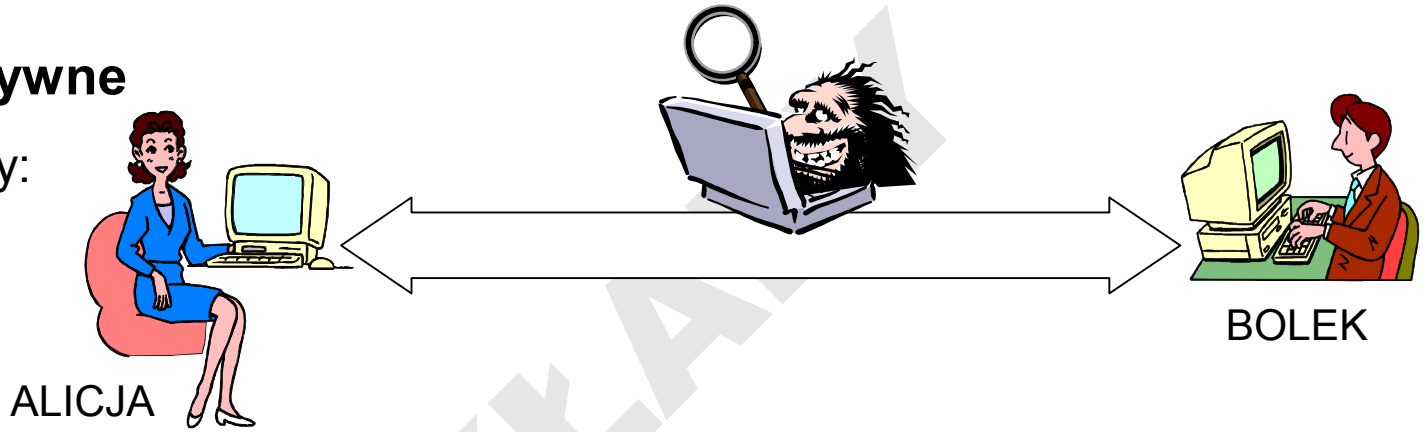
- włamywacze komputerowi
- infekcje wirusami
- destruktywność pracowników / personelu zewnętrznego
- błędy w programach
- kradzież dysków / laptopów (również w podróży służbowej)
- utrata możliwości korzystania z łączy telekomunikacyjnych
- bankructwo firmy serwisowej / producenta sprzętu
- choroba administratora / kierownika (jednoczesna choroba wielu osób)
- powódź

Atak na system informatyczny

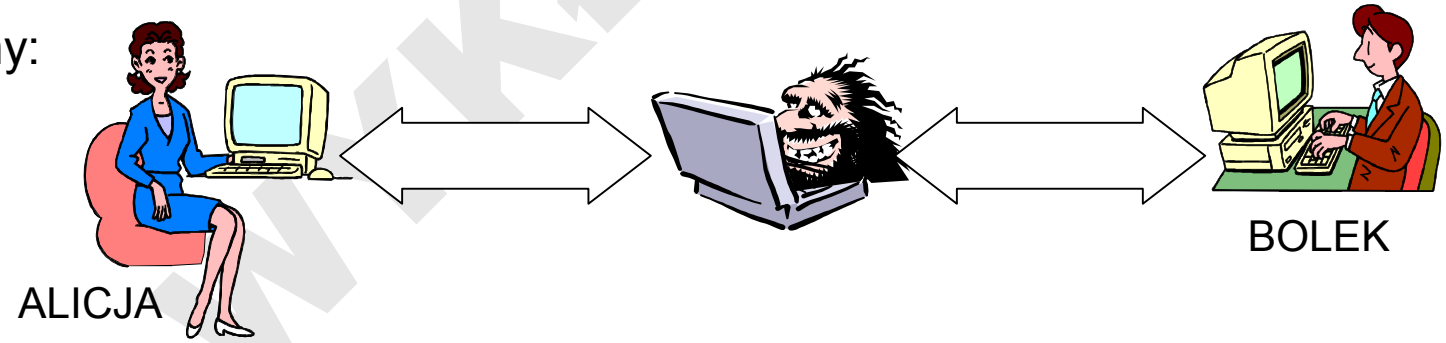
Klasy ataków

pasywne / aktywne

- pasywny:



- aktywny:



lokalne/zdalne

- lokalny: atakujący już ma dostęp do systemu (konto) i próbuje zwiększyć swe uprawnienia

Atak na system informatyczny

Ogólne metody ataku elektronicznego

- podszywanie (ang. *masquerading*)
- podsłuch (ang. *eavesdropping*)
- odtwarzanie (ang. *replaying*)
- manipulacja (ang. *tampering*)
- wykorzystanie luk w systemie (ang. *exploiting*)

Atak na system informatyczny

Podstawowe fazy ataku

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

Elementarna ochrona stacji roboczej

- 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

Podstawowe środki ostrożności

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

Podstawowe środki ostrożności

Elementarna ochrona usług sieciowych

Procedura ochrony dostępu do usług sieciowych:

1. usunięcie wszystkich usług zbędnych
2. zastąpienie usług niezbędnych odpowiednikami o podwyższonym bezpieczeństwie (jeśli to możliwe)
3. filtracja dostępu do pozostałych usług (zapory sieciowe – *firewall*)

Zabezpieczenia

Złożoność problemu stosowania zabezpieczeń

- **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.

Zabezpieczenia

Stosowanie mechanizmów bezpieczeństwa

1. Zasada naturalnego styku z użytkownikiem
2. Zasada spójności poziomej i pionowej
3. Zasada minimalnego przywileju
4. Zasada domyślnej odmowy dostępu

Zabezpieczenia

Elementarne pojęcia:

1. **Identyfikacja (ang. *identification*)**
   - użytkownicy są identyfikowani w systemie za pomocą UID (*user identifier*)
2. **Uwierzytelnianie (ang. *authentication*)**
   - jest to proces weryfikacji tożsamości użytkownika; najczęściej opiera się na tym:
     - co użytkownik wie (*proof by knowledge*), np. hasło
     - co użytkownik ma (*proof by possession*), np. elektroniczną kartę identyfikacyjną

Доверяй но проверяй

Zabezpieczenia

Elementarne pojęcia:

3. **Autoryzacja (ang. *authorization*)**
   - jest to proces przydzielania praw (dostępu do zasobów) użytkownikowi

4. **Kontrola dostępu (ang. *access control*)**
   - jest to procedura nadzorowania przestrzegania praw (dostępu do zasobów)

Zabezpieczenia

Elementarne pojęcia:

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. **Niezaprzeczalność (ang. *nonrepudiation*)**
   - ochrona przed fałszywym zaprzeczeniem
     - przez nadawcę – faktu wysłania danych
     - przez odbiorcę – faktu otrzymania danych

Autoryzacja

Model

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

Autoryzacja

Filozofie przydziału uprawnień

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.**

Kontrola dostępu do danych

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

- 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

Kontrola dostępu do danych

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

- 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

Poziomy zaufania:

etykiety poziomu zaufania (*sensitivity labels*):

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

public < company confidential < executives only < CEO secret

w innego typu instytucji:

jawne < poufne < tajne < ściśle tajne

unclassified < confidential < secret < top secret

Kategorie przynależności danych:

- nie są hierarchiczne i reprezentują rodzaj wykorzystania danych

FINANSOWE, OSOBOWE, KRYPTO, MILITARNE

Ścisła kontrola dostępu

Etykiety ochrony danych

- składają się z 2 parametrów: poziomu zaufania i kategorii informacji

(tajne, {KRYPTO})

(ściśle tajne, {KRYPTO,MILITARNE})

Relacja wrażliwości:

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

ale:

(ściśle tajne, {KRYPTO,MILITARNE}) **?** (tajne, {FINANSOWE,KRYPTO})

Podmiot nie może czytać danych o wyższej etykiecie (*read-up*) niż swoja aktualna.

Podmiot nie może zapisywać danych o niższej etykiecie (*write-down*) niż swoja aktualna.

Reguły MAC

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.

Klasy bezpieczeństwa systemów komputerowych

Standardy certyfikacji:

- Trusted Computer System Evaluation Criteria (TCSEC "Orange Book") – USA
  http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html ; 1983-2000;

- Information Technology Security Evaluation Criteria (ITSEC) – EU
  http://www.cesg.gov.uk ; 1991-1997 (powstał głównie z angielskiego CESG2/DTIEC, francuskiego SCSSI i niemieckiego ZSIEC)

- Common Criteria Assurance Levels (EAL) = ITSEC + TCSEC + CTCPEC (Canada) od 1996
  Common Criteria for Information Technology Security Evaluation (CC) – ISO15408
  = EAL v.2 – od 1999; http://www.commoncriteria.org

Klasy bezpieczeństwa systemów komputerowych

(wg TCSEC “Orange Book”)

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

Klasy bezpieczeństwa systemów komputerowych

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

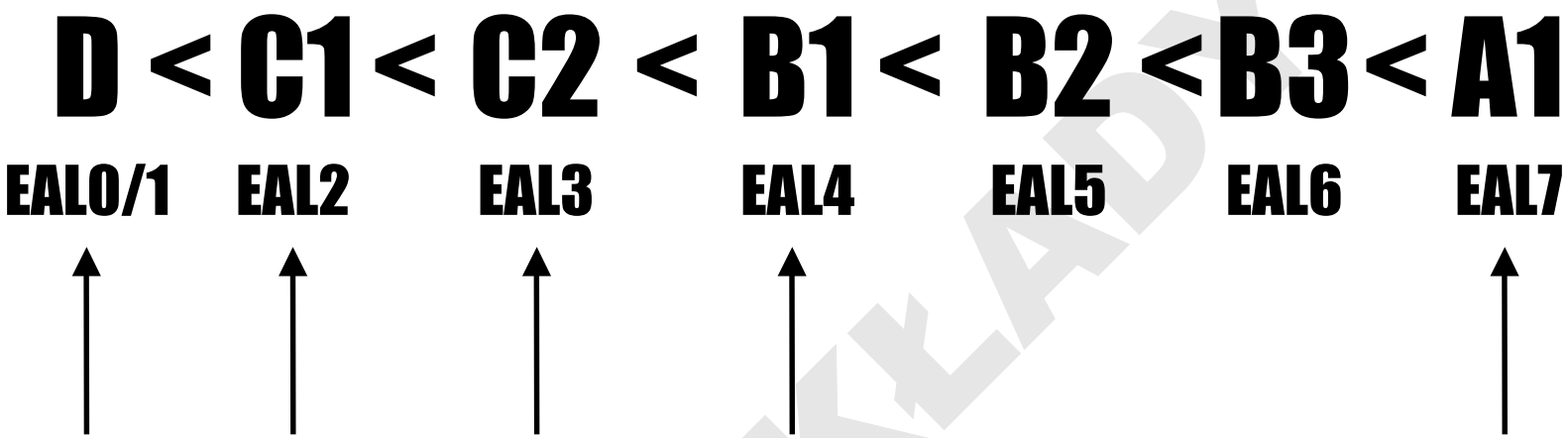
A1 - formalne procedury analizy i weryfikacji projektu i implementacji systemu

Klasy bezpieczeństwa systemów komputerowych

Porównanie klas:

TCSEC	ITCES	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

Klasy bezpieczeństwa systemów komputerowych



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