Politechnika Wrocławska

Internetowe Bazy Danych

dr inż. Roman Ptak
Katedra Informatyki Technicznej
roman.ptak@pwr.edu.pl

Plan wykładu 2.

- E-commerce – bezpieczeństwo i zagrożenia
- Typy ataków, ataki bazodanowe
- Umiejscowienie bazy danych w architekturze sieci firmowej
- Sieci wirtualne, szyfrowanie
- Składowanie, archiwizacja i ochrona danych

e-commerce

HANDEL ELEKTRONICZNY

Handel | biznes elektroniczny

- *e-commerce* (e-handel)
- *e-business* (e-biznes)
  - *B2B (business-to-business)*
  - *B2C (business-to-consumer/client)*
  - *Intra-business (intranet)*
- e-usługi
  - A2A, A2B, A2C (G2G, G2B, G2C)
  - A2E (G2E)
  - F2B, F2C

e-banking

e-economy

e-society

e-enterprise

e-learning

e-government

E-commerce i bezpieczeństwo

- Komercyjne witryny internetowe
- Bezpieczeństwo komercyjnych stron WWW
- Bezpieczeństwo aplikacji internetowych
- Uwierzytelnianie przy użyciu PHP i MySQL
- Zabezpieczenie transakcji przy użyciu PHP i MySQL

Komercyjne witryny internetowe - zagrożenia biznesowe

- Dostarczanie mało interesujących informacji
- Niska jakość prezentacji
- Brak reakcji na zgłoszenia potencjalnych klientów
- Zaniedbywanie aktualizacji witryny
- Silna konkurencja
- Przyciąganie niewystarczającej liczby klientów

Ryzyko i zagrożenia

- Zmiana polityki rządowej
- Awarie sprzętu komputerowego
- Awarie sieci elektrycznych, komunikacyjnych, komputerowych
- Błędy w oprogramowaniu
- Ograniczenie pojemności systemów
- Crackerzy

1. Kategorie zagrożeń

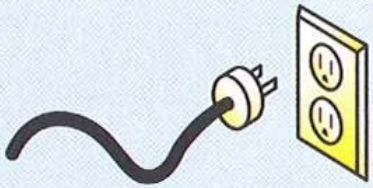
ZAGROŻENIA BEZPIECZEŃSTWA

Związane z postępowaniem człowieka

- **Złe intencje**
  - Napastnicy zewnętrzni, np. krakerzy i hakerzy
  - Napastnicy wewnętrzni, np. niezadowoleni pracownicy
- **Bez złych intencji**
  - Nieprzeszkoleni pracownicy

Niezwiązane z postępowaniem człowieka

(sprzęt/oprogramowanie/sieć)
Błędy i furtki w oprogramowaniu
Awarie produktów (MTBF)
Awarie zasilania
(mogą tworzyć luki w bezpieczeństwie)



Katastrofy naturalne

Powodzie, pożary, trzęsienia ziemi, huragany

2. Profile napastników

Napastnicy	Umiejętności	Znajomość celu	Środki	Motywy
Wywiad gospodarczy	Średnie-wysokie	Średnia-wysoka	Średnie-duże	Finansowe, konkurencja
Szpiedzy (agencje wywiadu)	Wysokie	Średnia-wysoka	Duże	Interesy narodowe
Napastnicy wewnętrzni (personel, kontrahenci)	Średnie	Wysoka	Średnie	Finansowe, zemsta
	UWAGA: Zwykle dysponują pewnymi prawami dostępu			
Terroryści	Wysokie	Średnia	Średnie-duże	Fanatyzm religijny i polityczny
Karierowicze łamiący prawo	Średnie-wysokie	Średnia	Średnie	Finansowe, zdobycie władzy
Hakerzy				
• Nowicjusze (Script Kiddie, Wannabe)	Niskie	Niska	Małe	Ciekawość, chęć wyróżnienia się
	UWAGA: Mają mnóstwo wolnego czasu i są niebezpieczni, bo nie zawsze zdają sobie sprawę, co robią			
• Black Hat (źli)	Średnie-wysokie	Wysoka	Średnie	Chęć wyróżnienia się, rzekome zwiększanie bezpieczeństwa
• Grey Hat	Średnie-wysokie	Średnia	Średnie	Działający jako Black i White Hat, do wynajęcia lub nie
• White Hat (dobrzy)	Średnie-wysokie	Brak celu	Średnie	Zwiększanie bezpieczeństwa (ale tworzą narzędzia, które są wykorzystywane przez nowicjuszy)
• Hacktivist	Średnie-wysokie	Średnia-wysoka	Małe-średnie	Polityczni aktywiści, którzy chcą coś zademonstrować

3. Techniki zdobywania informacji

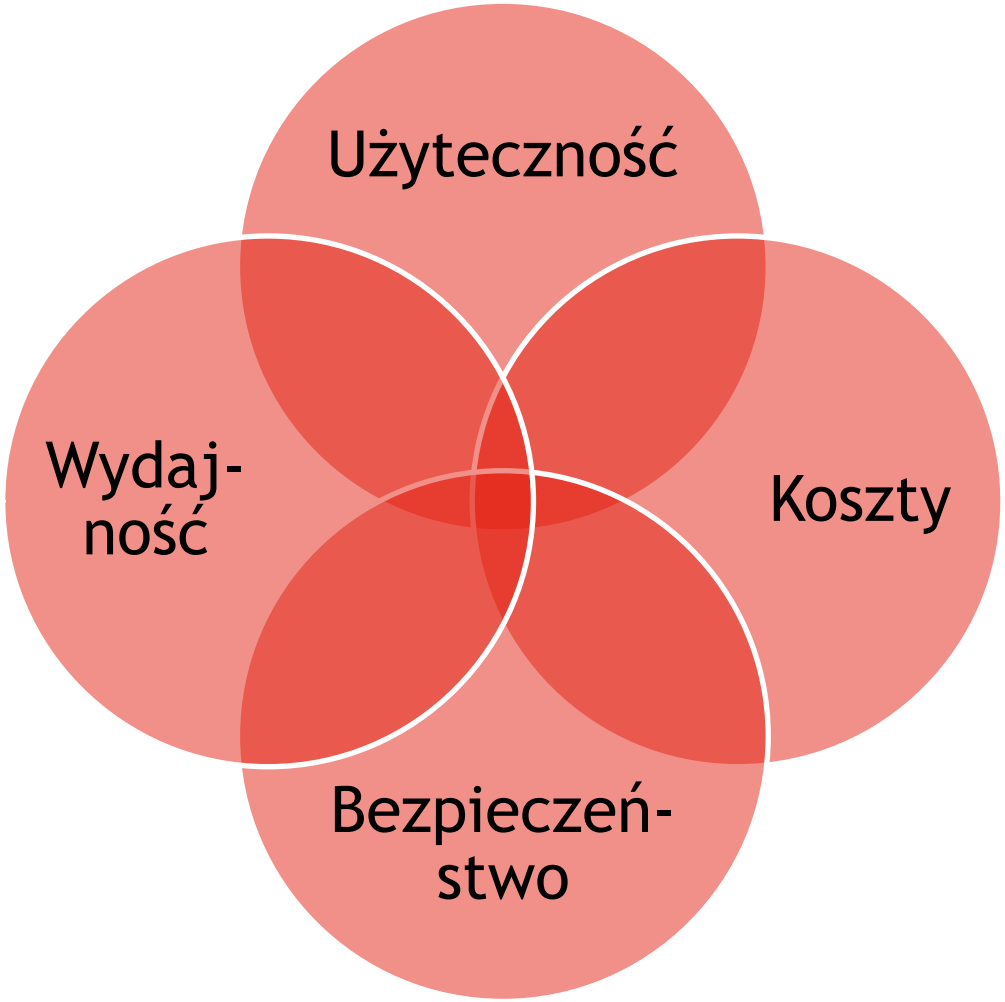
- **Metody socjotechniczne (Social Engineering) do zdobycia numerów kont, haseł itp.**
- **Dostęp do materiałów publicznych:**
  1. Strony internetowe władz państwa, wyszukiwarki, InterNIC i inne serwisy online
  2. Fora dyskusyjne, ekrany logowania, książki telefoniczne, artykuły i wycinki prasowe, wyniki finansowe
  3. Usługi detektywistyczne
- **Skanowanie adresów IP:** ping, TJping, traceroute
- **Skanowanie portów:** Ultrascan, NMAP, Slow Scan Attack (w celu uniknięcia wykrycia)
- **Programy narzędziowe i instrukcje Unix/NT:** Finger, Netstat, Rpcinfo, nslookup, whois, przeglądarka do śledzenia źródła, Telnet do połączenia z dostępnym portem i zdobycia jakichś danych (np. numeru wersji oprogramowania), expn root @foo.com, rlogin, rsh, rexecd, próby znalezienia plików: /etc/shadow, /etc/passwd, /etc/aliases i przesłania ich do siebie
- **Man-in-the-middle:**

  Przechwytywanie pakietów za pomocą analizatorów protokołów (np. ethfind, sniff, netmon, tcpdump), wykorzystując:
  1. Fizyczny dostęp do sieci: podsłuch przez szafkę telefoniczną, wolne gniazdko sieciowe lub modem kablowy
  2. Kontrolę przejętą nad hostem w sieci
  3. Przekierowywanie danych przy użyciu podrobionych pakietów RIP, DNS lub ICMP Redirect
- **War Dialing:** zautomatyzowana technika skanowania linii telefonicznych w poszukiwaniu niezabezpieczonych modemów. Inne przykłady to ToneLOC, AIO, Modem Hunter i Demon Dialer
- **Wrogie aplikacje:** GetAdmin, NetBus, BackOrifice do zdobycia informacji, haseł itp.
- **Przeszukiwanie śmieci:** firmowe odpadki są cennym źródłem informacji
- **Informacje podejrzane lub podsłuchane:** podczas rozmowy w samolocie, restauracji i innych miejscach publicznych
- **Użycie internetowych robotów wyszukiwawczych:** do znalezienia źle zabezpieczonych stron internetowych (luki w cgi bin)

Zagrożenia bezpieczeństwa

- Ujawnienie poufnych danych
- Modyfikacja lub zniszczenie danych
- Uniemożliwienie świadczenia usług
- Nieuznawanie transakcji

Konieczność kompromisu



Metody socjotechniczne (*Social Engineering*)

Atak z podszywaniem się
Wykorzystywanie fałszywego identyfikatora, ubioru służb porządkowych itp. do zdobycia informacji lub dostępu; wykorzystanie informacji o pewnych osobach w celu podania się za ich przyjaciół lub znajomych; podawanie się za osobę uprawnioną i żądanie informacji

Atak „na ignoranta"
Nakłonienie kogoś, by wyjaśnił, zaprzeczył lub uzupełnił „pseudowiedzę" napastnika;

Atak z podpuszczaniem
Wypowiadanie wyjątkowych kłamstw i niedorzeczności, by zdobyć informacje w odpowiedzi

Atak nieustający
Ciągłe nękanie ofiary poczuciem winy, onieśmielanie i inne negatywne oddziaływania, by zdobyć informacje

Atak przez obserwację
Rejestrowanie aktywności i działań ludzi w czasie, dostaw towarów itp.

Atak z przynętą
Wykorzystanie atrakcyjności seksualnej w celu zdobycia informacji lub dostępu

Atak brutalny
Atak z użyciem siły, zastraszenie, grożenie bronią, szantaż

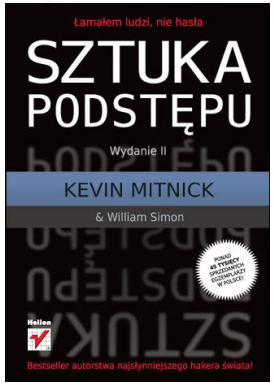
Atak przez łapówkę
Użycie zwykłego przekupstwa

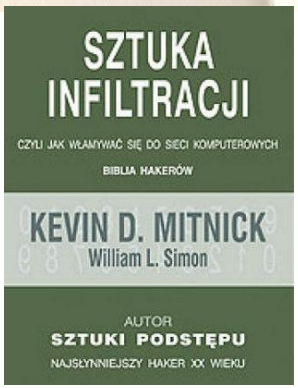
Atak z fałszywym alarmem
Wszczynanie serii fałszywych alarmów, by ofiara wyłączyła swój system alarmowy

Atak z Help Desk
Podszycie się pod obecnego lub nowego użytkownika potrzebującego pomocy, by zdobyć dostęp do sieci lub serwera

Atak z „wmieszaniem się w tłum"
Spotkania i imprezy firmowe są znakomitym miejscem zdobycia informacji i dostępu. Wmieszanie się w grupę pracowników i udawanie jednego z nich

Atak z fałszywą ankietą
Obietnica wygrania wycieczki do egzotycznych krajów po udzieleniu odpowiedzi na kilka pytań dotyczących firmowej sieci





Działania hakerskie

1. Wykorzystanie złego administrowania

- Użycie odgadniętego lub wykradzionego hasła do zdobycia dostępu do konta, wykorzystując dziurę w zaporze ogniowej lub modem
- Wykorzystanie pozostawionych niebezpiecznych usług: TFTP itp.
- Wykorzystanie do zdobycia dostępu pozostałości po debugowaniu: phf.cgi, files.pl

2. Wykorzystanie błędów programowych

- Doprowadzenie do przepełnienia bufora, by uruchomić złośliwy kod
- Wstawienie specjalnych znaków do aplikacji lub strony internetowej ofiary
- Użycie opcji debugowania lub furtek programowych w oprogramowaniu bez poprawek
- Użycie "wyścigu" (race condition) do zwiększenia zakresu dostępu (zdobycia uprawnień root lub administratora)

3. Skłonienie ofiary do uruchomienia konia trojańskiego (pod postacią gry lub atrakcyjnego obrazka), instalującego tylne drzwi

NetBus, BackOrifice, dające napastnikowi dostęp

4. Wykorzystanie funkcji dostępnych z zewnątrz lub na hostach klienckich

- Złośliwy kod osadzony w aktywnym/mobilnym kodzie
- JavaScript (np. wykorzystanie funkcji CALL w Excelu)
- ActiveX - Java
- NTFS Streams - PostScript
- Przygotowanie płyty CD z funkcją AutoPlay, która instaluje wirusa lub program tylnych drzwi

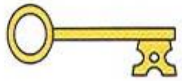
5. Różne narzędzia hakerskie

- Analizator pliku Core dump
- Hex editor
- Modem Jammer: zapobiega wykrywaniu połączeń modemowych
- Netcat: doskonałe narzędzie do połączeń TCP/UDP, autorzy: „The Hobbit" i Weld Pond

6. E-shoplifting

- Zmodyfikowany html przesłany z powrotem do strony dostawcy

Cracking



Lekki
(Mały wysiłek umysłowy)

- Dostęp nie zabezpieczony hasłami
- Hasło zapisane w miejscu łatwym do znalezienia
- Konto, w którym nazwa użytkownika = hasło
- Hasło wywodzące się z nazwiska lub imienia użytkownika (efektywność 5-10%)
- Tylne drzwi pozostawione przez poprzedniego napastnika

Pracochłonny
(Pochłaniający dużo czasu)

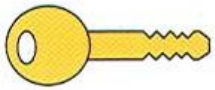
- Ataki słownikowe oparte na:
  1. Słowniku wyrazów powszechnie używanych
  2. Słowniku wyrazów danego języka
  3. Słownikach wyrazów i wzorów w innych językach
  4. Filtry podstawień; o=0, 1=!, dla=4, do=2, E=3
- Przykłady narzędzi wykorzystywanych przy odgadywaniu haseł

  Crack v5.0
  L0pht Crack v2.0 for NT
  NetBUS
  FastZip Password
  Jack the Ripper

Średni
(Wymaga zarówno wysiłku umysłowego, jak i zasobów obliczeniowych)

- Wyczerpujące wyszukiwanie klucza
- Złamanie szyfru asymetrycznego/ symetrycznego może zabrać wiele czasu w zależności od długości użytego klucza
- 40-bitowy: minuty
- 56-bitowy: godziny/dni
- 128-bitowy: nie do złamania!
- SSL PKCS#1

  Saltine Cracker



Ciężki
(Najbardziej zaawansowane metody kryptoanalityczne)

- Kryptoanaliza linearna
- Kryptoanaliza różnicowa
- Łamanie z kryptogramami
- Łamanie ze znanym tekstem jawnym
- Łamanie z wybranym tekstem jawnym
- Łamanie z adaptacyjnie wybranym tekstem jawnym
- Łamanie z wybranymi kryptogramami
- Łamanie z wybranym kluczem

Ataki hybrydowe

- Istnieje nieskończona liczba ataków hybrydowych wykorzystujących dowolną kombinację rozmaitych metod w różnych sekwencjach, zależnie od celu, poziomu wiedzy i doświadczenia napastnika.
- Ataki hybrydowe stanowią zdecydowaną większość wszystkich ataków.
- Uwaga! 80% włamań obejmuje działania wykorzystujące:
  1) znane, niezałatane luki,
  2) łatwe do odgadnięcia hasła.

Ataki hybrydowe

- Kilka przykładów …

Gromadzenie informacji

- Skanowanie portów
- Przechwytywanie pakietów
- Metody socjotechniczne
- War Dialing

Włamanie i przejęcie kontroli

- Wykorzystanie dobrze znanych słabych punktów
- Wykorzystanie złej konfiguracji systemu operacyjnego
- Odgadywanie haseł/Cracking
- Instalowanie narzędzi „rootkit”
- Dodawanie użytkownikom przywilejów by przejąć zdalnie kontrolę

Przestępstwa

- Zmienić, ukraść, zniszczyć ….
- DDoS, przerobienie strony internetowej
- Manipulowanie danymi
- Kopiowanie własności intelektualnej (bazy danych HR, listy płac, karty kredytowe…)

TYPY ATAKÓW

1. Buffer overflow

- zapisanie łańcuchów danych przekraczających rozmiar bufora, przy niedopracowanych aplikacjach może spowodować uzyskanie uprawnień do wykonywania swoich programów
- zapobieganie: instalacja łatek
- przykład: błędy ODBC w serwerze webowym Microsoft (Windows NT)

2. Wirusy, robaki i konie trojańskie

- znane z życia codziennego ☹
- zapobieganie: aktualne oprogramowanie antywirusowe, wyłączanie zbędnych usług

Wirusy komputerowe

Klasyfikacja wirusów

Wirus właściwy	Złośliwy program, który dokleja część lub cały swój kod do innego pliku. Zarażone pliki to zwykle pliki wykonywalne lub pliki danych z częścią wykonywalną.
Robak (Worm)	Złośliwy program, który ma zdolność do rozprzestrzeniania się do komputerów innych użytkowników. Najczęściej spotykaną formą dystrybucji jest e-mail.
Koń trojański	Złośliwy program, który kamufluje się jako oprogramowanie użyteczne lub służące do rozrywki, ale w rzeczywistości przeprowadza szkodliwe działania, np. niszczy dane.

Chociaż podział obejmuje trzy klasy złośliwych programów, to zdarza się, że autorzy wirusów piszą programy, które można zaliczyć do więcej niż jednej klasy. Przykładem są konie trojańskie, które usuwają dane i mogą rozprzestrzeniać się za pośrednictwem poczty elektronicznej.

Złośliwa działalność	Opis	Symptomy	Przykłady
Infekcja sieci	Znajduje dostępne w sieci serwery z plikami i infekuje znajdujące się tam pliki.	Zainfekowane pliki wykryte na serwerach i komputerach ze współdzielonymi zasobami. Wirusy takie mogą bardzo szybko się rozprzestrzeniać w sieci.	W32.Funlove, W32.HLLW.Bymer, Worm.ExploreZip
Masowy mailing	Wysyła e-maile do innych użytkowników, zwykle zawierające złośliwy kod osadzony w treści lub załączony do przesyłki.	Serwery pocztowe zaczynają pracować wolniej i załamują się. Wykorzystanie tego typu programu może być uważane za atak typu Denial of Service.	VBS.LoveLetter, Wscript.Kakworm, W32.Prolin.Worm, Worm.ExploreZip
Niszczenie plików	Różne pliki są usuwane z systemu lub uszkadzane. Usuwane pliki mogą obejmować określone typy lub wszystkie pliki atakowanego systemu.	Programy nie startują, pliki z danymi nie są dostępne, ogólna niestabilność systemu.	W32.Kriz, Worm.ExploreZip, VBS.NewLove.A
Eksport danych	Znajduje osobiste informacje, takie jak hasła i numery kart kredytowych, i wysyła je pod ustalony adres e-mailowy lub internetowy.	Zwykle nie ma zauważalnych od razu objawów działania, ewentualnie wyższe rachunki za dostęp do Internetu.	Buddylist, PWSteal.Trojan
Przejęcie systemu	W różnych składnikach systemu są instalowane punkty zaczepienia, pozwalające monitorować lub unieruchamiać te składniki, ewentualnie zmieniać sposób ich działania. Czasami punkty zaczepienia są wykorzystywane do uruchamiania złośliwych programów.	Z normalną pocztą mogą być wysyłane dodatkowe e-maile; funkcjonowanie przeglądarki może być ograniczone lub zmienione.	W95.MTX, W32.Navidad, Happy99.Worm
Niszczenie sprzętu	Próbuje wymazać BIOS lub usunąć ustawienia CMOS.	Wewnętrzny test po włączeniu urządzenia może nie startować; dyski twarde mogą nie być właściwie rozpoznawane.	W32.Kriz, W95.CIH W32.Navidad, KeyPanic.Trojan
Wizualne treści	Wyświetla komunikaty lub grafikę.	Mogą się pojawiać różne komunikaty lub obrazki. W paskach narzędziowych mogą się pojawić nowe ikony.	Happy99.Worm
Tylne drzwi/ zdalna kontrola	Po zainstalowaniu w systemie programy te „nasłuchują" instrukcji z innych komputerów, a następnie je wykonują.	Zwiększony ruch sieciowy. Nietypowa aktywność na portach IP/UDP. Napastnicy przeprowadzający atak typu Denial of Service często wykorzystują mechanizmy tylnych drzwi.	Backdoor.SubSeven, BackOrifice, NetBus
Socjotechnika	Metody, jakimi twórcy wirusów posługują się, by fałszywie przedstawić swój program użytkownikom i zachęcić ich do uruchomienia go.	Użytkownik może otrzymać e-mail, który ma intrygujący, zachęcający temat lub treść. Czasami można natknąć się na pliki wysłane do grup dyskusyjnych, które są rzekomymi zdjęciami o treściach seksualnych itp.	W32.Funlove, PrettyPark.Worm, Mypics.Worm

Uwaga: *Informacje o tych i innych złośliwych programach można znaleźć na stronach Symantec AntiVirus Research Center, http://www.sarc.com*

3. Spoofing (podszywanie się)

- podrabianie wiarygodnej tożsamości,
  - fałszowanie adresu IP (zaufanie serwera lub udawanie kogoś innego),
  - podrabianie zaufanej witryny (może klient się „zaloguje”),
  - inne;
- zapobieganie: zabezpieczenia firewall’a, podpisy cyfrowe, urządzenia.

4. Podszywanie się/Spoofing

Rodzaj	Scenariusz	Jak to możliwe	Jak zapobiegać
E-mail	Wysłanie podrobionego e-maila z fałszywym wierszem „Od:" do serwera SMTP	Brak uwierzytelniania w SMTP	Sprawdzać źródłowy adres IP komunikatu lub używać podpisów cyfrowych
Przekaźnik poczty anonimowej	Napastnik wysyła e-mail z konta na przekaźniku poczty anonimowej	Brak uwierzytelniania w SMTP	Używać podpisów cyfrowych
Login	Wykorzystanie czyjejś nazwy użytkownika i hasła do dostania się do hosta	Brak ostrożności przy hasłach	Chronić hasła lub używać silnego uwierzytelniania
Rutowanie	Wysłanie podrobionych pakietów RIP lub ICMP do routera lub pakietu w trybie source routed do hosta	Brak uwierzytelniania w protokołach RIP, przekierowanie ICMP, trybie source routed	Nie używać tych protokołów w komunikacji z niezaufanymi sieciami
Partner	Wysłanie podrobionego e-maila do InterNIC z prośbą o zmianę nazwy domeny internetowej lub podmianę adresu IP	InterNIC nie stosuje pełnego uwierzytelniania, chyba że żąda tego klient	Zapewnić uwierzytelnianie zmian domeny w InterNIC
Spoofing DNS	Wysłanie nieproszonej odpowiedzi z podrobioną nazwą domeny i adresem do serwera DNS ofiary	Brak uwierzytelniania w DNS	Używać zmodyfikowanego DNS, który nie buforuje wpisów
Adres IP	Wysłanie pakietu z podrobionym źródłowym adresem IP do „ufającego" hosta	Adres źródłowy jest rzadko sprawdzany	Zablokować dostęp z zewnątrz przez zaufane wewnętrzne adresy
Przejęcie kontroli nad sesją	Napastnik wstawia podrobione pakiety do zestawionej sesji; przykładowe narzędzia: HUNT i Juggernaut	Uwierzytelnienie już było	Szyfrować sesje
Spoofing www http://www.cs.princeton.edu/sip/pub/spoofing.html	Napastnik sporządza kopię całej strony internetowej, ruch przechodzi przez komputer napastnika, co pozwala mu śledzić działania ofiary, przechwytywać hasła i numery kont	W ataku "man-in-the-middle" napastnik przepisuje wszystkie adresy URL ze strony internetowej, tak że kierują one ofiarę na serwer napastnika	Wyłączyć obsługę JavaScript, zwrócić uwagę, by w przeglądarce była wyświetlana linia adresu, kontrolować wyświetlany adres URL

5. Denial of Service (DoS)

- DoS (odmowa świadczenia usługi) przy użyciu standardowych protokołów lub procesów blokuje usługi, np. „ping śmierci”, otwierająca się ogromna liczba okienek,
- zapobieganie: właściwa konfiguracja firewall’a oraz zabezpieczenia po stronie komputera klienta, a także np. monitorowanie sieci.

Denial of Service (DoS, DDoS)

Atak	Dysk	Pasmo	Wewnętrzna struktura danych lub przepełnienie bufora	Cykle CPU lub załamanie	Uwagi
Przesłanie dużych plików przez FTP	X				Wypełnia dysk danymi-śmieciami
Spowodowanie wpisu obszernych komunikatów o błędach do dziennika	X		X	X	Przepełnia dysk lub bufor
SYN Flood			X		Zamyka port na krótki czas
Teardrop			X	X	Wykorzystuje nachodzące na siebie fragmenty pakietów IP
Smurf		X			Przekierowuje broadcast, jako źródło podaje adres IP ofiary
Snork		X			Wysyła fałszywy komunikat o błędzie do portu 135 w NT
Bomba UDP		X		X	Fałszywy pakiet pomiędzy portami echo i chargen
Atak OOB			X	X	Użycie podrobionych wartości istotnych wskaźników danych
Ping of Death			X	X	Przepełnienie bufora datagramami IP
Flood Ping		X		X	Zalewa sieć
WinNuke			X	X	Wysyła śmieci do portu 139 w NT
Land			X	X	Podaje jako źródło adres ofiary
Bomby e-mailowe, spam	X			X	Zapycha serwer/bramkę pocztową lub skrzynkę użytkownika

Przykłady: Mailbombs, SYN FLOOD, Aenima 2.0, WIN NUKE, ZERO LENGTH, Wnuke5, WinGenocide, Avalanche 3.0 4.0, Nuker, LiquidNuker

Atak Distributed Denial of Service (DDos) Przykłady: Trinoo, TFN, TFN2K, Stacheldraht

Bardzo poważne zagrożenie, wykorzystujące wiele komputerów w skoordynowanym ataku mającym na celu wyczerpanie przepustowości routera i zasobów stosu sieciowego, a w rezultacie zerwanie łączności

1) Stworzenie sieci komputerów do ataku DDoS przez włamanie się do tych komputerów, zdobycie uprawnień root, zapewnienie zdalnej kontroli i zainstalowanie oprogramowania służącego do ataku
2) Wysłanie do wszystkich przejętych komputerów pakietów z instrukcjami o typie ataku, czasie jego trwania i adresie celu
3) Sieć komputerów DDoS wysyła strumienie pakietów (z fałszywymi adresami źródłowymi) do ofiary (np. atak Smurf, wysyłanie do ofiary dużej ilości pakietów echo)

6. Session Hijacking

- przejęcie istniejącego połączenia i odgrywanie roli jednej ze stron,
- zapobieganie: instalacja łatek, właściwe projektowanie i implementacja oprogramowania.

ATAKI BAZODANOWE

Ataki bazodanowe

- Wstrzyknięcia kodu SQL (ang. *SQL Injection*)
- DoS (ang. *Denial of Service*, odmowa usługi) za pomocą SQL Injection
  - DDoS (ang. *Distributed Denial of Service*, rozproszona odmowa usługi)
- Account lockout attack
  - eBay (2007 r.), Allegro (2010 r.) ukryły nicki użytkowników

Ataki bazodanowe (2)

- *Cross Site Scripting* (XSS)
- *Wildcard attack*
- Sposób ataku na serwis WWW polegający na osadzeniu w treści atakowanej strony kodu (zazwyczaj JavaScript).
- Dane, które pochodzą z zapytania otrzymanego od klienta (np. pola formularzy), są ponownie wyświetlane na stronie serwisu bez uprzedniego sprawdzenia, czy nie występują w nich niebezpieczne metaznaki.

Uzyskiwanie dostępu do systemu

- Uzyskiwanie dostępu do systemu

```
SELECT * FROM USERS WHERE USERNAME LIKE 'POBRANY_LOGIN' AND
PASS LIKE 'POBRANE_HASLO';
```

- Przykład ataku

```
SELECT * FROM USERS WHERE USERNAME LIKE ' ' OR 1 = 1; --
```

- Przekazywanie wielu zapytań (modyfikacja bazy danych)

```
SELECT * FROM USERS WHERE USERNAME = 'x'; DROP TABLE USERS;
SELECT '1';
```

DoS za pomocą SQL Injection

```
SELECT * FROM USERS WHERE USERNAME = 'x' OR
BENCHMARK(9999999,
BENCHMARK(999999,
BENCHMARK(999999, MD5(NOW()))))) = 0;
```

Inne ataki bazodanowe - *Wildcard attack*

```
SELECT * FROM TABLE WHERE COLUMN LIKE '%something%,
_[^!_%/%a?F%_D)_(F%)_%([)({}%){()}£$&N%_)$*£()$*R"_)][
  %](%[x])%a][$*„£$-9]_
```

Jak chronić swoje aplikacje przed SQL Injection?

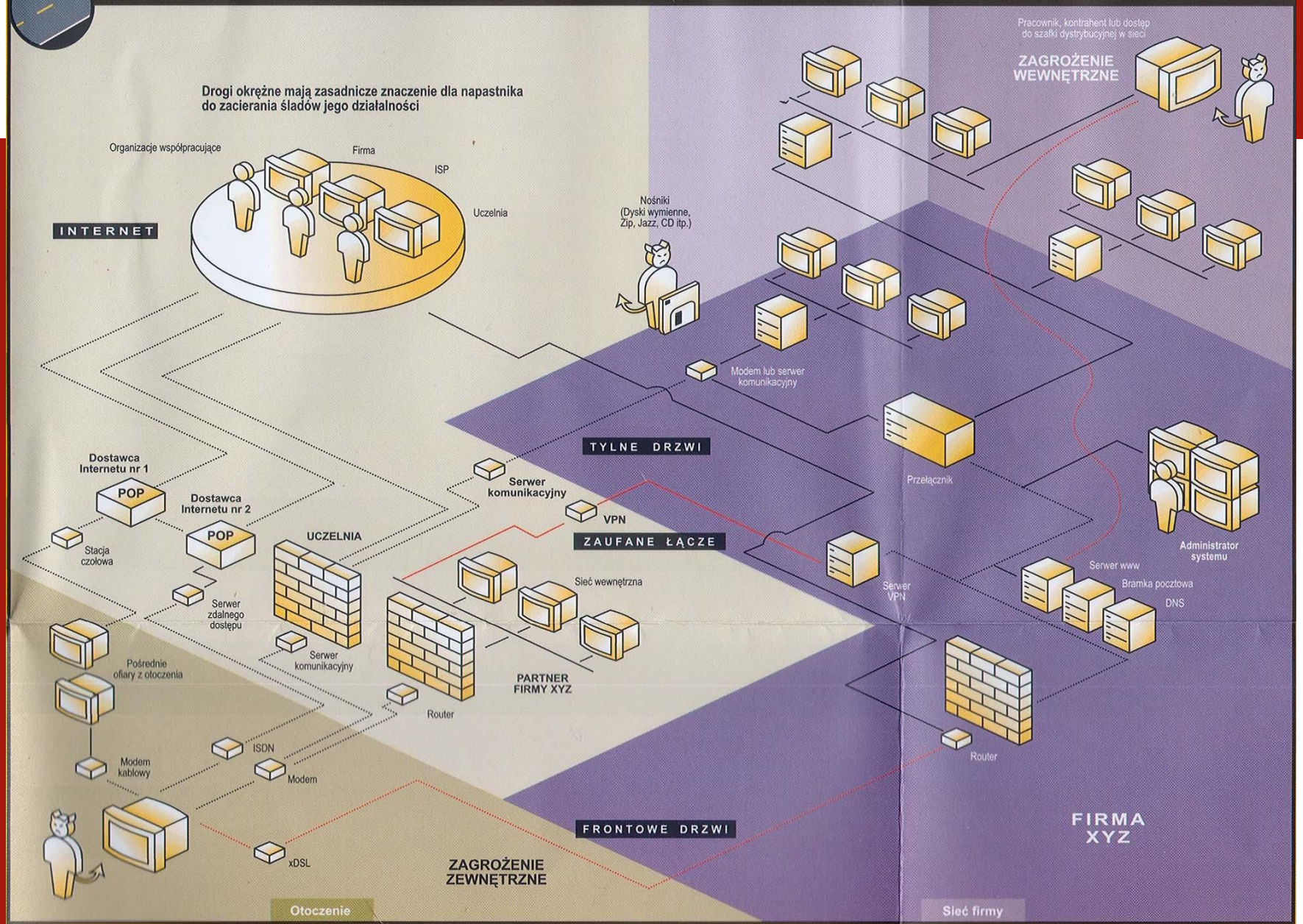
- Na poziomie aplikacji
  - Niedopuszczenie do przekazania znaku ’ do zapytania
  - „Zaślepki”
  - Rzutowanie łańcucha znaków na wartość liczbową.
  - Wyłączenie komunikatów o błędach lub ich zastąpienie.
- Na poziomie bazy danych
  - Ograniczenie uprawnień aplikacji
- Na poziomie serwera aplikacji
  - Odfiltrowywanie podejrzanych zapytań

Przykład

- AltoroMutual Bank – strona (http://demo.testfire.net/bank/login.aspx)

UMIEJSCOWIENIE BAZY DANYCH W ARCHITEKTURZE SIECI FIRMOWEJ

7. Drogi ataku



8. Luki w zabezpieczeniach

1. Łatwe do odgadnięcia hasła

- Zbyt krótkie
- Zbyt proste (niewykorzystujące cyfr, małych i wielkich liter oraz znaków specjalnych)
- Wykorzystujące pospolite wyrazy (słownikowe)
- Oparte na prostych trikach (dodanie cyfry do nazwy użytkownika lub odwrócenie nazwy użytkownika)

2. Nieaktualne oprogramowanie (niezainstalowane poprawki programowe bezpieczeństwa)

3. Złe administrowanie systemem

- Niewyłączone usługi (każdy system operacyjny ma dużo ustawień domyślnych)
- Konta niezamknięte lub zbyt wiele kont
- Pozostawione konta domyślne
- Niedostatecznie kontrolowane usługi zaufane

4. Złe obchodzenie się z informacjami poufnymi

- Zapisywanie haseł (w miejscach dostępnych dla innych)
- Przesyłanie poufnych danych w e-mailu (to jak na pocztówce)
- Użycie protokołów przesyłających jawnie hasła (FTP, HTTP, POP3, Telnet, SNMP)
- Przesyłanie poufnych informacji przez FTP lub HTTP

5. Nieprzeszkolony personel bez świadomości zagrożeń bezpieczeństwa

- Podatny na metody socjotechniczne
- Nieznający powodów i metod ochrony prywatności informacji

6. Wykorzystanie zaufanych usług w niezaufanych sieciach

- NFS
- Współdzielenie dysków w Windows
- Komendy „r" (rsh, rlogin, rexec)
- X Window

7. Brak ostrożności przy protokołach bez uwierzytelniania

- DNS
- SMTP
- RIP
- ICMP Redirect
- Tryb source routing

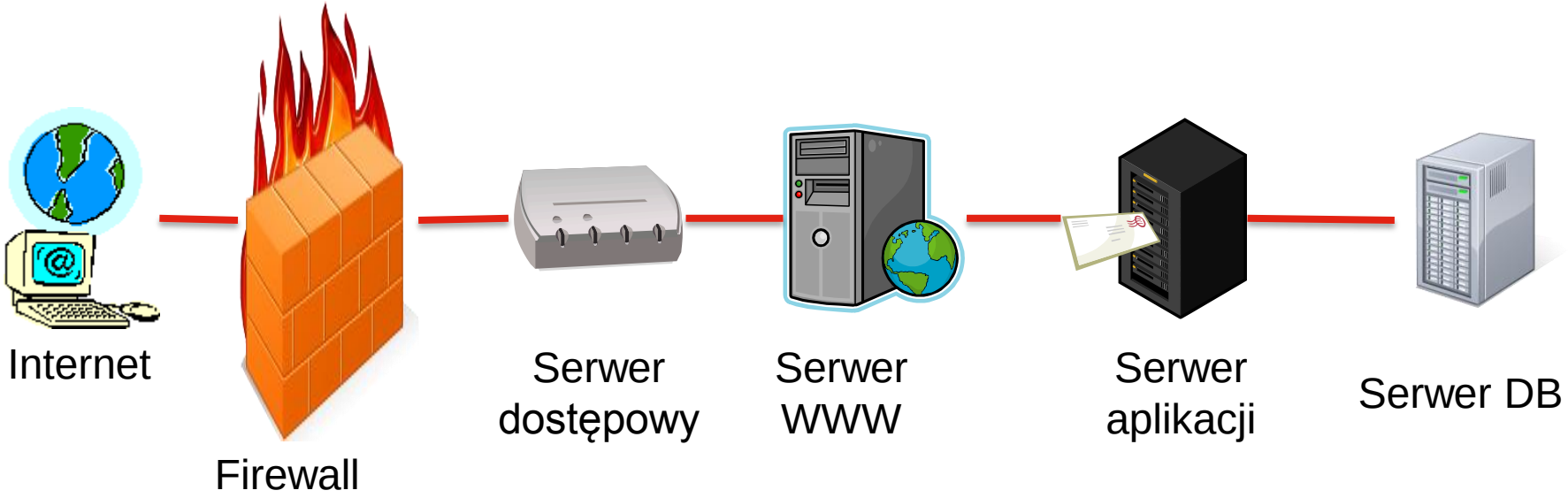
8. Brak ostrożności w obchodzeniu się z otrzymanym od innych oprogramowaniem

- Kod wykonawalny (konie trojańskie, wirusy)
- Aktywna zawartość (szczególna forma kodu wykonawczego, np. JavaScript, ActiveX, Java, makra, PostScript)
- Wstawianie danych do swoich skryptów (mogą zawierać specjalne znaki, ukryte komendy lub doprowadzać do przepełnienia bufora)

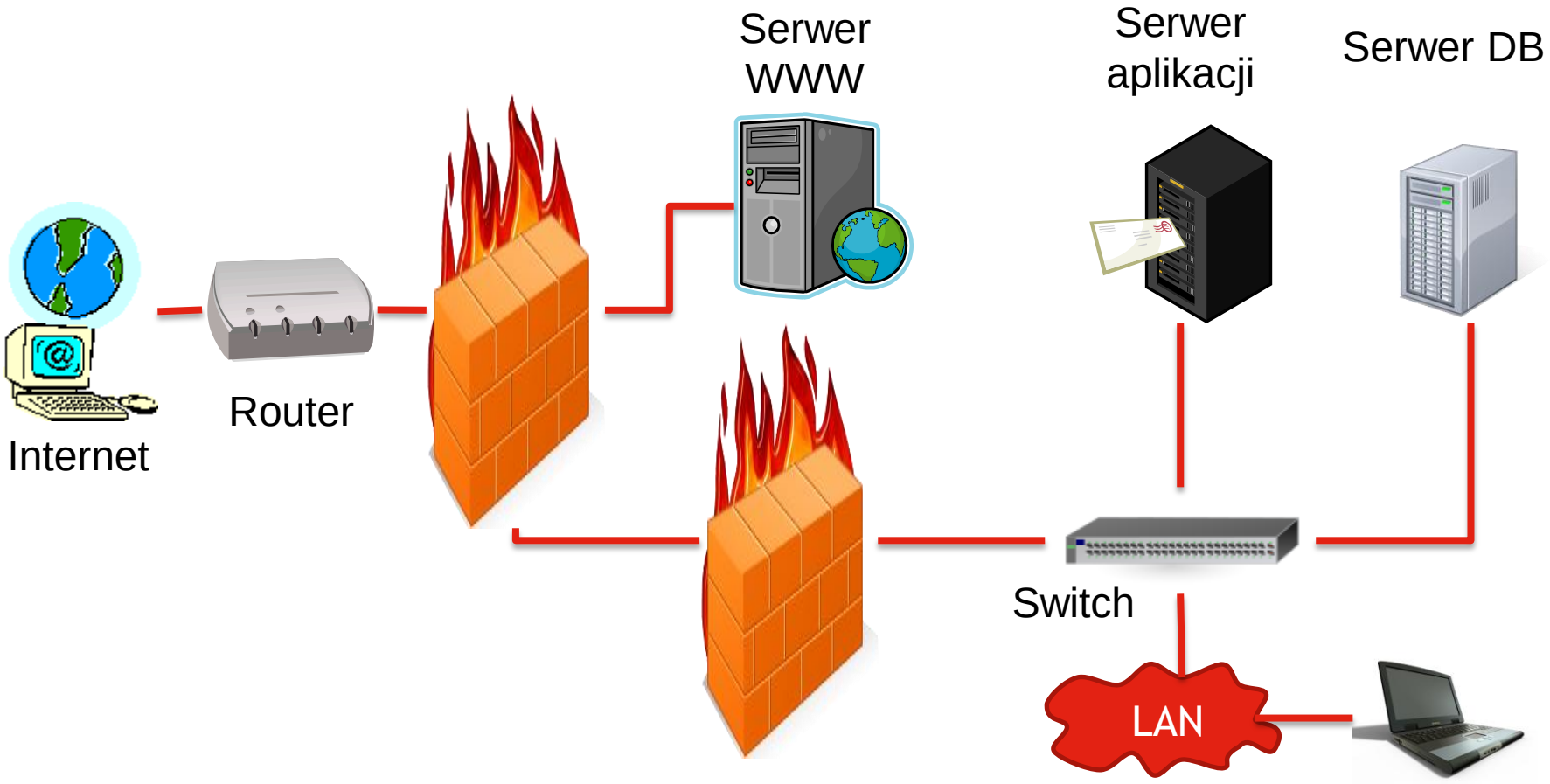
9. Nieodpowiedzialność producenta

- Pozostawione furtki w oprogramowaniu
- Brak wbudowanych zabezpieczeń
- Słaba kryptografia, wykorzystanie kluczy 40-bitowych

Umiejscowienie BD - przykład 1.



Umiejscowienie BD - przykład 2.



Metody i standardy bezpiecznej transmisji danych w niezabezpieczonej sieci?

SIECI WIRTUALNE

Słabość protokołów sieciowych

- Protokoły HTTP, POP3 → IMAP, SMTP przesyłają dane przez sieć w sposób jawny
  - „podsłuchanie”
  - modyfikacja przesyłanych danych

⇨HTTPS (ang. *Hypertext Transfer Protocol Secure*) – szyfrowana wersja HTTP:

- szyfruje dane niegdyś przy pomocy protokołu SSL, natomiast obecnie używany jest protokół TLS
- HTTPS działa domyślnie na porcie nr 443 w protokole TCP

Podstawy szyfrowania

- **Szyfrowanie symetryczne** - do szyfrowania i deszyfrowania wykorzystywany jest ten sam klucz
- **Szyfrowanie asymetryczne -** klucz szyfrujący jest inny niż deszyfrujący
- **Klucz prywatny** (tajny) i **Klucz publiczny**
- **Podpis cyfrowy**
- **Certyfikat cyfrowy**; centrum certyfikacji (ang. CA – *Certificate Authority*)

Przykładowe algorytmy szyfrujące

- **DES** - jeden z najpopularniejszych symetrycznych algorytmów szyfrujących, używany m. in. przez rząd USA do szyfrowania ważnych wiadomości
- **RSA -** najpopularniejszy algorytm z kluczem publicznym oparty na liczbach pierwszych. Stosuje się go do szyfrowania oraz do podpisów cyfrowych
- **DSA -** algorytm szyfrujący wykorzystywany do podpisów cyfrowych
- **MD5 -** algorytm szyfrujący w jedną stronę - takiej wiadomości nie można odszyfrować, stosowany np. do szyfrowania haseł użytkowników. Zaszyfrowane hasło jest przechowywane w bazie. Weryfikacja użytkownika polega na zaszyfrowaniu podanego hasła i porównaniu go z hasłem przechowywanym w bazie

Protokół SSL (ang. *Secure Socket Layer*)

- Zapewnia podstawowe funkcje bezpieczeństwa:
  - uwierzytelnianie stron – czyli potwierdzanie ich autentyczności na podstawie certyfikatów
  - poufność i integralność przesyłu – tzn. ochronę przed podsłuchiwaniem i modyfikacją
- Proces uwierzytelniania przy użyciu asymetrycznych algorytmów kryptograficznych
- Po uwierzytelnieniu stron następuje wymiana danych przy użyciu któregoś z symetrycznych algorytmów – znacznie szybszych

Protokół TSL (ang. *Transport Layer Security*)

- Rozwinięcie protokołu SSL
- Wersje: **SSL** 1, 2, 3, **TLS** 1.0, 1.1, 1.2
- HTTP → HTTPS
- Może służyć do zabezpieczania wielu innych protokołów np.: Telnet, SMTP, POP, IMAP, FTP

Umiejscowienie BD – sieci wirtualne

Tunelowanie:

1. z wykorzystaniem SSL (przezroczyste dla zapory).
2. z wykorzystaniem IPSec,

VPN (*Virtual Private Network*) – wirtualna sieć prywatna korzysta z publicznej infrastruktury telekomunikacyjnej, protokołów tunelowania i procedur bezpieczeństwa danych (Uwaga: wykorzystywana również w ramach LAN do odseparowania fragmentu sieci).

Ramka IPSec w trybie transportowym i tunelowym

http://pl.wikipedia.org/wiki/IPsec

Tryb transportowy i tunelowy [edytuj]

Nagłówek IPSec - ESP można stosować w dwóch trybach: transportowym lub tunelowym. Natomiast nagłówek AH wykorzystywany jest tylko w trybie transportowym. Przypomnijmy jak wygląda typowy pakiet IP (załóżmy że protokołem wyższej warstwy będzie TCP):

```
+----+-----+--------------------
| IP | TCP | dane użytkownika...
+----+-----+--------------------
```

Tryb transportowy

```
+----+-----+==========================
| IP | ESP | TCP | dane użytkownika...
+----+-----+==========================
```

Tryb tunelowy zapewnia wyższy poziom ochrony

```
+-----+-----+================================
| IPn | ESP | IP | TCP | dane użytkownika...
+-----+-----+================================
-------------------------------(VPN)-------------------------------
10.1.1.0/24 ----- B1 ========= B2 ------ 10.2.2.0/24
```

	MODEL OSI	INTERNET	PROTOKOŁY
Dane	Aplikacji Prezentacji Sesji	Aplikacji	HTTP, DNS, SMTP, POP3, FTP, SSH, DNS ...
Segment	Transportowa	Transportowa	TCP, UDP, SPX
Datagram	Sieci	Sieci	IP, IPX, AppleTalk
Ramka	Łącza danych	Łącza danych	Ethernet 802.11, token ring, PPP
Bity	Fizyczna	Fizyczna	

Źródło: http://pl.wikipedia.org/wiki/IPsec

ZAGROŻENIA?

SKŁADOWANIE, ARCHIWIZACJA I OCHRONA DANYCH

Fizyczne zagrożenia

	1. Zdobycie fizycznego dostępu	2. Atak
Podstawowe	- Włamanie przez wyważenie drzwi, użycie łomu... - Przeczołganie się pod podniesioną podłogą, wzdłuż duktów kablowych lub przez przestrzeń międzysufitową - Otwarcie mechanicznego zamka, zdobycie lub skopiowanie kluczy - Aktywacja wewnętrznego przycisku otwierającego drzwi lub wsunięcie pod drzwi płytki w celu uaktywnienia sensora ruchu	Kradzież komputera, laptopa (np. na lotnisku), taśmy z kopią zapasową, dysków i zastąpienie ich niezapisanymi nośnikami - Użycie dysku startowego do zabezpieczonego systemu, hack NTFS2DOS.exe - Włamanie do szafek dystrybucyjnych w miejscach publicznych, a następnie podsłuchiwanie/ zniszczenie/inne działania - Przeszukiwanie śmieci w celu znalezienia dokumentacji papierowej - Odzyskiwanie dokumentów z niszczarek - Podglądanie, wykorzystanie dużych powiększeń fotograficznych, podsłuchiwanie wprowadzania numerów PIN
Zaawansowane	- Pokonanie systemu alarmowego, wrażliwego na ruch, z pasywnym detektorem IR (zmiany temperatury), mikrofalami (odbicia) - Wykorzystanie systemu identyfikatorów/czytnika kart/FOBS/ataku man-in-the-middle ze strojonymi obwodami LC pomiędzy „panelem" a „maszyną kontrolną" - Złamanie czytnika kart lub zduplikowanie kart relatywnie łatwe (12-bitowy kod osobisty, 8-bitowy kod instalacyjny) - Wykorzystanie błędnej weryfikacji przez system biometryczny (wady projektowe), złamanie czytnika odcisków palców, użycie powtórzeń	- Podsłuchiwanie łączy przewodowych oraz nagrywanie wideo i audio - Ataki z wykorzystaniem koni trojańskich (niewykrytych agentów) - Rejestrowanie użytkowania klawiatury, zastąpienie klawiatury podobnie wyglądającą klawiaturą rejestrującą lub przesyłającą sygnał radiowy - Fałszowanie kart elektronicznych, może być bardzo trudne - Wykorzystanie nadajnika radiowego, efektu van Ecka, przechwytywanie obrazu z monitora - Wykorzystanie wad BIOS-u (specjalne hasło, pewne kombinacje klawiszy) - Zdobycie prywatnych kluczy szyfrujących - z CA lub lokalnych, a następnie złamanie ich

Zagrożenia

- Zagrożenia miejsca (budynku, pojazdu itp.)
  - huragan, trzęsienie ziemi, powódź itp.,
  - utrata zasilania, wojna, terroryzm;
- Awarie sprzętu
  - uszkodzenia pamięci masowej (np. dysku),
  - błąd procesora,
  - niedziałająca infrastruktura sieciowa;
- Awaria logiczna
  - błędy oprogramowania,
  - wirusy, robaki, itp.
  - przypadkowe usunięcia danych.

Zagrożenia miejsca – wybrane techniki zapobiegania utratom danych:

- redundancja sprzętu – replika bazy danych wraz ze sprzętem na serwerze zapasowym (np. 30 km dalej),
- zasilacze UPS, własne generatory,
- monitorowanie i zabezpieczenie obiektów, systemy alarmowe itp.

Awarie sprzętu – wybrane techniki zapobiegania utratom danych:

- redundancja sprzętu,
- macierze RAID 1 (mirroring), RAID 5,
- backup i archiwizacja.

Błędy w oprogramowaniu - wybrane techniki zapobiegania utratom danych:

- takie, jak poprzednio,
- ochrona antywirusowa, aktualizacja oprogramowania, zapory sieciowe, itp.
- projektowanie, implementacja, testowanie i walidacja oprogramowanie metodami formalnymi

Archiwizacja

- Rodzaje backupów
  - pełny (ang. *full backup*),
  - różnicowy (ang. *differential backup*)
    - w odniesieniu do ostatniej pełnej kopi zapasowej,
  - przyrostowy (ang. *incremential backup*)
    - nie kumuluje plików nowych i zmodyfikowanych,

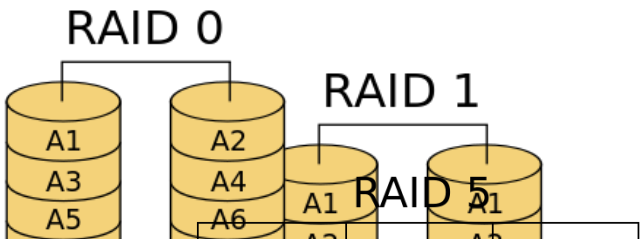
  - lokalny
  - sieciowy

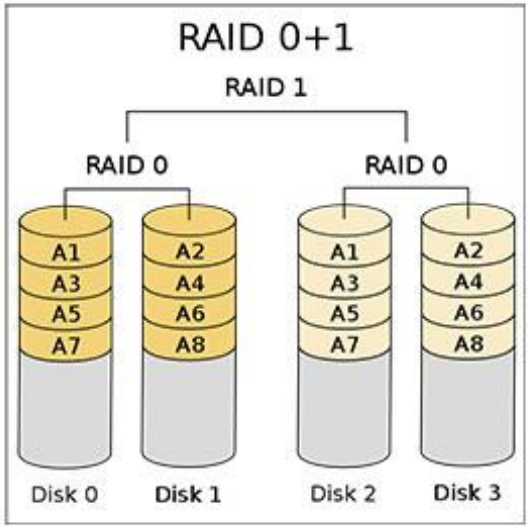
Przykłady urządzeń wykorzystywanych do archiwizacji:

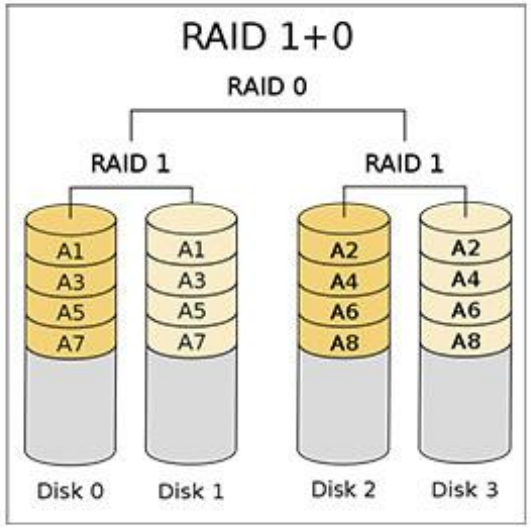
- macierze dyskowe RAID (ang. *Redundant Array of Independent Disks)* – nadmiarowa macierz niezależnych dysków
- urządzenia taśmowe (ang. streamer)
- nośniki optyczne (CD/DVD/…) i magnetooptyczne

Macierze dyskowe

- pojemności dysków: do 6 TB
- macierze dyskowe RAID
  - RAID 0 (stripping)
  - RAID 1 (lustrzany)
  - RAID 2
  - RAID 3
  - RAID 4
  - RAID 5
  - RAID 6
  - RAID 0+1
  - RAID 1+0







RAID

Poziom RAID	Minimalna liczba dysków (N)	Dostępna przestrzeń	Max liczba dysków, które mogą ulec awarii
0	2	N	0
1	2	1	N-1
2	3	N-log N	1
3	3	N-1	1
4	3	N-1	1
5	3	N-1	1
6	4	N-2	2
0+1	4	zależnie od konfiguracji	zależnie od konfiguracji
1+0	4	zależnie od konfiguracji	zależnie od konfiguracji

Urządzenia taśmowe

- Strimer (ang. *streamer*);
- DDS (ang. *Digital Data Storage*) zapis skośny na taśmach muzycznych DAT (ang. *Digital Audio Tape*),
- DLT (ang. *Digital Linear Tape*),
- LTO (ang. *Linear Tape-Open*),
- AIT (ang. *Advanced Intelligent Tape*),
- QIC (ang. *Quarter Inch Cartridge*).

Urządzenia taśmowe (2)

- Zapis liniowy:
  - szeroka taśma, ang. wide (19 – 25,4 mm)
  - ½" (12,7 mm)
  - 8 mm
  - ¼" (6,35 mm)
  - „ósemka”, ang. „*eighth*” (0,15) inch (3,81 mm)
  - żyłka, ang. *stringy* (1,58–1,9 mm)
- Zapis skośny (helikalny):
  - ¾ " (19 mm)
  - ½" (12,7 mm)
  - 8 mm
  - „cztery milimetry” (3,81 mm)

Urządzenia taśmowe (3)

- Przykłady:
  - DAT (ang. *Digital Audio Tape*), np. DDS-6 80 GB, 5MB/s
  - DLT (ang. *Digital Linear Tape*), np. SDLT600 300GB/600 GB, 36 MB/s
  - LTO (ang. *Linear Tape-Open*), np. LTO-2 200/400GB; LTO-3 400/800 GB; LTO-4 800/1600 GB; LTO-5 1600/3200 GB; LTO-6 2500/6250 GB, 160 MB/s
  - przyszłościowe: LTO-7 … LTO-10 do 48 TB,

Urządzenia taśmowe (4)

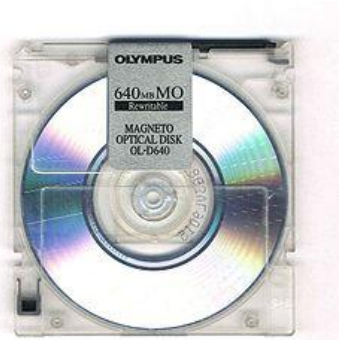
- AIT (ang. *Advanced Intelligent Tape*), np. AIT-5 400 GB, 24 MB/s
- QIC (ang. *Quarter Inch Cartridge*)
  - Travan (TR), np. TR-5 10000 MB, 1024 kB/s

Nośniki optyczne

- CD
  - pojemności: ok. 700 MB
- DVD
  - pojemności: 4,7 GB – 17,08 GB
- HD DVD
  - pojemności: 15 GB, 20 GB
- Blu-ray Disc (BD)
  - pojemności: 25 GB, 50 GB, 100/128 GB (BDXL)

Nośniki magnetooptyczne (MO)

- pojemności: 5,2 GB, 9,1 GB
- dysk z danymi jest umieszczony w specjalnej kasecie co pozwala na wydłużenia okresu archiwizacji nawet do 100 lat,
- dostępne także w wersji WORM (ang. *Write Once, Read Many*) – do jednorazowego zapisu; RW – wielokrotnego zapisu.



UWIERZYTELNIENIE I AUTORYZACJA

Uwierzytelnienie i autoryzacja

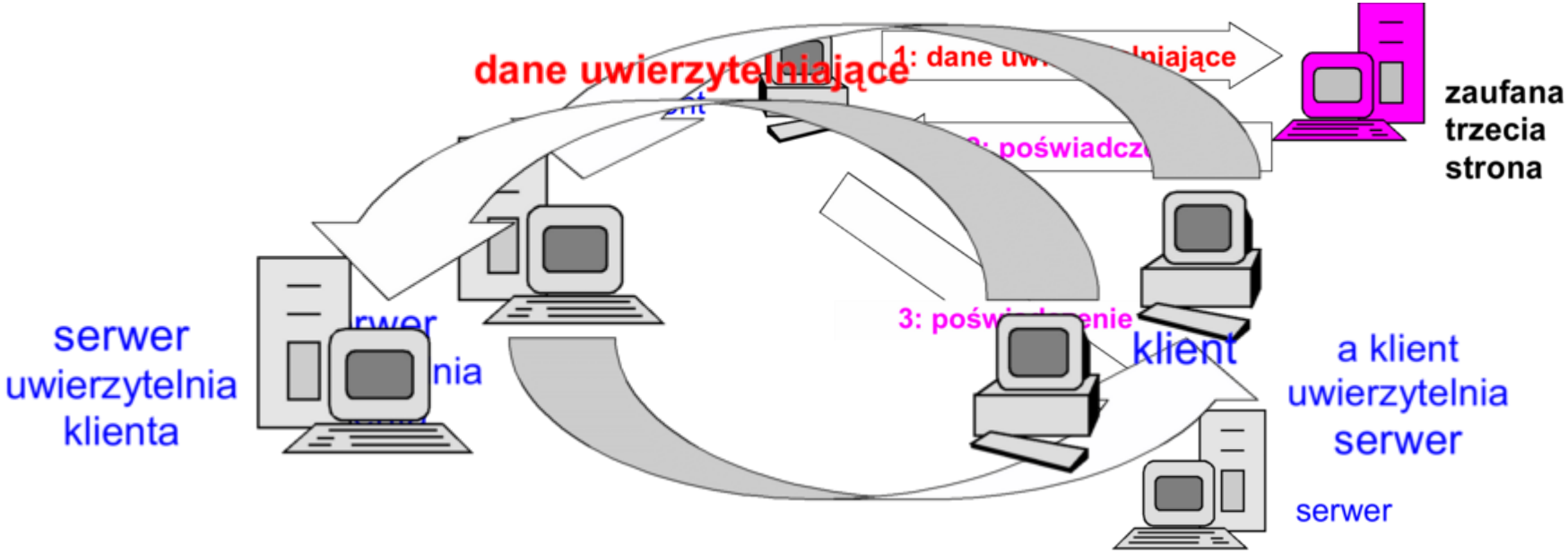
- **Uwierzytelnienie** – proces mający na celu identyfikację klientów aplikacji, np. użytkowników końcowych, usług, procesów lub komputerów
- **Autoryzacja** – proces mający na celu ustalenie, które zasoby i operacje powinny być dostępne danemu uwierzytelnionemu klientowi. Dotyczy to zasobów takich jak pliki, bazy danych, zasoby systemowe.

Uwierzytelnienie i autoryzacja (2)

- Mechanizmy uwierzytelnienia i autoryzacji są różne i zależą od konkretnego SZBD
- Zazwyczaj użytkownicy dzieleni są na **grupy** natomiast grupom nadawane są określone **uprawnienia**
- Ponadto niezbędnym dobrym nawykiem administratora baz danych powinno być rejestrowanie i monitorowanie zdarzeń na serwerze w poszukiwaniu nietypowych zdarzeń

Uwierzytelnienie

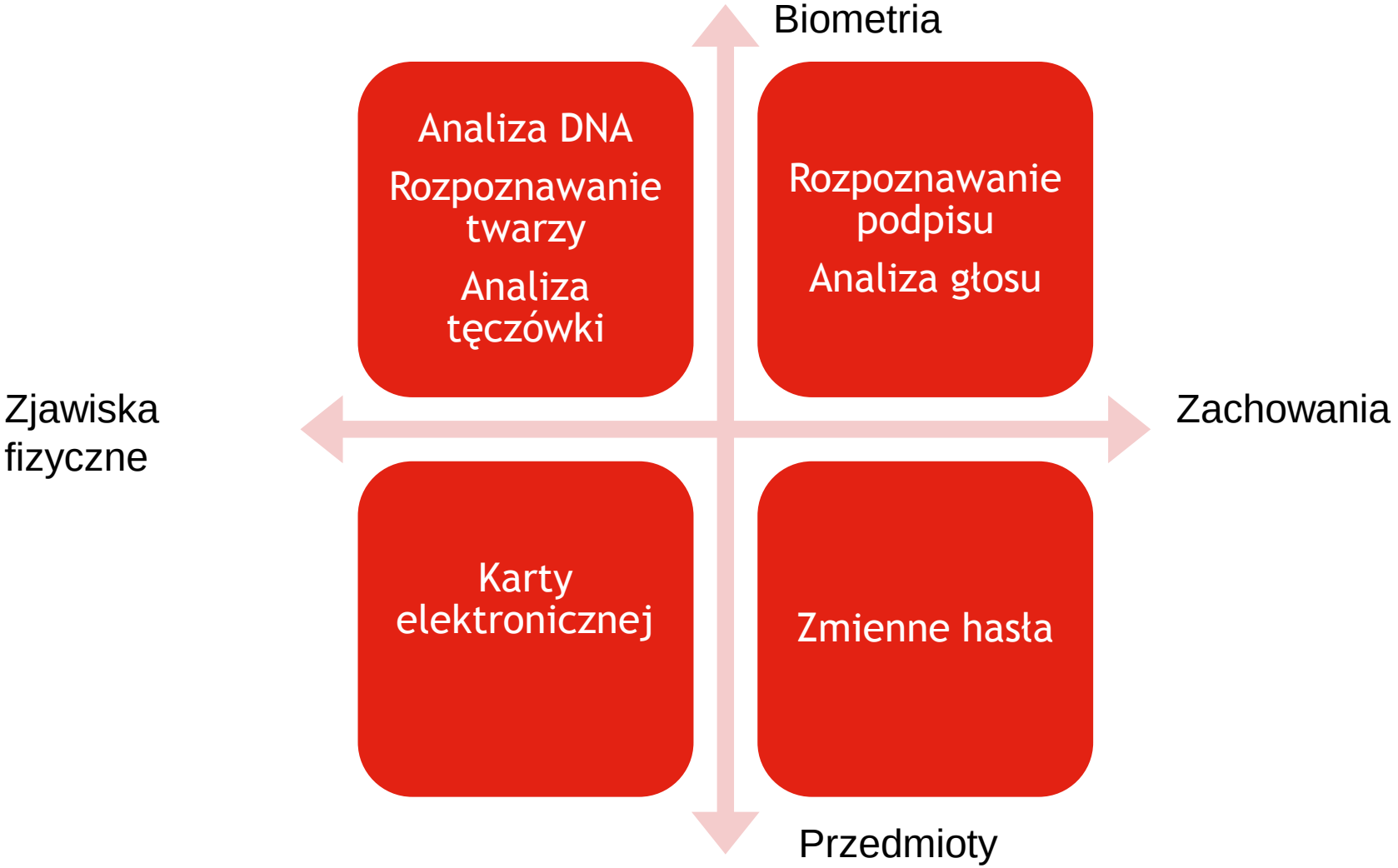
- Jednokierunkowe
- Dwukierunkowe
- Z udziałem zaufanej trzeciej strony



Uwierzytelnianie - typy metod

1. „WIEM” = coś, co wiesz (ang. *something you know*)
2. „MAM” = coś, co masz (ang. *something you own*)
3. Biometryczne (ang. *something you are*)

Klasyfikacja metod uwierzytelniania



Uwierzytelnianie – „WIEM”

- Hasła
  - najprostsza i najczęściej wykorzystywana metoda typu „WIEM”
  - ciąg znaków alfanumerycznych (czasem tylko liczby, np. PIN)

Metody nielegalnego pozyskiwania haseł:

- Wykradnięcie hasła z bazy (zabezpieczenie: szyfrowanie jednokierunkowe haseł, szyfrowanie danych na dysku)
- Przechwycenie – podsłuchanie transmisji (zabezpieczenie: np. techniki związane z bezpieczną transmisją, odpowiednie technologie trudne do podsłuchu, np. światłowody)
- Metoda siłowa (zabezpieczenie: wymuszenie odpowiedniego doboru haseł, okresów ważności itp.
- Metody socjotechniczne (zabezpieczenie: szkolenie pracowników, kontrole, audyty)

Przykłady zaleceń odnośnie haseł:

- minimalna liczba dni między zmianami: 0
- maksymalna liczba dni między zmianami: 40
- sugerowany okres stosowania: 30
- minimalna długość: 8
- rozmiar alfabetu: 36
- niepowtarzalność: TAK

Hasła – uwagi

- Zbyt trudne hasła – „konieczność” zapisywania, najczęściej karteczka naklejona na monitorze ☺
- Zbyt częsta konieczność zmiany – taka sama nazwa jak wcześniej z kolejną cyferką na końcu
- Wiedzę zawsze można z człowieka „wydobyć”

Uwierzytelnianie – „MAM”

- Do uwierzytelnienia wykorzystujemy przedmiot będący w posiadaniu uprawnionej osoby
- W procesie weryfikacji wykorzystujemy informację zapisaną lub generowaną „w przedmiocie” (dodatkowo może być wymagana zapamiętana informacja – „WIEM”)

Uwierzytelnianie – „MAM”

- Cechy metod tego rodzaju:
  - przedmiot powinien być „wygodny w noszeniu” i trudny do wykradzenia,
  - zapisana informacja nie powinna być dostępna do uzyskania inaczej, jak tylko w procesie autoryzacji,
  - w przypadku zagubienia lub kradzieży istotna jest możliwość jak najszybszego unieważnienia dostępu z wykorzystaniem zagubionego przedmiotu.

Uwierzytelnianie – „MAM”

- Rodzaje przedmiotów
  - karty z tworzywa sztucznego,
  - tokeny,
  - listy haseł jednorazowych,
  - inne rozwiązania

Uwierzytelnianie – „MAM”

- Identyfikacja na kartach z tworzywa sztucznego
- Standardowa karta, np. bankowa, służąca do kontroli dostępu, identyfikacji, określona normami ISO 7810 i 7811 ma wymiary 53,98 mm x 85,60 mm i grubość 0,76 mm
- z nadrukowanym kodem paskowym (ang. *bare code*),
- magnetyczne,
- stykowe (mikroprocesorowe, pamięciowe)

Uwierzytelnianie – „MAM”

- **Karty z kodem paskowym:**
  - tanie rozwiązanie,
  - karta posiada najczęściej nazwę osoby lub firmy oraz kod kreskowy
  - przykłady: obsługa klientów w sieci MACRO, identyfikacja uczniów w placówkach szkolnych, biblioteka główna PWr

Uwierzytelnianie – „MAM”

- Karty magnetyczne:
  - LOCO (low coercivity) – niska koercja (koercja = natężenie powściągające, mówi o tym, jakie „pole zewnętrzne trzeba przyłożyć, by zlikwidować zapis”), tzw. współczynnik koercji rzędzu 300-400 erstedów (jednostka natężenia pola magnetycznego 1 Oe = ok. 79,5 A/m w układzie SI)
  - MECO (medioum coercivity) – średniej koercji, do 3000 erstedów,
  - HICO (high coercivity) – wysokiej koercji, do 4000 erstedów.

Uwierzytelnianie – „MAM”

- Karty magnetyczne (cd.):
  - zapis w trzech ścieżkach, odpowiednio po 76, 37, 105 znaków alfanumerycznych.
  - Przechowują zazwyczaj:
    - numer konta,
    - imię i nazwisko,
    - hasło,
    - datę ważności.

Uwierzytelnianie – „MAM”

- Karty stykowe
  - pamięciowe
    - od 256 B do ok. 512 kB
    - 100 tyś. cykli zapis/odczyt
    - trwałość zapisu ok. 10 lat
    - budowa: interfejs + EPROM
  - procesorowe

Uwierzytelnianie – „MAM”

- Inne rozwiązania
  - listy haseł jednorazowych
  - identyfikatory zbliżeniowe
  - tokeny

Identyfikatory zbliżeniowe

- Karty zbliżeniowe (komunikacja przez wbudowany interfejs radiowy)
- Identyfikatory zbliżeniowe (np. w pierścionku, torebce, portfelu, breloczku)
- Układy mogą być aktywne (działają do wyczerpania baterii, zasięg np. 2 m) lub pasywne
- NFC (ang. *Near Field Communication*) - komunikacja bliskiego zasięgu

Tokeny

- Funkcja jak lista haseł jednorazowych, np. generuje hasło na podstawie bierzącego czasu
- Użycie wymaga PINu
- Wygląd: jak „kalkulator”; rozebranie niszczy urządzenie

Uwierzytelnienie - metody biometryczne

- Metody oparte o pomiary unikalnych cech fizjologicznych, sposób zachowania itp.
- Każdy ma „identyfikator” od urodzenia i nie trzeba go generować.

Typowe metody biometryczne

- Pomiar geometrii dłoni
- Identyfikacja daktyloskopijna
- Analiza obrazu tęczówki
- Skanowanie siatkówki oka
- Weryfikacja głosu
- Rozpoznawanie podpisu
- Inne

Pomiar geometrii dłoni:

- Pomiar długości, grubości i szerokości palców, powierzchni oraz grubości kostek,
- Autoryzacja polega na porównaniu „opisu” zawartego w bazie danych z danymi pobranymi od osoby,
- Producent urządzenia dostarcza stosowne oprogramowanie,
- Uwaga: dłoń już po kilku sekundach od odcięcia traci swoje właściwości, ale problemy np. z pierścionkami, opuchlizną itp.

Przykład urządzenia

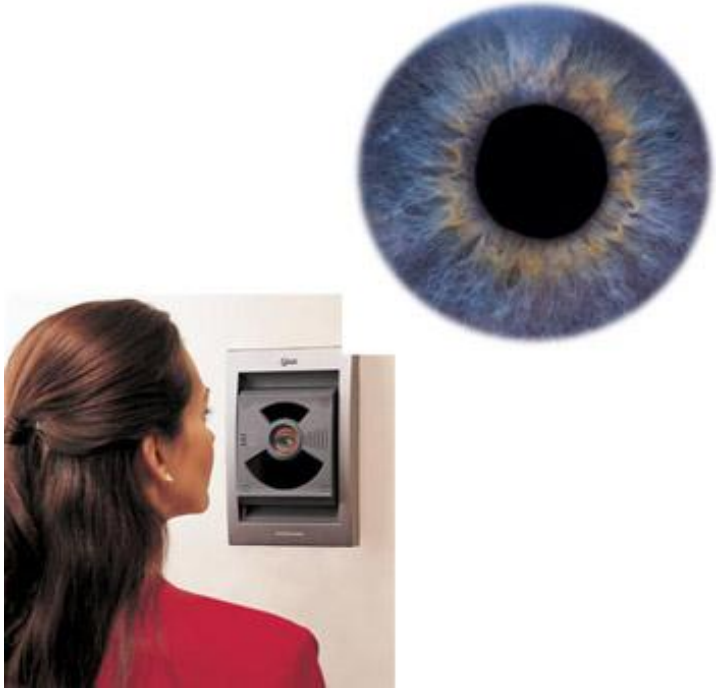
źródło: http://us.allegion.com/Products/biometrics/handkey2/Pages/default.aspx

Analiza obrazu tęczówki

- Kształtowana w ciągu dwóch pierwszych lat życia (cecha fenotypowa – możliwość rozpoznania bliźniaków)
- Niezmienność (naturalna ochrona przed uszkodzeniem)
- Dodatkowe możliwości np. pomiar reakcji na zmianę natężenia światła, pomiar odbicia światła,
- Koszt typowych urządzeń: 1000 $-3000 $
- Zastosowania: uwierzytelnianie w obszarach o wysokim stopniu zabezpieczenia, np. lotniska, obszary przechowujące tajne dokumenty

Przykład urządzenia

- **System:** IrisAccess 2200
- Lotnisko Heathrow
- **Zastosowanie:** odprawa paszportowa



Analiza obrazu siatkówki

- Bazuje na analizie układu naczyń krwionośnych położonych na siatkówce,
- Długi czas pomiaru (nawet kilkadziesiąt sekund)
- Lepsza weryfikacja niż poprzednia metoda, ale wyższy koszt urządzeń
- Zastosowanie: obszary wymagające bardzo wysokiego stopnia zabezpieczenia

Weryfikacja głosu

- Analiza takich parametrów jak: częstotliwość, poziom sygnału, rezonans
- Zalety
  - możliwość wykonania autoryzacji przez telefon,
  - niedrogi koszt urządzenia (np. tylko mikrofony)
- Wada – mała stabilność tego bioparametru

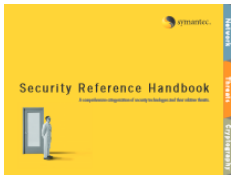
Rozpoznawanie podpisu

- Analiza podpisu i dynamiki jego składana: rytm, szybkość pisania, nacisk długopisu (on-line)
- Zalety: łatwe do zastosowania w Internecie przy zastosowaniu digitalizerów, odporne na kradzieże i zagubienie
- Zastosowania: systemy bankowe
- Przykład: www.cybersign.com

Inne metody biometryczne

- Pomiar dynamiki pisania na klawiaturze
- Pomiar wyściółki pod paznokciem
- Skanowanie twarzy

Literatura dodatkowa



- *Security Reference Handbook*, Symantec Corporation, 2001 (https://www.cccure.org/Documents/Introduction/Security_Reference_Handbook.pdf; Scribd.com).
- ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych, GIODO, 2009 (http://www.giodo.gov.pl/plik/id_p/1560/j/pl/).
- M. Serafin, *Sieci VPN. Zdalna praca i bezpieczeństwo danych*, Helion, 2008.

Pytania?

DZIĘKUJĘ ZA UWAGĘ