Bezpieczeństwo

Bezpieczeństwo musi obejmować zewnętrzne otoczenie systemu i ochronę jego zasobów.
Naruszenia bezpieczeństwa (*security violations*)
Rodzaje:

naruszenie poufności,
naruszenie integralności,
naruszenie dostępności,
kradzież usług,
odmowa świadczenia usług.

Metody:

podszywanie się (naruszenie tożsamości),
atak z odbicia:
zmodyikowanie komunikatu,
atak „człowiek pośrodku”,
przechwycenie sesji.

Bezpieczeństwo musi być zapewnione na czterech poziomach: fizycznym, ludzkim, systemu operacyjnego i sieci.

Zagrożenia programowe (*program threats*)

- Koń trojański - segment kodu nadużywa środowiska, programy jednych użytkowników są wykorzystywane przez drugich
- Boczne drzwi - identyfikator lub hasło pewnego użytkownika do omijania procedur bezpieczeństwa
- Bomba logiczna - program powodujący zaburzenia w pewnych okolicznościach
- Przepełnienie stosu lub bufora - wykorzystanie błędu w programie
- Wirusy - fragment kodu wbudowany w poprawny program, mocno zależą od architektury, zwykle przemycane w poczcie lub w postaci makrodefinicji

Zagrożenia systemowe i sieciowe (*system and network threats*)

- Robaki - stosują mechanizm namnażania i wykorzystują błędy w systemach/programach
- Skanowanie portów - zautomatyzowana próba połączenia do grupy portów adresu IP
- Odmowa świadczenia usług - przeciążenie docelowego serwera uniemożliwiając mu normalną pracę

Bezpieczna komunikacja niezabezpieczonymi łączami (*secure communication over insecure medium*) za pomocą kryptografii.

Szyfrowanie (*encryption*)

- Symetryczne - ten sam klucz służy do szyfrowania i odszyfrowania
- Asymetryczne - klucz publiczny + klucz prywatny (np. RSA)

Uwierzytelnianie (*authentication*)

- Uzupełnia, czasem nadmiarowe względem szyfrowania
- Może dowodzić, że komunikat nie został naruszony
- Funkcja haszująca może służyć do stworzenia streszczenia komunikatu, następnie siecią wysyłany jest (komunikat+streszczenie) a odbiorca sprawdza czy hasz(komunikat) = streszczenie
- Czasem jest potrzebne tylko uwierzytelnienie a nie poufność - np. podpisanie poprawki oprogramowania

Certyfikaty cyfrowe (*digital certificates*)

- Dowodzą tego, kto jest właścicielem klucza publicznego
- Certyfikatem może być klucz publiczny podpisany przez organ zaufany
- Organ zaufany otrzymuje dowód tożsamości od danej jednostki i wydaje świadectwo, że okazany klucz publiczny należy do tej jednostki
- Organ publiczny jest zaufany, a jego klucze publiczne są dołączane do przeglądarek sieciowych.

Zapora sieciowa (*firewall*) - jest umieszczana między komputerem zaufanym, a niezaufanym. Ogranicza dostęp przez sieć między dwoma domenami bezpieczeństwa.