Kryptografia i bezpieczeństwo systemów informatycznych

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2024/2025

inf.ug.edu.pl/~amb/

Sieć komputerowa

Zagrożenia spowodowane zdalnym dostępem

- Nieuprawniony dostęp do systemu
  – zagrożona poufność, integralność, dostęp do danych
- Podsłuchanie / modyfikacja danych w transmisji
  – zagrożona poufność i integralność danych
  – pytanie, czy przeciwnik może zatrzymać przesłane dane
- Zmiana ustawień sieci
  – naruszy dostęp do danych
  – może naruszać integralność i poufność
  – możliwe podszywanie się pod innych uczestników

Historia

- Źródło standardów
  – zastosowania wojskowe
  – troska o przekazanie wiadomości
  – nie rozpatrywano możliwości dostępu przeciwników do sieci
- Brak zabezpieczeń kryptograficznych
  – brak szyfrowania
  – hasła przesyłane jawnie
  – kontrolowane jedynie błędy transmisji ale nie złośliwe modyfikacje

Model warstwowy sieci TCP/IP

1. Warstwa aplikacji:
   - FTP (file transfer protocol),
   - HTTP (hypertext transfer protocol),
   - SSH (secure shell),
   - SMTP (simple mail transfer protocol)
   - SET (secure electronic transactions)
2. Warstwa transportowa
   TCP (transmission control protocol,
   UDP (user datagram protocol))
   – ustawianie pakietów w kolejności, poprawność przesyłu, ew. powtórna transmisja
3. Warstwa internetowa
   IP (internet protocol), ARP, ICMP
   – przesyłanie pakietów, wyznaczanie drogi (routing)
4. Warstwa sieciowa (Ethernet, ATM, FrameRelay)
   – fizyczna transmisja danych, ciąg bitów

Model warstwowy sieci TCP/IP, c.d.

- Dane przesyłane → dane+nagłówki → j.w+kolejne nagłówki → ... → dane odebrane
  – aplikacja przygotowuje dane do przesyłania i przekazuje niższej warstwie
  – przesyłane są przez warstwę fizyczną
  – później proces odwrotny
- Problemy:
  – poufność
  – integralność danych i źródła danych
  – rozliczalność (potwierdzenie odbioru)

Sieć komputerowa – warstwa sieciowa

- *Sniffing* (węszenie)
  – model hub: ramki są wysyłane do wszystkich, odbierane tylko przez adresatów
  – ale atakujący odbiera wszystkie ramki i ma nadzieję na podsłuchanie wiadomości, np. loginów, danych osobowych, nawet haseł, jeśli nie są szyfrowane
  – model switch: ramki są wysyłane tylko do adresatów
  – atakujący stara się aktywnie przełączyć/wyłączyć switch
- *Sniffing* – ochrona
  – wysyłanie fałszywych ramek donikąd i testowanie, czy będą próby zapytania o takie adresy
  – wysyłanie zapytań o nieistniejące adresy MAC i testowanie pozytywnych odpowiedzi
  – pomiar czasu odpowiedzi, atakujący zarzucony dużą liczbą nieistniejących adresów będzie odpowiadał z nieuzasadnionym opóźnieniem

Sieć komputerowa – warstwa Internetu

- Protokół IP
  – zamiana adresu IP na adres MAC: protokół bez zachowania poufności i integralności
  – możliwa jest podmiana adresu
  – dostawca internetu być może sprawdza poprawność
  – atak man-in-the-middle: podmiana adresu obu komunikującym się stronom
- Routing
  – serwer może otrzymać zbyt wiele pakietów do przekierowania
  – skuteczny atak DOS
- Ochrona
  – nieprzyjmowanie nowych adresów MAC
  – statyczna tablica adresów, nie dokonuje się zmian
  – ale zmiany są jednak konieczne, nowe urządzenia itd.
  – sprawdzania integralności nowych adresów – DAI (Dynamic ARP Inspection)

Sieć komputerowa – warstwa Internetu c.d.

- Protokół kontrolny ICMP (Internet Control Message Protocol)
  – ping (packet internet groper) – szukanie po omacku
  – każdy ma prawo wysłać zapytanie
  – i oczekiwać odpowiedzi
- Atak DOS – duża liczba zapytań wyczerpująca zasoby atakowanego serwera
- Obrona
  – nie odpowiadanie na żądania ping z zewnątrz
  – ograniczenie liczby odpowiedzi
- Atak Smurf
  – przesłanie polecenia ping itp. do sieci z prośbą o odpowiedź na atakowany serwer
  – rodzaj ataku DDOS
- Obrona – wyłączenie odpowiedzi

Sieć komputerowa – warstwa aplikacji

- Model klient-serwer
  – serwer działa bez przerwy oczekując na wezwania
  – klient łączy się z serwerem z żądaniem usługi
- Przykłady
  – serwer poczty elektronicznej
  – serwer bazy danych
  – serwer Webowy
- Wstrzykiwanie kodu
  – pod pozorem przesłania danych przesyłany jest złośliwy kod
  – serwer interpretuje kod nieprzewidziany przez twórcę aplikacji
- Atak SQL injection – atak na sewer bazy danych
  – złośliwe zapytanie może mieć niespodziewane skutki
    - ujawnia dane
    - wykonuje nieuprawnione czynności
    - obciąża serwer (atak DOS)

Atak SQL injection

- Przykład PHP
  `$data1=pg_exec("SELECT * FROM lekarz WHERE peselL='$pesel';");`
  parametrem zapytania jest numer pesel, spodziewamy się numeru w rodzaju 12345678910 i będzie wykonane zapytanie
  `SELECT * FROM lekarz WHERE peselL='12345678910';`
- złośliwy użytkownik zapytany o numer pesel być może wstawi wartość
  `'; DELETE FROM lekarz; SELECT '`
  i spowoduje wykonanie zapytania SQL
  `SELECT * FROM lekarz WHERE peselL=''; DELETE FROM lekarz; SELECT '';`
- złośliwy użytkownik może na każdy parametr podawać `' OR '1'='1`
  i obserwować wywołane efekty

Sieć komputerowa – warstwa aplikacji c.d.

- Zewnętrzne linki w dokumentach XML
  – procesor XML wykona zapytania zawarte w takich linkach
- CSRF (cross site request forgery)
  – złośliwy adres http i zachęcenie użytkownika (phishing) by użył takiego adresu (adres może zawierać ukryte polecenia)
- Obrona – staranne przygotowanie aplikacji, przewidywanie zapytań
  – zakaz użycia niektórych znaków, średnik, $, cudzysłów itp., które mogą mieć znaczenie techniczne
  – zamiana podejrzanych znaków na wersje „dosłowne”, np. \' zamiast '

Poczta elektroniczna, problemy

- Brak uwierzytelnienia nadawcy
- Łatwość modyfikacji treści wiadomości
- Brak poufności przekazywanych treści
  brak poufności listy adresatów
- Brak potwierdzenia otrzymania przesyłki
- Poczta niepożądana (spam)
- Niebezpieczne załączniki
- *phishing*: wyłudzanie danych poufnych od użytkowników

Poczta elektroniczna, rozwiązania

- Uwierzytelnianie nadawcy (i integralność)
  – podpis cyfrowy PGP lub S/MIME
- Poufność
  – szyfrowanie PGP, S/MIME, PEM
- Spam, phishing, niebezpieczne załączniki
  – filtrowanie nagłówków podczas transferu
  – dokładniejsza analiza treści podczas dostarczenia emaila adresatowi, samouczące się filtry
  – jw. program pocztowy użytkownika
- Niebezpieczne załączniki
  – programy antywirusowe