Kryptografia i bezpieczeństwo systemów informatycznych

Andrzej M. Borzyszkowski

Instytut Informatyki
Uniwersytet Gdański

sem. letni 2024/2025

inf.ug.edu.pl/~amb/

Podsumowanie

Wykład 1 – Problemy bezpieczeństwa wg PN-I-13335

1. Poufność (tajność)
2. Dostępność – dla uprawnionego użytkownika
3. Autentyczność (uwierzytelnianie) – użytkownik jest naprawdę tym, za kogo się podaje
4. Integralność (spójność) danych i systemu – ani dane ani system nie zostały zmienione w sposób nieuprawniony
5. Rozliczalność – działania użytkownika są jednoznacznie przypisane – Niezaprzeczalność – brak możliwości zaprzeczenia autorstwa dokumentu lub wykonania czynności
6. Niezawodność

Wykład 1 – Kryptografia klasyczna

- Cele stosowania kryptografii
- Założenia dotyczące kryptoanalizy
  - przeciwnik ma tylko tekst zaszyfrowany
  - przeciwnik ma przykłady tekstów jawnych plus ich zaszyfrowane wersje
  - przeciwnik ma prawo żądać zaszyfrowania lub odszyfrowania wiadomości
- Zasada Kerckhoffsa
- Szyfry klasycznej kryptografii: Cezara i Vigenere'a, Enigma
- Problemy:
  – Czy mała przestrzeń kluczy może zapewnić bezpieczeństwo szyfru?
  – Czy duża przestrzeń kluczy jest gwarancją bezpieczeństwa

Wykład 2

- Zasady nowoczesnej kryptografii (dyskusja definicji wymagań bezpieczeństwa)
- Szyfr doskonale bezpieczny, czy taki szyfr istnieje? dlaczego stosujemy szyfry, które nie są doskonale bezpieczne?
- Generatory liczb pseudolosowych, które z nich nie mogą być stosowane w kryptografii?
- Szyfr strumieniowy, definicja, własności, tryby synchroniczny i asynchroniczny szyfru strumieniowego
- Przykłady szyfrów niedeterministycznych
- Niedeterminizm jest konieczny, by szyfr był odporny na atak z wielokrotnym szyfrowaniem, z wybranym tekstem jawnym

Wykład 3 – Tryby szyfrów blokowych

- Tryby pracy szyfrów blokowych, wady i zalety różnych trybów
  - ECB: electronic codebook
  - CBC: cipher block chainig
  - OFB: output feedback
  - CFB: cipher feedback
  - CTR: counter
- Elementy składowe algorytmu DES
  – konfuzja i dyfuzja (podstawienia i „permutacje")
- Czy DES jest dzisiaj bezpieczny?
  – czy i w jaki sposób dwukrotne szyfrowanie DES zwiększa bezpieczeństwo szyfru?
  – jak działa i jakie bezpieczeństwo zapewnia 3DES? DESX?
- AES

Wykład 4 – Integralność danych

- Pojęcie integralności, definicja ataku
  – czy i w jakim zakresie odporne są na atak znane szyfry
- Różnice pomiędzy szyfrem blokowym w trybie CBC a kodem uwierzytelniającym (MAC) w tym samym trybie
- Zasada „szyfruj, potem uwierzytelniaj"
- Zastosowania funkcji skrótu we współczesnej kryptografii (integralność, przechowywanie haseł, podpis cyfrowy, zobowiązanie bitowe, dowód pracy, generowanie kluczy)
- Pożądane własności funkcja skrótu dla celów kryptografii
  – nieodwracalność, trudność 1. przeciwobrazu
  – słaba bezkolizyjność, trudność 2. przeciwobrazu
  – silna bezkolizyjność
  – nieprzewidywalność
- Atak urodzinowy, konsekwencje istnienia tego ataku

Wykład 4 – Kryptografia klucza publicznego

- Nowe możliwości kryptografii klucza asymetrycznego
  – komunikacja bez wstępnego przekazania klucza
  – możliwość uzgodnienia klucza tajnego publicznym kanałem komunikacji
  – podpis cyfrowy
- Ograniczenia kryptografii klucza asymetrycznego
  – wydajność
  – atak z wybranym tekstem jawnym (konieczny niedeterminizm)
  – doskonałe bezpieczeństwo (nie ma)
- Uwierzytelnianie klucza publicznego
  – atak przez pośrednika (*man-in-the-middle*)
  – fałszerstwo podpisu
- Szyfr hybrydowy: wymiana klucza sesyjnego
- Podpis: skrótu wiadomości

Wykład 5 – Teoria liczb, implementacja idei klucza publicznego

- Teoria liczb
- Operacje arytmetyczne łatwe i trudne w arytmetyce modularnej dla liczb kilkusetbitowych
  – algorytm Euklidesa, odwrotności modularne, szybkie potęgowanie
  – złożoność: wielomian stopnia dwa/trzy, czyli wykonalne ale dla tysięcy bitów, nie milionów
- Główne schematy kryptografii klucza asymetrycznego
  – RSA (problem rozkładu na czynniki, funkcja Eulera)
  – problem Diffie'go-Hellmana (grupy cykliczne i generatory, problem logarytmu dyskretnego)
  – szyfr ElGamala
- Teoria liczb – znajomość faktoryzacji liczby, znajomość funkcji Eulera, znajomość nietrywialnego pierwiastka z 1
  – testy Fermata i Rabina-Millera (świadkowie pierwszości)

Wykład 6 – Podpis cyfrowy, Infrastruktura klucza publicznego

- Cechy wymagane od podpisu cyfrowego
  – podpis cyfrowy a MAC
- Podpis cyfrowy w kryptografii klucza publicznego
  – schematy podpisu RSA i ElGamala, różnice
  – podpis skrótu jako zasada
  – konsekwencje ataku na funkcję skrótu
  – standard DSA
- Infrastruktura klucza publicznego – certyfikat standard X.509
- Zadania zaufanego centrum certyfikacji,
  – wystawianie certyfikatów
  – unieważnianie certyfikatów
  – znakowanie czasem
  – opcjonalnie: przechowywanie, odtwarzanie i aktualizowanie kluczy
- Modele zaufania, różnice pomiędzy infrastrukturą klucza publicznego a modelem zaufania PGP

Wykład 7 – Podpis i skróty, technologia blockchain

- Podpis jednorazowy i jego bezpieczeństwo
  – schemat Lamporta
  – schemat Winternitza
  – schemat Merkle'a
- Technologia blockchain
  – dowód pracy
  – stosowany również w przeciwdziałaniu atokom DOS (odmowy obsługi) i wysyłaniu poczty niechcianej (*spam*)
  – dlaczego w praktyce nie ma rozgałęzień
- Inne kryptowaluty

Wykład 8 – Uwierzytelnianie, klucze i hasła

- Klucze: długość, jakość, dystrybucja
  – klucze sesyjne i klucze długoterminowe
- Uwierzytelnianie: jedno/dwukierunkowe, za pośrednictwem zaufanej strony trzeciej , single sign-on, hasło–odzew, hasła jednorazowe
- Metody:
  – wiedza
  – posiadanie fizycznego przedmiotu
  – cechy indywidualne i niepowtarzalne
- Hasła: ataki
  – atak słownikowy, metody przeciwdziałania
  – przechowywanie haseł, skróty, z solą, z dowodem pracy

Wykład 8 – Steganografia i znaki wodne

- Steganografia: dodanie obcej treści do dzieła
- Znaki wodne: dodanie treści komplementarnej do dzieła
- Zastosowania
  – dowód autorstwa/bycia właścicielem praw
  – kontrola kopiowania (uniemożliwienie, nadzorowanie)
  – nowe standardy
- Własności
  – efektywność
  – wierność
  – nośność
  – odporność

Wykład 9 – Protokoły kryptograficzne

- Ataki
  – atak man-in-the-middle (pośrednik), przeciwdziałanie: uwierzytelnianie
  – atak przez powtórzenie, przeciwdziałanie: liczby jednorazowe, znaczniki czasu
  – atak DOS (*denial of service*), przeciwdziałanie: dowód pracy dla atakującego, minimalizacja wymagań dla atakowanego
- Kerberos, system scentralizowany, kryptografia symetryczna
- SSL, uwierzytelnianie uczestników, rola zaufanego centrum
- SET (*secure electronic transactions*)

Wykład 9 – Bezpieczeństwo sieci komputerowych

- Zagrożenia spowodowane zdalnym dostępem
- Model warstwowy sieci TCP/IP
- Poczta elektroniczna, problemy i rozwiązania
  - Uwierzytelnienie nadawcy – podpis cyfrowy PGP lub S/MIME
  - Łatwość modyfikacji treści wiadomości – j.w.
  - Brak poufności przekazywanych treści – szyfrowanie PGP lub S/MIME
  - Poczta niepożądana (spam) –
    – filtrowanie nagłówków podczas transferu
    – analiza treści przed dostarczeniem emaila, samouczące się filtry
    – dowód pracy
  - *phishing*: wyłudzanie danych poufnych od użytkowników – j.w.
  - Niebezpieczne załączniki – programy antywirusowe
  - Brak potwierdzenia otrzymania przesyłki – ??