PA159 – Bezpečnostní aspekty

19. 10. 2007

Formulace oblasti

- Kryptografie (v moderním slova smyslu) se snaží minimalizovat škodu, kterou může způsobit nečestný účastník
- Oblast bezpečnosti počítačových sítí řeší v podstatě identický problém

Bezpečnost

1. AAA
   - Autentizace
   - Autorizace
   - Accounting („účetnictví“)
2. Zabezpečená komunikace

Podpora na úrovni sítě

Autentizace

- Identifikace: *Já jsem já*
- Varianty
  - Sdílené tajemství: hesla
  - Důvěryhodná třetí strana: Kerberos
  - Asymetrické funkce: X.509 certifikát, Infrastruktura veřejných klíčů
- Delegování:
  - proxy certifikáty
- Federativní přístupy

Autorizace

- Oprávnění použít určitou službu nebo zdroj
- Následuje autentizaci
- „Přístupová práva“: ACL (Access Control List)
- Anonymní autorizace

Accounting

- Účtování: kdo, co, kdy a v jakém rozsahu použil
- Vyžaduje autentizaci
- Využití
  - Skutečné finanční účtování za využití zdrojů
  - Kontrola
    - Autorizace: záznam neoprávněného využití
    - Férovosti využití
  - Predikce

Zabezpečená komunikace

- Klasický problém *kryptografie*
  - Bezpečná komunikace po nezabezpečených komunikačních kanálech
- Požadované vlastnosti:
  - Utajení: jen odesílatel a příjemce rozumí zprávě
  - Autentizace
  - Integrita: zpráva nebyla pozměněna
  - Non-repudiabilita: příjemce ani odesílatel nemohou popřít, že zprávu přijali/odeslali

Nové problémy

- Anonymita
  - Nemožnost spojit konkrétní osobu a činnost
- Nesledovatelnost
  - Nemožnost spojit různé akce jedné osoby/entity

Míra bezpečnosti

- Informačně-teoretický přístup
  - Míra informace z původního textu přítomná v textu zašifrovaném
  - Optimální při klíči stejně dlouhém nebo delším než vlastní text
- Výpočetně/složitostní přístup
  - *cena* rozluštění
  - *proveditelnost* vs. *možnost rozluštění*
  - je *efektivní* získat původní text bez znalosti klíče?

Symetrická kryptografie

- Stejný klíč pro šifrování i rozluštění
- Základní princip: substituce
- Podstatná složitost, tj. teoretický počet možných kombinací
- Klasika: monoalfabetické a polyalfabetické systémy
- Problém: distribuce klíčů

Asymetrická kryptografie

- Různé klíče pro šifrování a rozluštění
- Veřejný a soukromý klíč
  - částečné řešení problému distribuce klíčů (samo o sobě nestačí)
  - použitelné pro šifrování i rozluštění
  - $(m^e)^d \bmod n = m = (m^d)^e \bmod n$

Digitální podpis

- Součást kryptografie až v „digitálním“ věku
- Nepodvržitelný podpis
  - Každý se musí dokázat podepsat
  - Každý může snadno ověřit podpis druhého
  - Nikdo nemůže snadno druhého podepsat
- Řeší problém autentizace zpráv (ale není řešením problému autentizace)

Zdroje informací o šifrovacích algoritmech

- RFC, např. http://zvon.org
- FIPS publikace (Federal Information Processing Standards Publications), http://csrc.nist.gov/encryption
- Přednášky z kryptografie (prof. Gruska)
- Standardní publikace (články, příspěvky, knihy)

Symetrická kryptografie – základní algoritmy

- DES, Data Encryption Standard (FIPS Pub 46-3)
- 3DES, Triple DES (FIPS Pub 46-3)
- AES, Advanced Encryption Standard aka Rijndael (FIPS Pub 197)

DES

- Bloky dat délky 64 bitů s pomocí klíče délky 64 bitů
  - Reálně klíč pouze 56 bitů, 8 bitů jsou paritní bity (lichá parita)
- Symetrický
- Algoritmus
  - Vstupní permutace IP
  - Vlastní šifrování
  - Výstupní permutace IP^{-1}

DES II

- Šifrování:
  - 16 identických průchodů
  - 32 „pravých“ bitů je posunuto doleva
  - Samostatné klíče (48 bitů) pro každý průchod (odvozeny z původního klíče)
  - Všech 64 bitů transformováno (expanze, XOR, substituce, XOR) na 32 bitů, ty se stanou pravými bity výsledku

Bezpečnost DES

- Není jednoznačně definována
- Je možno ji prorazit (cena pod $ 250 000)
- „Vylepšení“: 3DES

Tripple DES (3DES)

- Postupná aplikace DES se třemi klíči
  - K1=K2=K3, ekvivalentní DES
  - K1=K3$\neq$K2
  - K1$\neq$K2$\neq$K3
- Šifrování
  - I $\longrightarrow$ DES K1 $\longrightarrow$ DES K2 $\longrightarrow$ DES K3 $\longrightarrow$ C
- Rozluštění
  - C $\longrightarrow$ DES K3 $\longrightarrow$ DES K2 $\longrightarrow$ DES K1 $\longrightarrow$ I

AES

- Rovněž blokový algoritmus
- Klíče délky 128, 192 a 256 bitů
- Blok standardně délky 128 bitů (varianty pro 192 a 256 bitů)
- 9, 11 nebo 13 průchodů (podle délky klíče/bloku)
- Pracuje po bytech (8 bitů)
- Vysoce efektivní hw implementace
- Princip viz animace

Message digest – Hashovací funkce

- Problém integrity zprávy
- Řešení: použití hash funkce (analogie kontrolního součtu)
- Hash: Řetězec pevné délky vygenerovaný ze zprávy proměnné délky, pro nějž platí:
  - hash(Řetězec_1) $\neq$ hash(Řetězec_2) $\Leftrightarrow$ Řetězec_1 $\neq$ Řetězec_2
  - Jednosměrné: ze znalosti hashe neodvodím (snadno) původní text
- MD5 Message Digest (RFC 1321): 128 bitů
- SHA1 FIPS Pub 180-1: 160 bitů

Digitální podpis – algoritmy

- RSA (RFC 2437)
- DSA, požadováno použití SHA1 (FIPS Pub 186)

RSA – typy klíčů

- Veřejný klíč:
  - n, modulus, nezáporné celé číslo
  - e, veřejný exponent, nezáporné celé číslo
- $n = p \times q$, p a q jsou prvočísla
- $2 < e < n, \gcd(e, (p-1) \times (q-1)) = 1$

RSA – soukromý klíč 1

- n, modulus, nezáporné celé číslo
- d, soukromý exponent, nezáporné celé číslo
- Vztahy
  - $n = p \times q$
  - $e \times d = 1 \bmod ((p-1) \times (q-1))$

RSA – soukromý klíč 2

- p, q, první a druhý faktor, nezáporná celá čísla
- dP, exponent p, nezáporné celé číslo
- dQ, exponent q, nezáporné celé číslo
- `qInv`, CRT koeficient, nezáporné celé číslo
  - $e \times dP = 1 \bmod (p - 1)$
  - $e \times dQ = 1 \bmod (q - 1)$
  - $q \times \texttt{qInv} = 1 \bmod p, 0 < \texttt{qInv} < p$

RSA – šifrování

- RSAEP((n, e), m)
  - (n, e): RSA veřejný klíč
  - m: zpráva, celé číslo mezi $(0, n - 1)$
  - C: výsledek, zašifrované m nebo zpráva „Message representative out of range“
- C = $m^e \bmod n$

RSA – rozluštění

- RSADP(K,C)
  - K: soukromý klíč (v jedné nebo druhé variantě)
  - C: zašifrovaný text
  - m: výsledek, rozluštěná zpráva; případně text „Ciphertext representative out of range“, pokud C není číslo v intervalu $(0, n-1)$
- 1. varianta klíče: $m = c^d \bmod n$

RSA – rozluštění, 2. varianta klíče

- $m_1 = c^{dP} \bmod p$
- $m_2 = c^{dQ} \bmod q$
- $h = \mathtt{qInv} \times (m_1 - m_2) \bmod p$
- $m = m_2 + h \times q$

RSA – ověření podpisu

- RSAVP1((n, e), s)
  - (n, e): veřejný klíč
  - s: podpis, číslo z intervalu $(0, n - 1)$
  - m: zpráva, číslo z intervalu $(0, n - 1)$
- Pokud s není z intervalu $(0, n - 1)$, vypiš „invalid“ a skonči
- $m = s^e \bmod n$
- Podpis zpravidla MD5 nebo SHA1 hash