

Kryptológia – úvod

Martin Stanek

Katedra informatiky
FMFI UK, Bratislava
stanek@dcs.fmph.uniba.sk

Úvod do informačnej bezpečnosti (LS 2011/2012)

Obsah

Úvod

Základné kryptografické prvky

Dĺžky kľúčov

Protokoly

Kryptológia v kontexte

Úvod

- ▶ Náhodnosť kryptografických kľúčov (napr. Debian)
- ▶ Timing útoky na porovnávanie
- ▶ PKCS #11 a kryptografické tokeny
- ▶ WPS (WiFi Protected Setup)
- ▶ Šifrované USB kľúče (certifikované FIPS 140-2)
- ▶ Kolízie v hašovacích tabuľkách
- ▶ Heslá alebo komunikácia v otvorenom tvare
- ▶ ...

Úvod – kryptológia

- ▶ kryptológia – dôležitá súčasť informačnej bezpečnosti
- ▶ informačná bezpečnosť \setminus kryptológia = ???
- ▶ kryptológia = kryptografia + kryptoanalýza
- ▶ kryptografia slúži na zabezpečenie:
 - ▶ dôvernosti – šifrovanie
 - ▶ integrity a autentickosti – autentizačné kódy, podpisy
- ▶ ďalšie objekty záujmu: protokoly, zdieľanie tajomstva, ...

Kryptológia

- ▶ kryptológia
 - ▶ matematika
 - ▶ detaily sú podstatné
 - ▶ implementácia a použitie
- ▶ poskytuje (falošný ?) pocit bezpečia
 - ▶ „šifrujeme“ – ako? mód? správa kľúčov? kontext? ...
 - ▶ „podpisujeme“ – ako? implementácia? správa kľúčov? ...

Symetrické šifrovanie – úvod 1

- ▶ klasický cieľ kryptografie – dôverný prenos dát
- ▶ komunikujúce subjekty zdieľajú **tajný kľúč**
- ▶ kľúč je rovnaký pre odosielateľa aj príjemcu \Rightarrow symetrické šifrovanie
- ▶ otvorený text = pôvodná správa, text, dokument, dáta
- ▶ šifrový text = zašifrovaný text, výstupné dáta šifrovacieho algoritmu

Symetrické šifrovanie – úvod 2

▶ šifrovanie: $E : P \times K \rightarrow C$

▶ dešifrovanie: $D : C \times K \rightarrow P$

▶ korektnosť:

$$\forall k \in K \forall p \in P : D_k(E_k(p)) = p$$

▶ Kerckhoffov princíp:

bezpečnosť šifrovania nezávisí na utajení algoritmu, ale výlučne na utajení kľúča

Vernamova šifra (one-time pad)

- ▶ správa $m = m_1, m_2, \dots, m_t \in \{0, 1\}^t$
- ▶ kľúč $k = k_1, k_2, \dots, k_t \in \{0, 1\}^t$
- ▶ šifrovanie: $c = m \oplus k$ ($c_i = m_i \oplus k_i$)
- ▶ dešifrovanie: $c \oplus k = (m \oplus k) \oplus k = m$
- ▶ výhody:
 - ▶ jednoduché (rýchle) šifrovanie a dešifrovanie
 - ▶ absolútne bezpečná šifra
- ▶ nevýhody:
 - ▶ kľúč rovnako dlhý ako otvorený text
 - ▶ „jednorazový“ kľúč

Prúdové šifry

- ▶ krátky kľúč použitý na (deterministické) generovanie **bežiaceho** kľúča
- ▶ zväčša používané – (aditívne) synchrónne prúdové šifry
- ▶ najznámejšie prúdové šifry: RC4 (softvér), A5 (GSM), E0 (Bluetooth)
- ▶ zvyčajné výhody (oproti blokovým šifram):
 - ▶ vhodné pre prúd OT, jednoduchší algoritmus, rýchlejšie šifrovanie/dešifrovanie
- ▶ zvyčajné nevýhody:
 - ▶ vyžadujú synchronizáciu, bez akejkoľvek integrity, zložitý „seek“

Blokové šifry

- ▶ šifrovanie/dešifrovanie blokov dát: $E_k, D_k : \{0, 1\}^n \rightarrow \{0, 1\}^n$
- ▶ E_k a D_k sú inverzné bijekcie
- ▶ **mód** – spôsob šifrovanie dlhých OT, napr.
 - ▶ ECB (Electronic Code Book)
 - ▶ CBC (Cipher Block Chaining)
 - ▶ CTR (Counter)
- ▶ najpoužívanejšie blokové šifry: AES, (3)DES

Typy útokov na šifrovacie algoritmy

- ▶ základné útoky:
 - ▶ (COA) len so znalosťou šifrovaného textu
 - ▶ (KPA) so znalosťou otvoreného textu
 - ▶ (CPA) s možnosťou voľby otvoreného textu
 - ▶ (CCA) s možnosťou voľby šifrovaného textu
- ▶ ciele útokov: získať kľúč, dešifrovať neznámy ŠT, zašifrovať nový OT,
...

Štandardy (blokové šifry)

- ▶ AES (Advanced Encryption Standard)
 - ▶ algoritmus Rijndael
 - ▶ verejný výber štandardu (NIST, 1997-2001)
 - ▶ štandard: FIPS PUB 197, 2001
 - ▶ bloková šifra, 128 bitov dlhý blok
 - ▶ variabilná dĺžka kľúča: 128, 192, 256 bitov
- ▶ DES/3DES
 - ▶ predchádzajúci štandard, 70-te roky 20. storočia
 - ▶ bloková šifra, 64 bitov dlhý blok (**málo!**)
 - ▶ DES: dĺžka kľúča 56 bitov (**málo!**)
 - ▶ 3DES: dĺžka kľúča 168 (resp. 112) bitov

Výkon – softvérové implementácie

- ▶ knižnica Crypto++ v.5.6.0, (Windows Vista)
- ▶ hardvér: Intel Core 2, 1.83 GHz

alg.	MB/s
AES-128	109
AES-192	92
AES-256	82
3DES	13

- ▶ špecializovaný HW: AES-128 \sim 21 Gbit/s

Asymetrické šifrovanie

- ▶ dvojica rôznych kľúčov:
 - ▶ **verejný** – šifrovanie \Rightarrow ktokoľvek vie šifrovať
 - ▶ **súkromný** – dešifrovanie \Rightarrow len vlastník vie dešifrovať
- ▶ jednoduchšia správa kľúčov
- ▶ bezpečnosť:
 - ▶ CPA útok je vždy možný
 - ▶ verejný kľúč \nrightarrow algoritmus na dešifrovanie
- ▶ najznámejšie systémy: RSA, ElGamal

RSA

- ▶ (1978) Rivest, Shamir, Adleman
- ▶ bezpečnosť súvisí s problémom faktorizácie veľkých čísel
- ▶ konštrukcia:
 - ▶ $n = p \cdot q$, p, q sú veľké prvočísla
 - ▶ $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$
 - ▶ verejný kľúč: (e, n)
 - ▶ súkromný kľúč: d
- ▶ šifrovanie ($E : Z_n \rightarrow Z_n$): $E(m) = m^e \pmod n$
- ▶ dešifrovanie ($D : Z_n \rightarrow Z_n$): $D(c) = c^d \pmod n$
- ▶ RSA je bijekcia
- ▶ RSA je deterministické (**fuj!**) \Rightarrow v praxi sa znáhodňuje

RSA – štandardy

- ▶ RSA PKCS #1 v1.5 (žiadny dôkaz bezpečnosti)
 - ▶ veľmi rozšírené a v praxi používané
- ▶ RSA PKCS #1 v2.1 – RSA-OAEP
 - ▶ znáhodnený padding (zarovnanie)
 - ▶ „dôkaz“ bezpečnosti (v modeli s náhodným orákulom)

Výkon – softvérové implementácie

- ▶ knižnica Crypto++ v.5.6.0, (Windows Vista)
- ▶ hardvér: Intel Core 2, 1.83 GHz

alg.	ms/oper.
RSA-1024 šifr.	0.08
RSA-1024 dešifr.	1.46
RSA-2048 šifr.	0.16
RSA-2048 dešifr.	6.08

Hybridné šifrovanie

- ▶ asymetrické šifry sú pomalé (v porovnaní so symetrickými)
- ▶ čo s prenosom objemných dát?
- ▶ riešenie:
 - ▶ šifrujme symetricky s náhodným kľúčom k
 - ▶ kľúč k zašifrujeme asymetricky pre adresáta
$$\langle AES_k(m), E_A^{RSA}(k) \rangle$$
- ▶ v praxi špeciálne schémy (KEM – Key Encapsulation Method), napr. RSA-KEM (ISO/IEC 18033-2)

Hašovacie funkcie

- ▶ funkcia $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$
- ▶ „odtlačok“ správy, dokumentu
- ▶ kontrola integrity, digitálne podpisy
- ▶ kryptografické vlastnosti:
 - ▶ **jednosmernosť**: pre dané y nájsť x : $h(x) = y$
 - ▶ **odolnosť voči kolízám**: nájsť $x \neq x'$: $h(x) = h(x')$
- ▶ najznámejšie hašovacie funkcie: MD5, SHA1, SHA-(224,256,384,512)

Bezpečnosť hašovacích funkcií

- ▶ nedávne výsledky:
 - ▶ nájdené kolízie v MD5 (2005)
 - ▶ kolízie v certifikátoch s MD5 (!)
 - ▶ kolízie $\sim 2^{24}$ (2007)
 - ▶ SHA-1 (160 bitov) kolízie $\sim 2^{57}$ (2010)
- ▶ generický útok – **narodeninový útok**
 - ▶ hľadanie kolízií
 - ▶ využíva tzv. „narodeninový“ paradox
 - ▶ zložitosť útoku $O(2^{n/2})$

Výkon – softvérové implementácie

- ▶ knižnica Crypto++ v.5.6.0, (Windows Vista)
- ▶ hardvér: Intel Core 2, 1.83 GHz

alg.	MB/s
MD5	255
SHA-1	153
SHA-256	111
SHA-512	99
Whirlpool	57

Budúcnosť

- ▶ verejný výber novej sady algoritmov (SHA-3)
- ▶ organizuje NIST (štandard očakávaný v 2012)
- ▶ finalisti: BLAKE, Grøstl, JH, Keccak, Skein
- ▶ detaily: csrc.nist.gov/groups/ST/hash/sha-3/index.html

Autentizačné kódy správ (MAC)

- ▶ hašovacie funkcie s kľúčom (symetrické)
- ▶ zabezpečenie autenticity správ (bez nepopierateľnosti !)
- ▶ rýchle (oproti digitálnym podpisom)
- ▶ použitie napr. SSL/TLS, IPsec
- ▶ najznámejšia konštrukcia: HMAC (RFC 2104)

$$\text{MAC}_k(m) = H(k \oplus \text{opad} \parallel H(k \oplus \text{ipad} \parallel x)),$$

- ▶ pre HMAC-MD5/SHA1 je $\text{opad} = (0x5C)^{64}$, $\text{ipad} = (0x36)^{64}$

Digitálne podpisy

- ▶ autentickosť, integrita, nepopierateľnosť pôvodu . . .
- ▶ ekvivalent „vlastnoručného“ podpisu v elektronickom prostredí
- ▶ asymetrická schéma:
 - ▶ **súkromný kľúč** – podpisovanie \Rightarrow len vlastník vie podpísať
 - ▶ **verejný kľúč** – overovanie \Rightarrow ktokoľvek vie overiť
- ▶ podpis musí závisieť na podpísovanom dokumente/správe
- ▶ podpisuje sa odtlačok dokumentu ($H(m)$):
 - ▶ výkonové dôvody
 - ▶ bezpečnostné dôvody (falšovanie náhodnej správy)

RSA podpisy

- ▶ „prehodíme“ transformácie z klasického RSA:
 - ▶ podpisovanie: $s = H(m)^d \bmod n$
 - ▶ overovanie podpisu: platí $s^e \bmod n = H(m)$?
- ▶ (**len tu!**) bijektivnosť je zriedkavá vlastnosť asym. systémov
- ▶ v štandardoch zvyčajne so znáhodneným zarovnaním, napr. RSA-PSS (Probabilistic Signature Scheme) v RFC 3447, resp. v PKCS #1 v2.1
 - ▶ PKCS #1 v1.5 stále široko používané

DSA

- ▶ DSA – Digital Signature Algorithm
- ▶ súčasť štandardu DSS (aktuálne FIPS 186-3)
- ▶ bezpečnosť súvisí s problémom diskretného logaritmu
- ▶ parametre:
 - ▶ p, q – prvočísla, $q \mid (p - 1)$
(kde bitové dĺžky prvočísel sú (1024, 160), (2048, 224), (2048, 256) a (3072, 256))
 - ▶ g – vypočítame $g = h^{(p-1)/q} \bmod p > 1$, kde $h \in_R \{2, 3, \dots, p - 2\}$
 - ▶ súkromný (podpisový) kľúč: $x \in_R \mathbb{Z}_q^*$
 - ▶ verejný (overovací) kľúč: $y = g^x \bmod p$ a parametre p, q, g

DSA (pokračovanie)

► podpisovanie:

1. $k \in_R \{1, \dots, q - 1\}$
2. $r = (g^k \bmod p) \bmod q$
3. $s = k^{-1}(H(m) + xr) \bmod q$

► overovanie:

1. $u_1 = H(m) \cdot s^{-1} \bmod q$
2. $u_2 = r \cdot s^{-1} \bmod q$
3. platí $(g^{u_1} \cdot y^{u_2} \bmod p) \bmod q = r$?

PKCS

- ▶ Public-Key Cryptography Standards
- ▶ implementačné štandardy, napr.:

PKCS #1: RSA Cryptography Standard

PKCS #5: Password-Based Cryptography Standard

PKCS #7: Cryptographic Message Syntax Standard

PKCS #10: Certification Request Syntax Standard

PKCS #11: Cryptographic Token Interface Standard

PKCS #12: Personal Information Exchange Syntax Standard

Bezpečnosť – dĺžka klúča

- ▶ generický útok – úplné preberanie množiny K
- ▶ dostatočná veľkosť $|K|$ (dĺžka klúča)
 - ▶ **nutná**, ale
 - ▶ **nie postačujúca** podmienka bezpečnosti
- ▶ aká dĺžka klúča je dostatočná?
 - ▶ *Deep Crack – DES, \$200k, 1 klúč ~ 22 hodín, 1998*
... (2007) 1 DES klúč ~ 3 dni, \$12 000
 - ▶ *odhady: 80 bitový klúč ~ 1 rok, \$8M, 2006*
 - ▶ *odhady: 80 bitový klúč ~ 1 mesiac, \$33M, 2010*

 - ▶ ako dlho má šifra (ŠT) odolať („cena“ dát)?
 - ▶ aký progres v kryptoanalýze predpokladáme?
 - ▶ aký bude progres v technológii (Mooreov zákon)?
 - ▶ aký silný (ekonomicky) je/bude útočník?

Bezpečnosť – dĺžka kľúča 2

- ▶ rôzne doporučenia, rôzne metodiky výpočtu
- ▶ NSA Suite B Cryptography (2010)
- ▶ ECRYPT Report (2011)
- ▶ NIST Recommendations (2011)
- ▶ ... a ďalšie (www.keylength.com)

NSA Suite B Cryptography (2010)

- ▶ pre komerčne dodávané systémy
- ▶ Suite A – neverejné algoritmy, neznáme dĺžky kľúčov
- ▶ algoritmy:
 - ▶ šifrovanie: AES (FIPS 197) v GCM móde
 - ▶ podpisy: ECDSA (FIPS 186-3)
 - ▶ hašovanie: SHA-2 (FIPS 180-3)
 - ▶ výmena kľúčov: ECDH

	sym. šifr.	EC ($GF(p)$)	hašovanie
Secret	128/256	256	256
Top Secret	256	384	384

ECRYPT II Report (2011)

- ▶ ECRYPT – európska sieť excelencie v kryptológii
- ▶ rôzne aktivity
- ▶ pravidelný report o doporučených dĺžkach kľúčov
- ▶ level 1-8
 - ▶ level 4 – najmenšia všeobecná ochrana (do 2014)
„veľmi krátkodobá ochrana voči agentúram“
 - ▶ level 7 – dlhodobá ochrana (cca. 30 rokov)
 - ▶ level 8 – „prevídateľná budúcnosť“

	sym. šifr.	RSA	EC	hašovanie
level 4	80	1 248	160	160
level 7	128	3 248	256	256
level 8	256	15 424	512	512

Protokoly

- ▶ rôzne typy protokolov (účel):
 - ▶ výmena (distribúcia/dohoda) kľúča
 - ▶ autentizácia subjektu
 - ▶ slepé podpisy, voľby, peniaze, . . .
- ▶ bezpečnosť závisí na schopnosti útočníka:
 - ▶ odpočúvať / modifikovať ľubovoľné správy
 - ▶ legítimny subjekt prostredia / mimo
- ▶ (zvyčajne) chceme protokol odolný voči najsilnejšiemu útočníkovi

Diffieho-Hellmanov protokol

- ▶ protokol na dohodnutie kľúča
- ▶ súvisí s problémom diskretného logaritmu (DH problém)

$$A \rightarrow B : X = g^x$$

$$B \rightarrow A : Y = g^y$$

$$\text{výsledný kľúč: } K = X^y = Y^x = g^{xy}$$

- ▶ man-in-the-middle útok (len pre aktívneho útočníka)
- ▶ schopnosť overiť autentickosť dát (napr. dig. podpismi) znemožní MIM útok

SSL/TLS 1

- ▶ SSL – Secure Socket Layer (pôvodne Netscape)
- ▶ TLS – Transport Layer Security (TLS 1.0 ~ SSL v3.1)
- ▶ protokol nad TCP/IP, zabezpečuje integritu a dôvernosť
- ▶ v podstate ľubovoľný protokol nad SSL (FTP, SMTP)
- ▶ najčastejšie: HTTP/SSL (https)

SSL/TLS 2

- ▶ SSL protokoly:
 - ▶ Record Protocol – spodná vrstva (šifrovanie, MAC, kompresia¹)
 - ▶ Handshake Protocol – autentizácia (jednostranná – server, alebo vzájomná – aj klient) dohoda o kryptografických algoritmoch, dohoda o šifrovacom kľúči a MAC kľúči
 - ▶ Alert Protocol – oznamovanie chybových hlášok (napr. `certificate_expired`)
 - ▶ Change Cipher Spec Protocol – „prepnutie“ algoritmov
- ▶ kryptografia v SSL, napr.:

_KeyExchange_WITH_Cipher_MAC
SSL_DHE_DSS_WITH_DES_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

¹ktorú nikto nepoužíva

IPSec

- ▶ bezpečnostný „doplnok“ k IP vrstve
- ▶ oblasti pôsobnosti: dôvernosť, autentickosť, správa kľúčov
- ▶ výhody „nízkoúrovňového“ protokolu:
 - ▶ zabezpečená **celá** komunikácia nad IP
 - ▶ transparentné pre aplikácie
 - ▶ možnosť vytvoriť VPN
 - ▶ integrácia do sieťových zariadení (smerovače a pod.)
- ▶ nevýhody:
 - ▶ SW implementácia (v operačnom systéme) zatažuje server
 - ▶ identita zariadenia, nie používateľa/aplikácie

IPSec (2)

- ▶ základné protokoly – AH, ESP
- ▶ AH (Authentication Header) – len autentickosť/integrita
- ▶ ESP (Encapsulating Security Payload) – šifrovanie a voliteľne autentickosť/integrita
- ▶ transportný mód (spracúvajú sa vybrané časti IP paketu) a tunelovací mód (zabalenie celého IP paketu do nového) protokolov
- ▶ algoritmy: HMAC-MD5/SHA-1 (96), 3DES, Blowfish, ...
- ▶ správa kľúčov: manuálna, automatizovaná (ISAKMP/Oakley)

Kryptológia v kontexte

- ▶ aká dôveryhodná je implementácia?
- ▶ akým spôsobom sú spravované kľúče:
 - ▶ generovanie?
 - ▶ distribúcia?
 - ▶ backup?
 - ▶ riadenie prístupu?
 - ▶ ničenie?
- ▶ postranné kanály (čas, spotreba zdrojov, hyperthreading, chybové hlášky, ...)?

...je ľahké urobiť chybu.

Kryptológia v kontexte (2)

- ▶ kryptografia je obvykle použitá v niečom „väčšom“
- ▶ operačný systém, čipové karty, databázový systém, mail, webová aplikácia, e-commerce, sieťové protokoly, ...

ISO/IEC 27002

- ▶ Code of practice for information security management
- ▶ 12.3 Cryptographic controls
 - 12.3.1 Policy on the use of cryptographic controls
 - 12.3.2 Key management

Key management – hlbšie

1. Generating keys for different cryptographic systems
2. Generating and obtaining public key certificates
3. Distributing keys to intended users
4. Storing keys and how to obtain access to keys
5. Changing or updating keys
6. Dealing with compromised keys
7. Revoking and deactivating keys
8. Recovering keys that are lost or corrupted as part of BCM
9. Archiving keys
10. Destroying keys
11. Logging and auditing key management activities

Common Criteria

- ▶ ISO/IEC 15408 – Evaluation criteria for IT security
- ▶ časti:
 - ▶ Part 1: Introduction and general model
 - ▶ Part 2: Security functional requirements
 - ▶ Part 3: Security assurance requirements
- ▶ flexibilné – hodnotenie veľkých systémov (napr. operačné systémy), aj malých (napr. čipové karty, aplikácie)

Common Criteria (2)

- ▶ CC a kryptografické algoritmy:

The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

Common Criteria (3)

- ▶ požiadavky na bezpečnostné funkcie
- ▶ trieda FCS (Cryptographic support):
 - ▶ Správa kryptografických kľúčov
 - ▶ generovanie kľúčov
 - ▶ distribúcia kľúčov
 - ▶ prístup ku kľúčom
 - ▶ deštrukcia kľúčov
 - ▶ Kryptografická činnosť
- ▶ pre jednotlivé komponenty sa vyžaduje súlad s definovanými algoritmami, metódami, dĺžkami kľúčov, štandardmi.

FIPS 140-2

- ▶ Security Requirements for Cryptographic Modules
- ▶ požiadavky na kryptografické moduly (SW aj HW)
- ▶ 4 úrovne bezpečnosti:
 - Level 1: najnižšia úroveň
 - Level 2: + detekcia fyzickej manipulácie, ...
 - Level 3: + odolnosť voči fyzickej manipulácii, ...
 - Level 4: + ...
- ▶ Level 1,2 – najčastejšie úrovne
 - ▶ (za rok 2011) 64 certifikátov L1, 92 L2, 26 L3, 3 L4
- ▶ FIPS 140-2 \rightsquigarrow ISO/IEC 19790:2006 Security requirements for cryptographic modules
- ▶ (žiadna) certifikácia negarantuje bezpečnosť

FIPS 140-2 (oblasti)

1. Špecifikácia (dokumentácia) modulu
2. Časti modulu a rozhrania (vrátane segregácia)
3. Role, služby a autentizácia
4. Konečnosťavový model
5. Fyzická bezpečnosť
6. Operačné prostredie (operačný systém)
7. EMI/EMC
8. Správa kryptografických kľúčov
9. Samotestovanie
10. Záruky pre kvalitu návrhu a implementácie
11. Ochrana pred útokmi (napr. TEMPEST)

Záver

- ▶ bez kryptológie je ťažké (nemožné?) dosiahnuť bezpečnosť IS
- ▶ niekedy sú použité kryptografické konštrukcie zlé
- ▶ niekedy sú kryptografické konštrukcie použité zle