Key management and security management

PA018

Vašek Matyáš

Reminder – relevant topics…

- User authentication and identification
  - Passwords, replay attacks, challenge-response
- Cryptography, its applications

- Follow-up: Security in communications and networks
  - Authentication in networks
  - Kerberos

Key Management

- Generation
  - Random bit generators (coin tossing, el. noise, etc.)
  - Pseudorandom generators – usual in reality
    - Importance of (statistical) tests
    - Use of good ciphers
- Key storage
- Key distribution
- Key usage
- Key archiving / destroying

…

Key Managements Concepts I.

- Key Certification Center (CA center)
- Key Distribution Center
- Key Escrow
- Key Freshness
- Key Granularity
- Key Material

Key Managements Concepts II.

- Key Notarization
- Key Recovery
- Key Space
- Key Tag
- Trusted Third Party

Involvement of trusted parties

- For system setup and/or any protocol run
  - Off-line, on-line, in-line
- Key transport and/or generation
- Trust to keep secrets vs. trust to certify data
- Assumptions of following the course of action prescribed by the protocol, not knowingly collaborating with attackers, etc.

KDC Use – Usual Problems

- Delegation of trust might not be voluntary
- Attacks have to be watched by all parties
  - Key reuse
  - Impersonation of A towards C
  - Impersonation of A towards B

ISO/IEC 9798 – Entity Authentication

- Framework (1), Symmetric (2), Asymm. (3)
- Part 3 (*handouts*…):
  - Unilateral auth.
    - One-pass – signed sequence number or timestamp
    - Two-pass – challenge-response (random number)
  - Mutual auth.
    - Two-pass – signed sequence numbers or timestamps
    - Three-pass – challenge-response (random number)
    - Two-pass parallel – two unilateral two-pass protocols

Attacker can…

- Record messages
- Replay them later
  - Possibly in different order
  - Some repeatedly
  - Some not at all
- Modify a part of or whole message

Types of attacks on protocols

- Man-in-the-middle
- Replay
- Reflection
- Interleave
- Oracle (chosen-text)
- Forced delay
- …

Time-variant parameters (nonces)

- Random numbers (select from a uniform distribution), challenge-response
  - freshness
- Sequence numbers
  - Greater-by-one or only monotonic increase check
  - Counter maintenance, reset policy
- Timestamps
  - Acceptance window
  - Secure, synchronized & distributed time info (clocks)

Example: ISO/IEC 11770

- Information technology – Security techniques – Key Management
- Part 1: Key management framework
- Part 2: Mechanisms using symmetric techniques
- Part 3: Mechanisms using asymmetric techniques

ISO/IEC 11770-1

1. Scope
2. Normative references
3. Definitions
4. General Disc. of KM
    1. Protection of keys
        1. Crypt. means
        2. Non-crypt. means
        3. Physical means
        4. Organiz. means
2. Generic Key Life Cycle Model
    1. Transitions between Key States
    2. Transitions, Services and Keys

ISO/IEC 11770-1

5. Concepts of Key M.
    1. Key M. Services
        1. Generate-Key
        2. Register-Key
        3. Create-Key-Certificate
        4. Distribute-Key
        5. Install-Key
        6. Store-Key
        7. Derive-Key
        8. Archive-Key
        9. Revoke-Key
        10. Deregister-Key
        11. Destroy-Key
    2. Support Services
        1. Key M. Facility Services
        2. User-oriented Services
    3. Conceptual Models for Key Distribution
        1. KD between Communicating Entities
        2. KD within One Domain
        3. KD between Domains
7. Specific Service Providers

Annexes (!!!)

ISO/IEC 11770-3

- Secret key agreement (7 mechanisms)
- Secret key transport (6 mechanisms)
- Public key transport
  - Without a TTP (2 mechanisms)
  - Using a CA (1 mechanism ☺)

Related ISO standards

- 7498 – OSI – Security Architecture
- 9798 – Entity Authentication
- 10181 – Security Frameworks for Open Systems

Broader scope of standards related to information security

- Audit standards
  - Financial audit – IS/IT audit
- **IT security standards**
- (Other) IT standards

IT security standards

- Basic standards – OSI security architecture, entity authentication mechanisms
- Functional standards – how to use basic standards
- Evaluation criteria
- Industrial standards and methodologies
- Interpretative documentation – dictionaries, guidelines, etc.

Classification of standards

- By publisher
  - Worldwide – ISO, ISO/IEC, CCITT/ITU
  - US – ANSI, NIST
  - EU – CEN, CENELEC, ECMA
  - Groups – IETF-RFC, IEEE
  - Industrial – RSA – PKCS
- By content/cover

Basic cryptography standards

- Symmetric crypto – DES, AES
- Asymmetric crypto – encryption, signatures, key exchange and transfer
  - IEEE P1363 – Factoring-based, Discrete log based, Elliptic curve
  - NIST FIPS 186-3 – Digital Signature Standard
- Hash functions – SHA-1, RIPEMD, (MD5), SHA-512

Cryptographic algorithms

- Crucial to most systems
- National (self-)interests
- Decades of intentional avoidance of this topic for international standardization
- Crucial to DES importance – indirect support by missing widely accepted better standards
- Therefore high expectations of AES

Applied/Functional cryptography standards

- Digital certificates – X.509,
- PKCS – RSA, D-H, Certificate, Message, Private-Key, Attributes, Certificate Request, Crypto Token Interface & Information, ECC
- Security/Crypto protocols
  - Low level – basic standards (entity auth.)
  - ISO/IEC – Key Management 11770, Non-rep. 13888
  - IETF (Internet Engineering Task Force) – PKIX, IPSEC, S/MIME

Evaluation criteria

- USA – late 60s and 70s – need to minimize costs for individual evaluations
- 1985 – Trusted Computer System Evaluation Criteria – “Orange Book”
  - D class – no security
  - A1 – highest security (mathematical formalism)

Development of criteria

- Europe – ITSEC – separation of functionality and assurance
- Canada – CTCPEC – functionality separated into confidentiality, integrity, accountability, and availability
- US – Federal Criteria – development halted
- Common Criteria – worldwide standard
  - ISO/IEC 15408

Common Criteria

- Interests of users, manufacturers, evaluators
- Target of evaluation (TOE) – what is (to be) evaluated
- Protection profile (smartcards, biometrics, etc.)
  - Catalogued as a self-standing evaluation document
- Security target (ST) – theoretical concept/aim
- Evaluation of TOE – is the reality corresponding to theory (ST)?
- Functional and Assurance requirements

Importance of criteria

- Eases application and use of secure systems – easier comparison and choice-to-fit
- Eases specification of requirements
- Easier design and development

ISO 27k – BS7799

- Code of Practice for Information Security Management – 1995
- Specification for Information Security Management Systems – 1998
- Update of both in 1999
- ISO/IEC standard 17799
- ISO/IEC 27000 series
  - ISO/IEC 27001 replaces ISO/IEC 17799

One step after another…

1. Risk analysis
2. Specification of security policy and security architecture
3. Design and implementation of security mechanisms
4. Support, maintenance, control, re-evaluation (back to 1…)

Risk analysis

- Often rather risk assessment – less formal and rigorous process
- Quantitative vs. qualitative
- Quantitative
  - Easy to understand the results
  - Results usually in $$$ (risk exposure)
- Qualitative
  - Discrete scale (not $$$)
  - Easy to automate, not that easy to understand the results

Risk analysis – notes

- Information collection – questionnaires, interviews
- Control of completeness – formal checks, experience of the evaluator (!!!)
- Processing of inputs (semi-automated)
- Report with suggestions for risk reduction or even elimination

Incidents caused by

- Errors (not intended to happen): 50-70%
- Natural/utility influence: 10-15%
- Malicious software: 5-10%
- Intentional sabotage/attack/corruption by own/past employees/members: 10-20%
- External attackers: 1-5%

Impact of incidents is yet another issue!

Role of IT security manager

- Experience with IT security very important
- Art of persuasion critical!
- Experience: 60% management skills, 40% security expert skills
- Very demanding and challenging position
  - Criticized for incidents
  - Criticized for obstructions to “normal” processes
  - Can be appreciated for “nothing happening”? ☺

Security policy

- VERY IMPORTANT for improving the (IT) security in any company
- Company *business goals* → IT goals → IT security goals
- Helps with
  - Setting priorities (for IT, security departments)
    - Long-term goals vs. short-term goals
    - Improvement of services (vs.) company survival(!)
  - Getting management support and assuming direct responsibilities

Security policy and company culture

- The best security mechanisms are useless without effective support of all parties involved
- End-users must be trained and interested
- Management must be involved (or better lead!)
- Security is a process, not a product

Course reading – week 5

- Ron Rivest – Chaffing and Winnowing
  - *CryptoBytes* (RSA Laboratories), volume 4, number 1 (summer 1998), pp. 12-17

- http://theory.lcs.mit.edu/~rivest/chaffing-980701.txt

Coming back to the reading from last week…

Posílání PINů poštou...

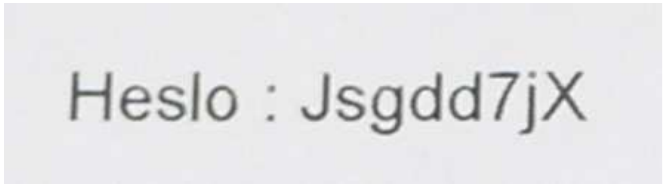
- Bezpečnost PINů zasílaných poštou
- Impulzem byla snadnost prosvícení u ČS
  - 100% úspěšnost s běžným zdrojem světla
- Šance útočníků nepozorovaně zjistit citlivé informace
- Česká spořitelna, eBanka, GE, HVB Bank
- Celkově 20 obálek (zaslané poštou, některé nedoporučeně)
- Zdroje světla: kapesní svítilna, LED, optická myš

Česká spořitelna

- PIN mailer využívající laserového tisku
- Prosvěcování bylo nejsnazší
- V obálkách jeden list papíru s PINem
- Prosvícení třech papírů + dvě černé krytí
- Nebyla nutná absolutní tma
- I začátečník dosáhl 100% úspěchu
- Starší obálky – průklepový tisk, bez úspěchu (PIN vytištěn velmi slabě)
- Průklepový tisk – nerovnosti na obálce -> umístění do další (vnější obálky)

eBanka a GE Money Bank

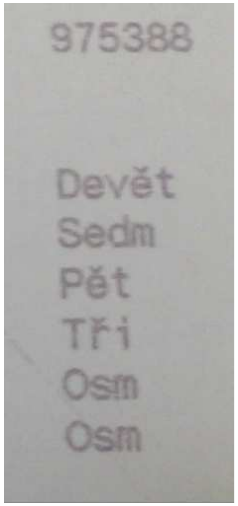
- PIN, přihlašovací údaje pro iBanking
- Průklepový tisk (až 4 vrstvy krytí)
- Horší výsledky (1 ze 4 PINů)



- PINy – průklepový tisk, bez úspěchu
- iBanking – laserový tisk
  - Heslo vytištěno výrazně větším písmem
  - Přečteno zcela bez problémů

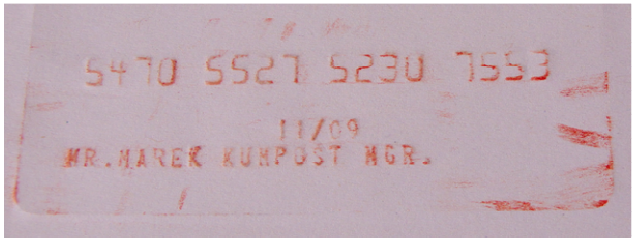
HVB Bank

- PINy – laserový tisk, odnímatelná fólie
  - Jeden PIN (ze dvou) se podařilo přečíst
- Tele-Banking – průklepový tisk, dvě krytí
  - Určení pozice a délky PINu + 6 řádků textu
  - 6místný PIN + číslice zapsané slovně
  - Možnost zjištění PINu podle slovního zápisu nebo prvního (velkého) písmene
  - I tak je určení hodnoty PINu poměrně obtížné



Embosované karty a další pozorování

- Problém při posílání karet poštou (HVB)
  - Snadno lze získat informace z obálky
  - Vytvoření padělku karty



- Různé úrovně vyškolení personálu banky
  - GE – hodnota aktivačního kódu
  - HVB – změna limitů zasláním e-mailu
    - Žádné ověření e-mailové adresy
- ČS – autentizační SMS zprávy
  - Potvrzení převodu peněz, ale ne změn příjemců
- eBanka – social engineering např. při tel. hovoru

Závěr

- Banky nereagovaly na publikované problémy PIN-mailerů
- Laserový tisk poskytuje menší ochranu
  - Dobré výsledky s ostrým světlem
  - Není nutná naprostá tma
- Průklepový
  - Dobré výsledky s kapesní svítilnou
  - Nutná naprostá tma
- Počet krycích vrstev nehrál významnou roli
- Redundantní informace o PINech ulehčují útoky
- Posílání embosovaných karet poštou zcela nevhodné
- Autentizační mechanizmy aplikovat na všechny operace