Cryptography, its applications, key management, standards

Vašek Matyáš

PA018 –
Advanced Topics in IT Security

Crypto mechanisms

- Workstation vs. LAN/firewall granularity
- Application vs. workstation granularity
- Traffic analysis, privacy services
  - Traffic padding
- Considerations (as usual):
  - Cost
  - Security
  - Administration/Logistics requirements

End-to-end vs. Link encryption

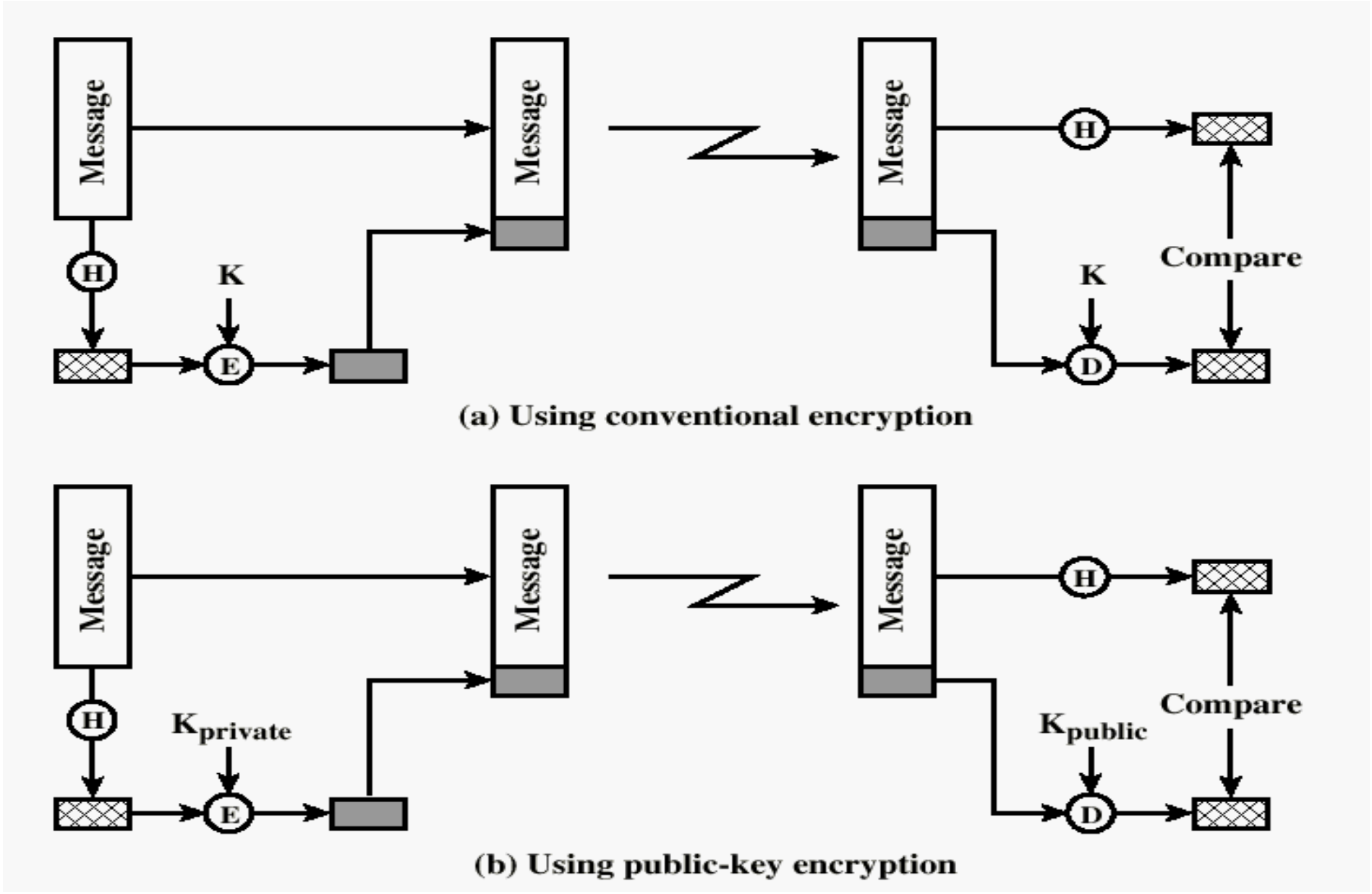
- En-/De-cryption device at sender/recipient ends
- Packet content protected at all nodes
- Headers available to all nodes on the way
- Many services cannot be provided
- IPsec

- En-/De-cryption device at ends of each link
- Processing and message avail. at each node
- Headers can be encrypted on the link (onion routing)
- Advanced network services can be provided

Public-key cryptography

- Shared-key crypto: good security vs. problems with key management
- Authentication of data
  - Hash functions (MAC)
  - Symmetric ciphers (MAC-like)
- GCHQ (UK, 1970) – non-secret encryption
  - Principles of Diffie-Hellman (76), RSA (78)
  - More at *www.gchq.gov.uk*

Data authentication



Shared-key data authentication

- Use the shared key to encrypt the data image
- Only those able to decrypt such message can verify the image correctness

- Use the shared key to create a Message Authentication Code (**MAC**) representing both the data and the key
- Only those able to recalculate the MAC can verify the image correctness

Public-key management

- Yellow Pages-like directory
  - Diffie-Hellman, “phonebooks”
  - Electronic form (browsers)
  - Efforts like Global Trust Register
- Trust models of PGP vs. (?) X.509
  - Web of trust vs. (?) Certification authority
  - PGP modified to accept X.509 certificates
  - Trust model not defined by software, but by the environment (that also implies type of S/W used)

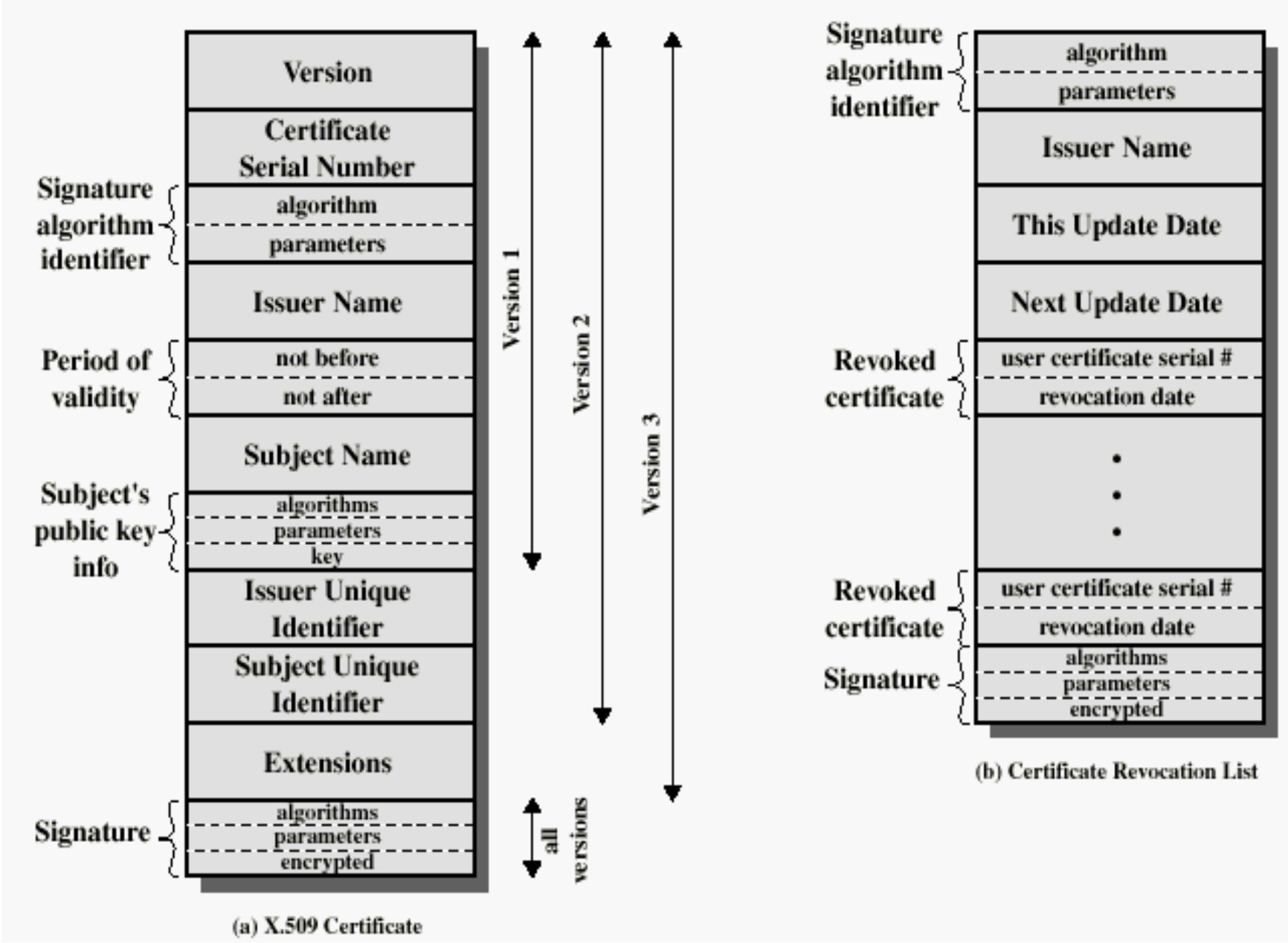
Reliance on the CA

- Anyone (with user X's certificate) can verify with X's CA that X's certificate is valid
  - That this CA created it (possibly off-line using CA's own public key)
  - That the CA still considers it valid (both off-line and on-line)
- No-one (except for the CA = owner of the CA's private key) can create/modify X's certificate

X.509 based authentication

- X.509 specifies the format for public-key certificates.
- The certificate contains the public key of a user and is signed with the private key of a Certification Authority (CA).
- Distributed environment using a database with certificate (user) information.
- Used in S/MIME, IP Security, SSL/TLS, SET.

X.509 certificate



Key/Certificate control

- **Liberal**: key/certificate is **valid** unless we are not explicitly and reliably told otherwise.
  - CRL – Certificate Revocation List.

- **Conservative**: key/certificate **invalid** unless we are explicitly and reliably told otherwise.
  - fresh confirmation, from a trusted party, and useful in case of dispute.
  - OCSP – Online Certificate Status Protocol

- **Revocation is the matter of highest importance!!!**

Certificate revocation

- Certificate revocation != key revocation
- User-lead (PGP) or CA-lead (X.509) revocation
- Reasons for certificate revocation
  - The user is no longer certified (represented) by a given CA
  - CA’s certificate or even private key misused
  - User’s private key misused

Revocation – Technical note

- PGP users can revoke their key without certifier's knowledge
- X.509 CAs can revoke user's key without her knowledge

PGP lessons

- Obviously, key servers unreliable <president@whitehouse.gov>
- Key IDs unreliable
  - should not be used for binding
- Key fingerprints better (yet not unique!!!)

CA operations

- Still immature public service market
- Banks and insurance companies uncertain where to step in
- Chicken-or-egg situation – users ready to use certs&dig.sigs or services ready?

- Closed User Groups (Extranets, Intranets)
- SSL certs enabling most e-commerce so far
- SET did not bring the break-through

PKI in use today

1) Internal systems (authentication in distributed environments)

2) With existing customers (online banking)

3) Communication with other players (partners, etc.) that have been previously known

Authenticity of documents

- Current approaches to digital signatures unsuitable to publishing, unclear liability issues, etc.

- Possible solutions:
  - Signing keys with shorter life than verification key(s)
  - Hash trees

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 one party towards another

ISO/IEC 9798 – Entity Authentication

- Framework (1), Symmetric (2), Asymm. (3)
- Part 3:
  - 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 ☺)

Broader view 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

Course reading – week 2

- Chaffing and Winnowing: Confidentiality without Encryption – Ron Rivest
  - *CryptoBytes* (RSA Laboratories), volume 4, number 1 (summer 1998), pp. 12-17
- http://people.csail.mit.edu/rivest/Chaffing.txt (link in the IS)

Reminder – term project report

- Approvals after March 7 with 50% penalty
  - All approved topics in the IS at the moment
  - Whatever is sent to me today and approved by myself tomorrow morning shall be without any penalty
  - Proposal approved March 1-7 with 20% penalty
- Your report should be:
  - Focused on the topic, analytical in nature (your own view/comments, at least in conclusions, is critical!)
  - 9-10 pages, sharp! Single lines, equiv. Times N. R. 11 (10 if necessary)
  - Delivered on/before the deadline – May 22nd
  - Either printed to H. Dvorackova or in the IS (/ Odevzdavarny / Term project reports)