copyright: Mirosław Kutyłowski, Politechnika Wrocławska

Security and Cryptography 2022

Mirosław Kutyłowski

grading criteria:

- up to 50 points from lecture (exam), up to 50 points from dr Kubiak (project...)
- the lecture at least 30% ot of 50 points must be earned to pass
- sum of points $\Rightarrow$ the final grade, 3.0: $\geq$40 points , 5.0 $\geq$ 80 points
- exam requires problem solving, memorizing facts is unnecessary

skills to be learned: developing end-to-end security systems, flawless in the real sense!

presence: obligatory during the lectures

exam date and form: subject to the situation

place: 13:15-15 Monday, 9:00-10:30 Wednesday

adjustments possible in order to ease logistics problems

grading system used last year:

- for each "chapter" consisting of a specific topic some verification of skills of the students
- possible verification forms:
  i. an assignment - homework to be returned via MS Teams (some concrete task/problem to be solved at home and returned within e.g. 1 week)
  ii. written exam

  (depending on heating ...)
- IPR taken very seriously

Online materials:

- available on my webpage

  https://kutylowski.im.pwr.wroc.pl/lehre/cs22/

- internal subpage: login: student, password: Hakan
- MS TEAMS will be used for 1-1 communiaction with the students (as it keeps a history of each conversation), avoid email
- tests – if online then MS TEAMS

Lectures:

I will try to record as much as possible via MS Teams

In case of absence you may follow the lecture on screen or replay later

Contact:

- email: yes, but for assignments etc over MS TEAMS
- phone at Politechnika – no!
- MS Teams for conf calls, Google Meet, etc

I. FAILURE EXAMPLES TO LEARN FROM

I.1. PKI for Signing Digital Documents

PKI - Public Key Infrastructure

- strong authentication of digital documents with digital signatures seems to be possible
- in fact we get an evidence that the holder of a private key has created a signature
- who holds the key? PKI has to provide a certified answer to this question
- PKI is not a cryptographic solution - it is an organizational framework (using some crypto tools)

PKI, X.509 standard

- a certificate binds a public key with an ID of its alleged owner,
- a couple of other fields, like validity date, key usage, certification policy, ...
- certificate signed by CA (Certification Authority)
- tree of CA's (or a directed acyclic graph), with roots as "roots of trust"
- **status of a certificate may change - revocation**
- checking status methods: CRL, OCSP

reasons for PKI failure:

a nice concept of digital signatures but

1. big infrastructure required:
   - substantial cost and effort
   - long time planning needed (so possible in China, but not in Europe)
   - unclear financial return
2. scope of necessary coordination,
   - in order to work must be designed at least for the Common Market
   - example of killing the concept: link to certification policy in Polish

3. lack of interoperability (sometimes as business goal)
   - companies make efforts to eliminate competition
   - standarization may be focused on securing market shares
   - a long process ⟨text-dots⟩
4. necessary trust in roots
   - how do you know that the root is honest?
5. registration: single point of fraud, (e.g. with fake breeding documents)
   - once you get a certificate you may forge signatures
6. responsibility of CA
   - fiancial risk – based on risk or responsibility
7. cost - who will pay? For the end user the initial cost is too high.
   - certificates are too expensive for just a few signatures (at least initially)
8. legal strength of signatures
   - if scheme broken or signing devices turn out to be insecure you are anyway responsible for the signatures. After revocation only the new signatures invalid

9. unsolved problem of revocation: possible to check the status in the past but not now

reason: mismatch of requirements and interests with the designed solution

"⟨text-dots⟩but there nothing one can do about it." – this is false

- Smart-ID project, Estonia (clever RSA-like solution, mediated signatures, no CRL, OCSP needed)
- SPKI idea (source centric certification), *suicide notes, certificates of health*

before Smart-ID in Estonia

- personal ID smart cards, implements RSA signature of the owner
- certificate of BSI for Infineon chip and software
- Czech colleagues from Brno found that the RSA keys generated so that the old attacks work
- an implementation bug or a trapdoor
- all smart cards had to be updated

Smart-ID

1. RSA:
   - "RSA" where n is a product of two RSA numbers
   - the same algebra – no difference seen unless you factorize n
   - but secret keys distributed between the card and a mediator server
   - nobody has full knowledge of the secret keys
2. links between consecutive signatures (to be checked by the mediator server)
3. revocation by blacklisting on the server