Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Security protocol design and evaluation

Example: the mBricks net protocol specification version 2.2

Bjarte M. Østvold, Truls Fretland,
Anders Moen Hagalisletto
Norsk Regnesentral (NR)

Norsk UMTS-Forum, 2008-06-04

On designing security protocols

- A notoriously difficult and error-prone activity
- Many examples of expert-made protocols that have security problems
- Lots of standard protocols that have been analyzed by clever people
- Safest advice: *Don't do it*

If you really need a custom security protocol

- Document protocol carefully
- Decrease risk by simplicity and reuse
- Evaluate protocol as separate activity

Levels of ambition in protocol specification

1. No description
2. Free text description, tables, diagrams
3. Formal language description of protocol, security goal

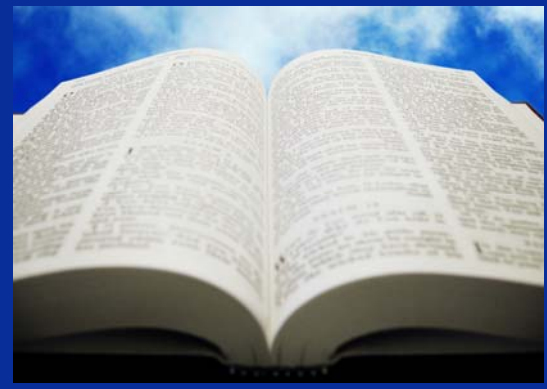
Levels of ambition in protocol evaluation

1. No evaluation
2. Informal evaluation
3. Structured evaluation:
   Compare to best practice in a systematic way
4. Formal evaluation:
   Analyze with formal methods and tools

More on structured evaluation

- Systematic, yet informal, analysis of specification
- Goal: Find out if it follows some best practice
- Need best practice to check against
- No formal guarantees about correctness, security

Abadi and Needham's 11 principles



- **Paper:** Prudent engineering practice for cryptographic protocols (IEEE Trans. Soft. Eng. 1996)
- **Serve as design guidelines for new security protocols.**
- **Require design decisions to be documented thoroughly**
- **Help avoiding common mistakes and subtle problems**

The 11 principles require a protocol to specify…

- The meaning of a message
- The actions to performs when receiving a message
- Where encryption and signing are used and for what purpose
- Same for: names, nonces, timestamps
- Key life-cycles
- Message encoding and recognition
- Trust relations

NR' structured evaluation of mBricks net protocol specification

- **Full disclosure:**
  NR participated in the writing of the protocol specification – before evaluation started
- **Process:**
  Specification was revised several times during evaluation – based on input from NR
- **Scope:**
  Evaluation did *not* cover key distribution, key revocation, pseudo-random number generation

Evaluation results for mBricks net version 2.2

- The protocol specification
  - complies with 10 of the principles
  - does not comply with 1 principle – key freshness
- The key freshness issues result from conscious choices made by the specification authors
- Remarks not related to the principles (on use of cryptography):
  - Should compare authentication scheme to those in the scientific literature
  - The protocol as specified is ‘UDP-like’ which creates some security weaknesses if the underlying transport mechanism also is UDP-like