Topics for the cryptography seminar, Autumn 2007

Peeter Laud

September 12, 2007

My topics

- Computationally sound, (more or less) automated analysis of cryptographic protocols.
- Secure information flow in programs.
- Meaning of and achieving of fairness, reputation, stability...

Analysis of cryptographic protocols

- Security proofs of cryptographic protocols — sequences of protocols ending with obviously secure protocols.
  - A protocol in the sequence is obtained from the previous one by applying one of well-defined protocol transformations.
- There is also a “big-step” method.
- There are great many different protocols using great many different primitives and having great many different security goals.
- There is an existing tool that already does something.

Secure information flow

- Assume the inputs and outputs of a program are partitioned into high- and low-security ones.
- The program is *non-interferent* if the high-security inputs affect the low-security outputs only in ways that are of no help to determine any properties of these inputs.
- Non-interference is often a too strong property. Declassification is often needed.
- I'm proposing a topic of studying various means of declassification:
  - What kinds of security policies they allow.
  - How are they semantically founded.
  - How can we verify that declassification is used correctly and security policies are not violated.

Guilt assignment and reputation management

- When the execution of a protocol fails to deliver the result, who is to blame?
- What it means that a party is guilty of letting the protocol fail?
- How can other parties pinpoint the guilty party?
- How can the communicate the bad deed of the guilty party? Why should the outsiders believe them?
- How to manage reputations over longer timeframes?

Research areas under this topic

- Reputation management.
- Modal logics for knowledge and belief, ability and obligations.
- Protocols for fair exchange.