Effective Reasoning, Concurrency, and Security Protocols

Arjan Mooij

FoP Away Day 2007

Research directions

- Effective mathematical reasoning
  - Reach out to new application areas
  - Where designing algorithms is hard
  - Make a real and actual contribution
- Mathematics
  - Discipline bridging (Mathematics, ICT, Engineering)
- Concurrency
  - Non-blocking algorithms
  - Security protocols

Security protocols

- The field
  - Actual topic
  - Notoriously difficult to reason about
  - Lots of work on formal verification
- Groundwork
  - Modelling security properties
  - Modelling intruder behaviour
  - Calculational derivation techniques
  - Needham-Schroeder-Lowe authentication protocol

Modelling security properties

- Distributed system
  - Honest components and intruder components
  - Communication using messages via intruders
- Modelling authentication
  - Existing definitions are operational
  - In terms of pre- and post- assertions?
  - Assertions are predicates in the program text
- Question:
  - When do two components authenticate each other?

Authentication

- Consider honest components A and B
  - A wants to communicate with component p
  - B wants to communicate with component q
- Desired (simple) post-conditions:
  - Component A: $p = B \;\Rightarrow\; q = A$
  - Component B: $q = A \;\Rightarrow\; p = B$
- This corresponds to agreement in [Lowe ’97].

Modelling intruder behaviour

- Public/private key encryption system
  - [k: m] is message m encrypted with key k

- Intruders behave as a kind of channel
  - Unreliable channel: message loss and duplication
  - Capabilities from Dolev/Yao intruder model
    - Message [k: m] composed from k and m
    - Message m decomposed from [k: m] and k^{-1}

Unreliable uni-directional messages

- Introduce variables
  - Set of ever transmitted messages C
  - Receive buffer R
  - Channel copies messages from C into R
  - R.m denotes that m is in set R

- To establish a stable assertion P
  - Insert a receive statement of a message m
  - Introduce an invariant R.m => P
  - Strengthen into invariant C.m => P
  - Each send statement of m gets a pre-assertion P

Add the Dolev/Yao capabilities

- Small modifications:
  - Channel copies *derived* messages from C into R
  - Let D denote the messages that can be derived from C:
    - D contains C
    - $D.k \ \wedge D.y \ \wedge D.z \quad \Rightarrow \quad D.[k: y,z]$
    - $D.k^{-1} \ \wedge \ D.[k: y,z] \quad \Rightarrow \quad D.y \ \wedge \ D.z$

- To establish a stable assertion P
  - Insert a receive statement of a message m
  - Introduce an invariant $R.m \Rightarrow P$
  - Strengthen into invariant $D.m \Rightarrow P$

Calculational derivation techniques

- Maintenance of such an invariant D.m => P
  - D is only expanded using the send statements
  - Each send statement of m gets a pre-assertion P
- Composition, suppose m = [k: y,z]
  - Require invariant $D.k \wedge D.y \wedge D.z \Rightarrow P$
  - Heuristic: strengthen antecedent into one conjunct
- Decomposition
  - Don't apply it to results of composition!
  - Only consider the transmitted messages

Calculational derivation techniques…

- Decomposition without key transmission
  - Only consider this single send statement [k: m,x]
  - Recursively require a pre-assertion
    - $D.k^{-1} \Rightarrow P$
- Decomposition with key transmission
  - Also consider the other transmitted messages
  - Require a pre-assertion using a generalisation ……
  - Ensure that the key is considered via the send statements of the other transmitted messages

Initial results

- Model of the important notion of authentication
- Integration of intruder and communication model
- Derivation techniques
- Applied to the Needham-Schroeder-Lowe protocol
  - Authentication protocol
  - Known trap was naturally avoided
  - Key distribution protocol
  - Integration of these protocols

- Exploratory work, so lots of future work