Modelling and Analysing of Security Protocol: Lecture 11

Modelling Checking

Tom Chothia
CWI

Today

• Model Checking is useful
• Probabilities can be an important part of a protocol (also next week).

The Rest of the Course

• Today: Model Checking.
• 26th Oct: When you have to have probability and Fair Exchange protocols (Homework due).
• 2nd, 9th, 16th, 23rd and 30th Nov
  Student presentations.
• E-mail me your presentation idea’s by Friday

Today

• Model Checking for finite systems
• Specifying properties in CTL
• Dinning Philosophers
  BREAK
• Probabilistic finite systems
• Specifying probabilistic properties in PCTL
• Dinning Cryptographers

A Quick History of Key Establishment and Authentication

• 50 BC to 1960s : Not relevant:
  – Pre-computer: Caesar cipher to Enigma. Keys prearranged by hand
• 1960s to 1980s : Not considered necessary
  – ARPAnet, an open network, no or little secret, e.g. telnet, open relays

A Quick History of Key Establishment and Authentication

• 1970s to 1990s : First tries
  – Early Internet, trying for security, e.g. SSL version 1, Needham-sroder.
• 1980-2000s : Becomes a science
  – Principles for protocol design, attacker models, Kerberos, TLS, SSH
• 1990s to present: Automation
  – Understood well enough to check by machine.
Anonymity Protocols

- Upto 1990s: Not relevant:
  - Little personal information on the Internet
- Upto 2000s: Not considered necessary
- 1990 to Now: First tries,
  - Dining Cryptographers,
  - Anonymous proxies,
  - Tor.

Anonymity Protocols

- Only now:
  - Becoming a Science
  - Limited automatic checking of automata protocols
    - Only for finite systems, no dedicated tools

Model Checking

- Idea:
  - Make a model of your system with a limited number of states
  - Check every single state to make sure it's OK
- Problem: making the model finite
- Problem: "state space explosion"
- Very effective, many industrial applications

Model Checking

- 1994 Pentium chip was missing a few entries in a table.
  Almost never used so missed by standard testing.
  If \( x=4195835 \) & \( y =3145727 \) then
  \( x/y =1.333739068902037589 \)
  rather than \( =1.333820449136241002 \)
  But \( x-(x/y)= 256 \) not 0

Result

- Public relations disaster
- Jokes:
  - How many Pentium designers does it take to change a light bulb?
    - 1.99995827903
- 100 of millions of dollars of replacement costs.
- Intel now model checks all hardware.

PRISM
Traffic Lights Example

State Space

CTL examples

CTL

CTL Derived Operators.

Dinning Philosophers
Dinning Philosophers in PRISM

Checking the Dinning Philosophers

Fixing the Deadlock

Today

- Model Checking for finite systems
- Specifying properties in CTL
- Dinning Philosophers example
  BREAK
- Probabilistic finite systems
- Specifying probabilistic properties in PCTL
- Dinning Cryptographers