جامعة كارنيجي ميلون في قطر
Carnegie Mellon
QATAR CAMPUS

Kerberos Verification Project

Iliano Cervesato

Carnegie Mellon University - Qatar

iliano@cmu.edu

Joint work with Andre Scedrov, Aaron Jaggard, Frederick Butler, Christopher Walstad, Joe-Kai Tsay, Michael Backes

Verifying Kerberos

جامعة كارنيجي ميلون في قطر
Carnegie Mellon
QATAR CAMPUS
مؤسسة قطر
Qatar Foundation

- Context: 2001
  - Enormous progress in protocol verification
  - NSPK, Clark-Jacob were becoming passé
  - What do to next?
    - Toy protocols in computational model
    - Real protocols in Dolev-Yao model
- We started looking into Kerberos 5
  - The real thing, not the 6-line idealization
    - Actually, fragments

Approach

جامعة كارنيجي ميلون في قطر
Carnegie Mellon
QATAR CAMPUS
مؤسسة قطر
Qatar Foundation

- Formal representation in flexible language
  - MSR 2.0
  - Multiple abstractions at different levels of detail
- Analysis based on inductive theorem proving
  - Manual
    - So far

MSR 2.0

جامعة كارنيجي ميلون في قطر
Carnegie Mellon
QATAR CAMPUS
مؤسسة قطر
Qatar Foundation

- Strongly-typed multiset rewriting framework
  - Low-level can be abstracted in type system
  - Models protocol and intruder
- Fully definable
- Independent from verification methodology
- Not specific to security protocols

Rank & Corank

- Inductive proofs over 2 measures
  - Rank supports authentication
  - Corank supports secrecy
- Protocols alternate secrecy and authentication layers
  - Each handled separately, but cooperatively
  - Later generalized into authentication and secrecy logics
    - Work with C. Meadows and D. Pavlovic

Results: Main Protocol

- Examined the main protocol at 3 levels of detail
  - 6-line core
  - Extension with flags, options, …
  - Extension with timestamps
- Abstract proof act as template for extensions
- Found that protocols are correct, but …
  - … a number of anomalies are possible
    - Unplanned behaviors, but not attacks

Results: Cross-Realm

- Kerberos 5 supports authentication across domains
- Findings:
  - If any domain is untrusted or compromised, no authentication guaranties
- Use of MSR and proof technique scale

Results: PKINIT

- "Public-Key" variant of Kerberos
- Findings:
  - Serious man-in-the-middle attack
    - Destroys authentication guarantees
  - Countermeasures
    - We worked with IETF working group to fix it
    - Immediate security patch from Microsoft, Linux
- Used again same methodology

Computational Proofs

جامعة كارنيجي ميلون في قطر
Carnegie Mellon
QATAR CAMPUS
مؤسسة قطر
Qatar Foundation

- We redid aspects in BPW model
  - Core Kerberos 5 with/without PKINIT
- Findings:
  - Our Dolev-Yao proofs acted as blueprints for BPW proofs
  - "Cryptographic key secrecy" is in the way
  - Complete lack of modularity
    - Had to redo everything for each option
  - Inability to treat timestamps

Future Research

جامعة كارنيجي ميلون في قطر
Carnegie Mellon
QATAR CAMPUS
مؤسسة قطر
Qatar Foundation

- Better understand link between
  - DY proofs
  - BPW proofs
- Modularize / extend BPW framework
- Investigate
  - Other aspects of Kerberos
  - Other protocols
- Automate our approach