

Reasoning About Security

Aaron D. Jaggard
Kevin O'Neill

Patrick Lincoln (introduction)

Two Security Presentations

- A Formal Analysis of Some Properties of Kerberos 5 Using Multi-Set Rewriting (MSR)

Frederick Butler, Iliano Cervesato,
Aaron D. Jaggard, and Andre Scedrov

- Secrecy in MultiAgent Systems:
A Knowledge-Based Approach

Kevin O'Neill, Joseph Halpern

How Do Threats Change in Diffuse Computing World?

No single
physical target

But information
infrastructure
(protocols, etc)
can present single
points of vulnerability



Critical Infrastructure Should Be Analyzed Critically

Big Question

- What is the right model for agent behavior wrt **Information, Services, and Security** in the future (more diffuse) internet?
- What are we doing?
 - Constructing logical models of agents, knowledge...
 - Analyzing increasingly realistic protocols for security (and other) anomalies
 - Providing useful input to designers
 - Providing ways to informally and formally think through implications of design choices
 - Finding anomalies in proposed designs

A Formal Analysis of Kerberos 5 Using MultiSet Rewriting

- A goal:
 - Provide useful input to protocol designers
 - For protocols regularly used in anger
- Kerberos family in widespread use (since 1989)
- MSR a convenient logical notation for protocols, enables interesting analysis
 - I identify and formalize protocol goals
 - I identify anomalous behavior
 - Suggest fixes

Initial feedback from key protocol designers is positive

Secrecy in MultiAgent Systems: A Knowledge-Based Approach

- Goal: precise, intuitive description of arbitrary secrecy properties in multiagent systems
 - Philosophy before engineering
- Multilevel security provisions:
 - Outsiders shouldn't be able to infer ANYTHING about the system
 - What does "infer" mean?
- A new way to define secrecy
- A syntactic characterization of noninterference using knowledge
 - Connections to algorithmic knowledge, etc.
- Definitions of probabilistic noninterference

On To The Talks:

- **A Formal Analysis of Some Properties of Kerberos 5 Using Multi-Set Rewriting (MSR)**
Frederick Butler, Iliano Cervesato,
Aaron D. Jaggard, and Andre Scedrov
- **Secrecy in MultiAgent Systems:
A Knowledge-Based Approach**
Kevin O'Neill, Joseph Halpern