

# Reasoning About Security and Policies

Aaron D. Jaggard

Vicky Weissman

Joe Halpern (introduction)

Two presentations that use logic:

- to reason about security protocols:  
A formal analysis of some properties of Kerberos 5 using MSR
  - Frederick Butler, Iliano Cervesato, Aaron D. Jaggard, and Andre Scedrov
- to reason about digital rights:  
A logic for reasoning about digital rights
  - Riccardo Pucella and Vicky Weissman

# Why Reason Formally About Security?

Experience has shown that even the simplest protocols suffer from subtle but significant bugs.

- We need tools to convince ourselves that the tools we're using to protect our critical infrastructure indeed provide the protection they claim to be providing.

Logic provides such a tool.

Big step now:

- Analyzing a widely used protocol (Kerberos) at finer and finer levels of detail
  - Some problems don't show up until you look at a finer level of detail

Kerberos designers are taking notice of this work.

## **A new direction: reasoning about policies**

- What rights are you granting with a licence?
- What can a client do/not do?

This will become more and more critical in the future:

- software/music/intellectual property is sold through licences.
- In the diffuse computing world, we won't buy products, but a licence to use a product.