Foundations of Computer Security

Lecture 63: Protocol Verification

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Verification of Cryptographic Protocols

Protocols can be notoriously difficult to get correct. Flaws have been discovered in protocols published many years before.

It would be nice to be able to reason formally about protocol correctness.

How do you characterize what a "spy" can do? We should at least assume that:

- the spy can see *all messages* sent;
- can compose messages from anything visible to it;
- can interject messages into the flow.

Verification

There are several major approaches to the verification problem:

1. *Belief logics* allow reasoning about what principals within the protocol should be able to infer from the messages they see. Allows abstract proofs, but may miss some important flaws.
2. *State exploration methods* (model checking) treat a protocol as a finite state system and conduct an exhaustive search checking that all reachable states are safe.
3. *General-purpose theorem proving* uses induction over potential traces of protocol execution.

We're only going to cover belief logics.

Belief Logics

A belief logic is a formal system for reasoning about beliefs. Any logic consists of a set of logical operators and rules of inference.

One trick is taking a sequence of message exchanges and generating a collection of *belief statements*.

You have to postulate some reasonable initial assumptions about the state of knowledge/belief of the principals.

Lessons

- Protocols are crucial to the Internet; it would be great to get them right.
- Reasoning rigorously about protocols requires some way of formalizing their behavior and properties.
- Belief logics is such an approach.

Next lecture: The BAN Logic