Foundations of Computer Security
Lecture 58: Cryptographic Protocols: Abstract View

Dr. Bill Young

Department of Computer Sciences

University of Texas at Austin

Cryptographic Protocols

A protocol involves a sequence of message exchanges of the form:

$$A \rightarrow B : M$$

meaning that principal A sends to principal B the message M.

There's a "temporal" aspect to protocols. Until and unless B receives the message, he can't respond to it.

In general, B won't be expecting the message unless he has already participated in earlier steps of the protocol.

Cryptographic Protocols: Abstract View

Taking an Abstract View

There is a lot involved in making a protocol work, particularly at the implementation level.

We'll ignore issues like:

- What are the mechanisms of message transmission?
- How does a principal know when decryption has succeeded?
- How can you reliably parse a message of multiple components?
- If a message contains the name of a principal, what is the form of that name?
- How are public keys maintained and distributed?

Those are all important issues, but we want to look at protocols abstractly.

Cryptographic Protocols: Abstract View

Protocol Questions

An analysis of any protocol attempts to answer the following types of questions:

- What are the goals of the protocol?
- What does the protocol actually achieve?
- Does it achieve its stated objective?
- Does it include unnecessary steps or messages?
- What assumptions are made?
- Does it encrypt items that could be sent in the clear?
- Is it susceptible to attack? What would an attack look like?

Cryptographic Protocols: Abstract View

Lessons

- We want to look at protocols abstractly and ignore issues at the implementation level.

- A standard set of questions can be asked of any cryptographic protocol.

Next lecture: Attacks on Cryptographic Protocols