Foundations of Computer Security

Lecture 59: Attacks on Cryptographic Protocols

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

Attacks

A difficult aspect of analyzing cryptographic protocols is answering the question: *What constitutes an attack?*

- Are both authentication and secrecy assured?
- Is it possible to impersonate one or more of the parties?
- Is it possible to interject messages from an earlier exchange (replay attack)?
- What tools can an attacker deploy?
- *If any key is compromised, what are the consequences?

Is the last question really fair?

Some protocols have been in use for years before someone noted a significant vulnerability.

Attacks on Protocols

This is a partial list of attacks on protocols:

Known-key attack: attacker gains some keys used previously and uses this info in some malicious fashion.

Replay: attacker records messages and replays them at a later time.

Impersonation: attacker assumes the identity of one of the legitimate parties in a network.

Man-in-the-Middle: attacker interposes himself between two parties and pretends to each to be the other.

Interleaving attack: attacker injects spurious messages into a protocol run to disrupt or subvert it.

Attackers

The designer of a protocol should assume that an attacker can access *all of the traffic* and interject his own messages into the flow.

Can the attackers messages be arbitrary? Why not? What restrictions do we impose on the attacker?

The protocol should be robust in the face of such a determined and resourceful attacker.

Important Point About Protocols

Due to the distributed nature of the system, protocols are highly asynchronous.

- A party to a protocol won't know anything about the current run of the protocol except the messages it has received and sent.
- Except for the initiator, other parties *will not even know that they are participating* until they receive their first message.

Each message sent must be of a form the recipient can identify and respond to.

Lessons

- One of the hardest things about analyzing a protocol is understanding what an attacker might do.
- The distributed nature of the system means that no-one but the initiator knows the protocol is running until they receive their first message.
- Consequently, each message must be clear enough so that the recipient can interpret it and respond appropriately.

Next lecture: Needham-Schroeder