Foundations of Computer Security

Lecture 57: Cryptographic Protocols II

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

Some Definitions

Almost everything that occurs on the Internet occurs via a protocol.

Definition: A *protocol* is a structured dialogue among two or more parties in a distributed context controlling the syntax, semantics, and synchronization of communication, and designed to accomplish a communication-related function.

Definition: A *cryptographic protocol* is a protocol using cryptographic mechanisms to accomplish some security-related function.

Possible Goals

Among the goals of cryptographic protocols are the following:

- *Unicity:* secret shared by exactly two parties
- *Integrity:* message arrived unmodified
- *Authenticity:* message claim of origin is true
- *Confidentiality:* message contents are inaccessible to an eavesdropper
- *Non-repudiation of origin:* sender can't deny sending
- *Non-repudiation of receipt:* receiver can't deny receiving

Cryptographic Protocols Fundamentals

All cryptographic protocols share the following characteristics:

- several *principals* are exchanging messages;
- they are attempting to accomplish some security-related function;
- they are operating in a hostile and insecure environment.

The protocol must be robust and reliable in the face of a determined attacker.

Cryptographic Protocols Fundamentals

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.

Because of the distributed nature of the system and the possibility of malicious actors, there is typically no guarantee that B receives the message, *or is even expecting the message.*

A Protocol Example

Consider the following simple protocol:

1. $A \rightarrow B : \{\{K\}_{K_a^{-1}}\}_{K_b}$
2. $B \rightarrow A : \{\{K\}_{K_b^{-1}}\}_{K_a}$

Informal goal: A shares with B a secret key K, and each party is authenticated to the other.

What are the assumptions? Precisely what are the goals? Are they satisfied? How can you be sure?

However, this protocol is fatally flawed. *Can you see how?*

Lessons

- Protocols are structured exchanges of messages at the very heart of distributed communication.
- Cryptographic protocols use cryptography to accomplish security-related functions.
- Protocols operate in a hostile environment, so cannot assume that messages are delivered.

Next lecture: Cryptographic Protocols: Abstract View