Foundations of Computer Security

Lecture 51: Key Exchange

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

The Key Exchange Problem

Suppose you want to establish a secure communication channel with someone you don't know. We call this a situation of *mutual suspicion*. This is extremely common.

- You submit your income tax on-line.
- You send your credit card information to a shopping website.
- You wish to exchange encrypted email with another party.

Once you agree on a shared secret (key) the communication can proceed. But how do you exchange the key? This is the *key exchange problem*.

Key Exchange: Attempt 1

Suppose both parties S and R have a public / private RSA key pair for asymmetric communication. Say S chooses a new symmetric key K and sends to R the following message:

$$\{K\}_{K_S^{-1}}.$$

R can decrypt the message using S's public key to retrieve K. *What is wrong with this scheme?*

Answer: Any eavesdropper can intercept the message and decrypt it using S's public key to retrieve K.

Key Exchange: Attempt 2

Instead, suppose S sends to R the following message:

$$\{K\}_{K_R}.$$

Since only R can decrypt this message, confidentiality is assured. *What's wrong this time?*

Now R doesn't have any assurance that the message actually came from S. An intruder may be "spoofing" (pretending to be S) to obtain information that R intends only for S.

Can we preserve both confidentiality and authentication with one transaction?

Key Exchange (Cont.)

A third attempt is for S to send R the following:

$$\{\{K\}_{K_S^{-1}}\}_{K_R}.$$

How does R extract K? What assurances does this provide?

1. Since, no one but R can decrypt the message, confidentiality is assured.
2. No one but S could have performed the inner encryption, so authentication is accomplished.

This notion of nested encryptions is very useful in a variety of cryptographic protocols. *Could you have done the encryptions in the other order?*

Lessons

- Public key cryptosystems can be used for key exchange, but you have to do it carefully.
- Key exchange requires both confidentiality and authentication.

Next lecture: Diffie-Hellman Key Exchange