Paxson
Spring 2017

CS 161
Computer Security

Discussion 7

Week of March 13, 2017

Question 1 ***Diffie–Hellman key exchange*** **(15 min)**

Recall that in a Diffie-Hellman key exchange, there are values a, b, g and p. Alice computes $g^a \bmod p$ and Bob computes $g^b \bmod p$.

(a) Which of these values are publicly known and which must be kept private?

(b) Eve can eavesdrop on everything sent between Alice and Bob, but can't change anything. Alice and Bob run Diffie-Hellman and have agreed on a shared symmetric key K. However, Bob accidentally sent his b to Alice in plain text. If Eve viewed all traffic since the beginning of the exchange, can she figure out what K is?

(c) Mallory can not only view all Alice↔Bob communications but also intercept and modify it. Alice and Bob perform Diffie-Hellman to agree on a shared symmetric key K. After the exchange, Bob gets the feeling something went wrong and calls Alice. He compares his value of K to Alice's and realizes that they are different. Explain what Mallory has done and what she can now do.

Question 2 *Perfect Forward Secrecy* (15 min)

Alice (A) and Bob (B) want to communicate using some shared symmetric key encryption scheme. Consider the following key exchange protocols which can be used by A and B to agree upon a shared key, K_{ab}.

RSA-Based Key Exchange Protocol

Message 1	$A \rightarrow B$:	$\{K_{ab}\}_{K_B^{pub}}$
Key exchanged		
Message 2	$A \leftarrow B$:	$\{secret1\}_{K_{ab}}$
Message 3	$A \rightarrow B$:	$\{secret2\}_{K_{ab}}$

Diffe-Hellman Key Exchange

Message 1	$A \rightarrow B$:	$g^a \mod p$
Message 2	$A \leftarrow B$:	$g^b \mod p$
Key exchanged $K_{ab} = g^{ab} \mod p$		
Message 3	$A \leftarrow B$:	$\{secret1\}_{K_{ab}}$
Message 4	$A \rightarrow B$:	$\{secret2\}_{K_{ab}}$

Some additional details:

- K_B^{pub} is Bob's long-lived public key.
- All messages are destroyed immediately after reading them.
- K_{ab} and DH exponents a and b are destroyed once all messages are sent.

Eavesdropper Eve records all communications between Alice and Bob, but is unable to decrypt them. At some point in the future, Eve is lucky and manages to compromise Bob's computer.

(a) Is the confidentiality of Alice and Bob's prior RSA-based communication in jeopardy?

(b) What about Alice and Bob's Diffe-Hellman-based communication?

Question 3 *Introduction to Networking* (10 min)

(a) **Protocol Layers.** At which network layer does each of the following operate (physical, link, network, transport, or application)?

- Ethernet
- SMTP (email)
- SYN packet
- UDP
- Fiber optics
- FTP
- DNS request
- BitTorrent
- IP address
- 127.0.0.1
- 802.11n WiFi

(b) **TCP and UDP.** The transmission control protocol (TCP) and user datagram protocol (UDP) are two of the primary protocols of the Internet protocol suite.

i. How do TCP and UDP relate to IP (Internet protocol)? Which of these protocols are encapsulated within (or layered atop) one another? Could all three be used simultaneously?

ii. What are the differences between TCP and UDP? Which is considered "best effort"? What does that mean?