Computer Networks
Homework #11

January 24th 2013

computer NETWORKS

NetSec

Q1: What are the security concerns network security is targeting at? What main areas of protection does network security cover?

1. Confidentiality:

   Interceptor cannot understand.

2. Authentication:

   Other party is indeed who or what they claim to be.

3. Message integrity:

   The content of their communication is not altered.

4. Access and availability:

   Services must be accessible and available to users.

Cryptopgraphy

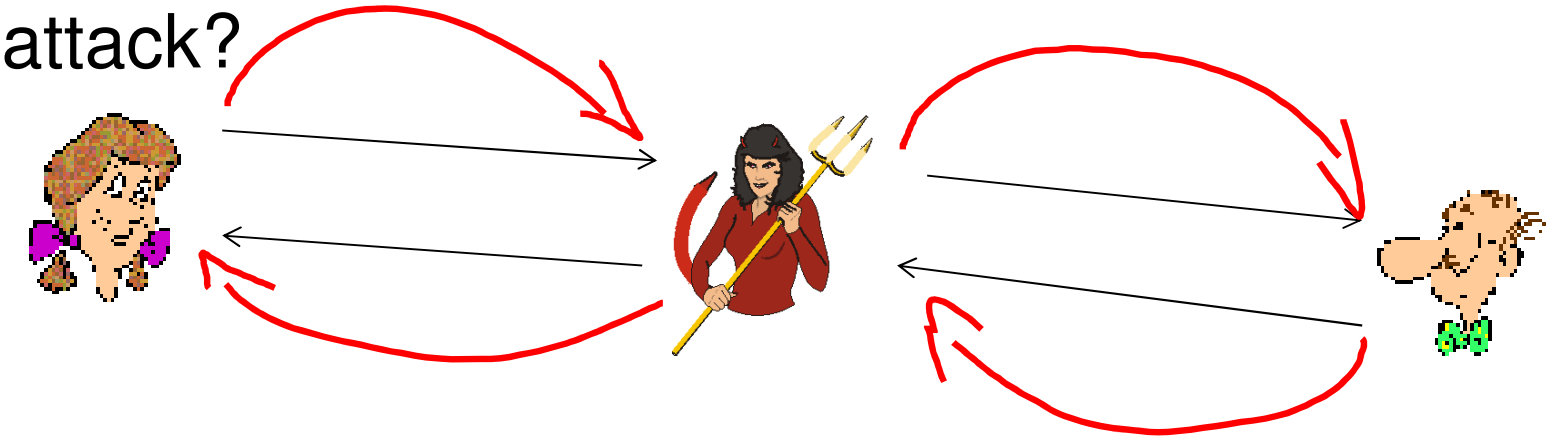
Q2: What are the two main types of cryptography?

- ✓ Symmetric crypto (encryption + decryption with the same key): DES, 3DES, AES etc.

- ✓ Asymmetric crypto (enc and dec with different keys): RSA, Public/Private keying, Diffie-Hellman

Authentication

Q3: What is a man-in-the-middle attack? Is public key cryptography save against that type of attack?



- ✓ The attacker intercepts queries from hosts and returns bogus replies.

Authentication

- ✓ An example:

1. Alice sends a message to Bob, which is intercepted by Mallory:
   Alice *"Hi Bob, it's Alice. Give me your key"*--> **Mallory** **Bob**
2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice:
   Alice **Mallory** *"Hi Bob, it's Alice. Give me your key"*--> **Bob**
3. Bob responds with his encryption key:
   Alice **Mallory** <--*[Bob's_key]* **Bob**
4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key:
   Alice <--*[Mallory's_key]* **Mallory** **Bob**
5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it:
   Alice *"Meet me at the bus stop!"[encrypted with Mallory's key]*--> **Mallory** **Bob**

Authentication

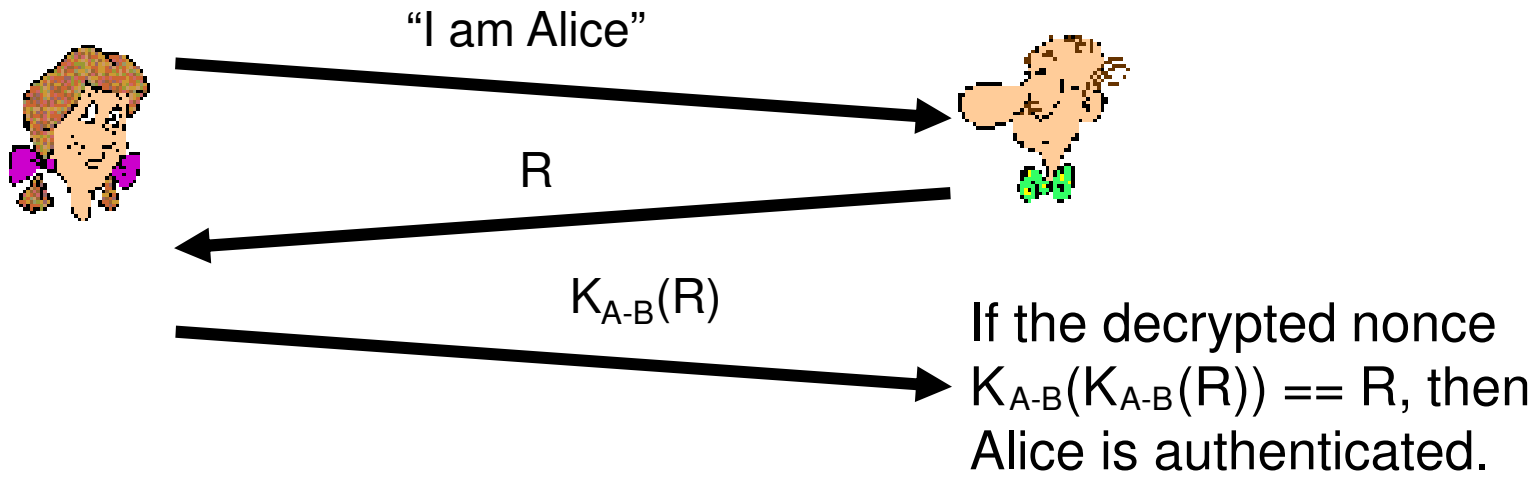
Q4: What other tricks does attackers use to overcome authentication protection? Please explain using the AP protocols presented in the lecture.

- AP 1.0/2.0): Just faking IDs (“I am Alice”) or spoofing an IP address
- Often record and playback attacks as in AP 3.0/3.1

Nonces

Q5: What is the purpose of a nonce in an end-point authentication protocol?

- ✓ A **nonce** is a number that a protocol will use only once in a lifetime.
  - Brings freshness, whether the sender is alive or not?
  - Prevents replay attacks
  - Example:



Hashes

Q6: What is the conceptual difference between a crypto-hash function and other hash functions?

- Additional requirement:

  Computationally infeasible to find two different messages, x, y such that H(x) = H(y)

  equivalently:

  given m = H(x), (x unknown), can not determine x.

Thank you

Any questions?