Computer Networks
Homework #11

Yachao Shao
yshao@gwdg.de

Exercise Exam + Q&A

- Exercise exam
  - Available in wiki
  - Intended for self-study; there will be no answer sheet or exercise session
- Question and Answer Session
  - **January 31th 2019**
  - Entirely for your benefit!
  - If there are no questions, there will be no answers
  - If you want a well prepared answer, please send us an email in advance (yali.yuan@informatik.uni-goettingen.de)

1 -- NetSec

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

1 -- NetSec

- Confidentiality: only sender, intended receiver should “understand” message contents
- Authentication: sender, receiver want to confirm identity of each other
- Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- Access and availability: services must be accessible and available to users

2 -- Cryptography

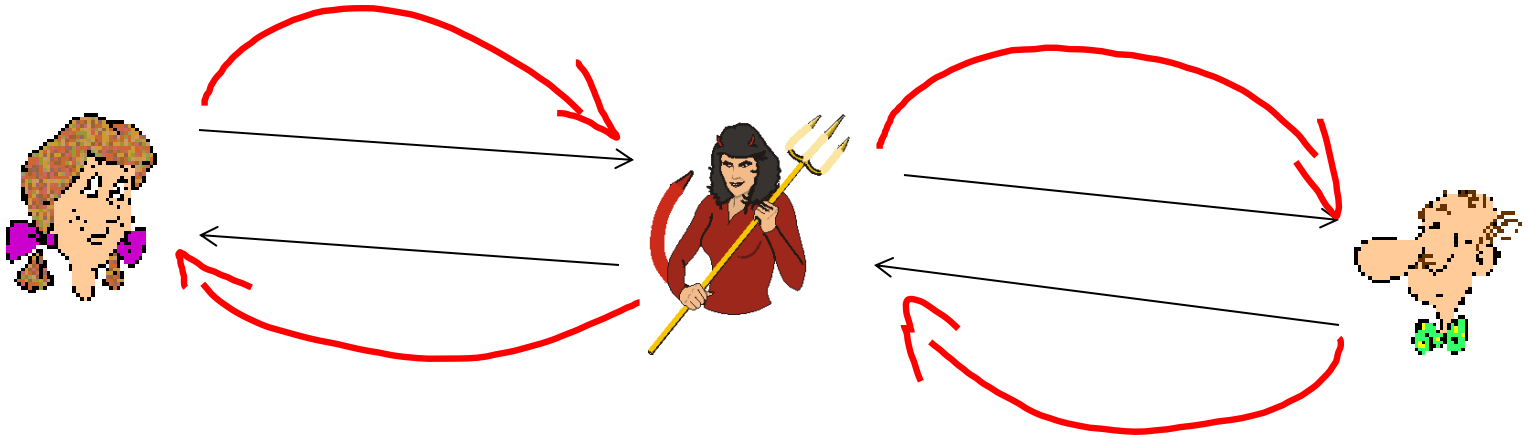
- What are the two main types of cryptography regarding Keys' type?

- 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

3 -- Authentication

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



- Asymmetric keying only helpful if public keys are pre-known or certificate bound.

4 -- Authentication

- 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

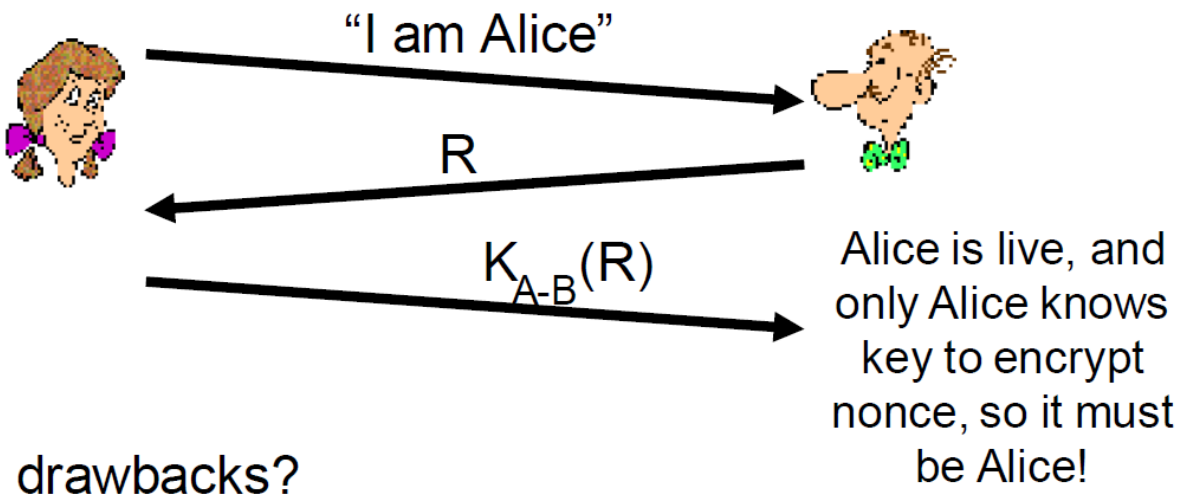
5 -- Nonces

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

Goal: avoid playback attack

Nonce: number (R) used only *once –in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice a nonce, R. Alice must return R, encrypted with shared secret key



Failures, drawbacks?

6 -- Hashes

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

- SHA-1, MD5 operate without a shared secret
- Additionally, key based Hash-based MACs (HMACs) HMAC-MD5 or HMAC-SHA1 available e.g. for signatures

7 – Authenticate Big Messages

1. Alice: $M_C = K^-_A(M)$ → Bob: $K^+_A(M_C)$
2. Alice: $[M_C = K^-_A(H(M))] + M$ → Bob: $K^+_A(M_C)$ and $H(M)$

8 – Secure Big Messages

1. Alice: $M_C = K^+_B(M)$ → Bob: $K^-_B(M_C)$
2. Efficient Way
   1. Share a symmetric key (K_S) using public key:

      Alice: $K^+_B(K_S)$ → Bob: $K^-_B(K_S)$
   2. Send big message using shared symmetric K_S

      Alice: $M_C = K_S(M)$ → Bob: $K_S(M_C)$

Thank you

Any questions?