Computer Networks WS20/21

Exercise 11

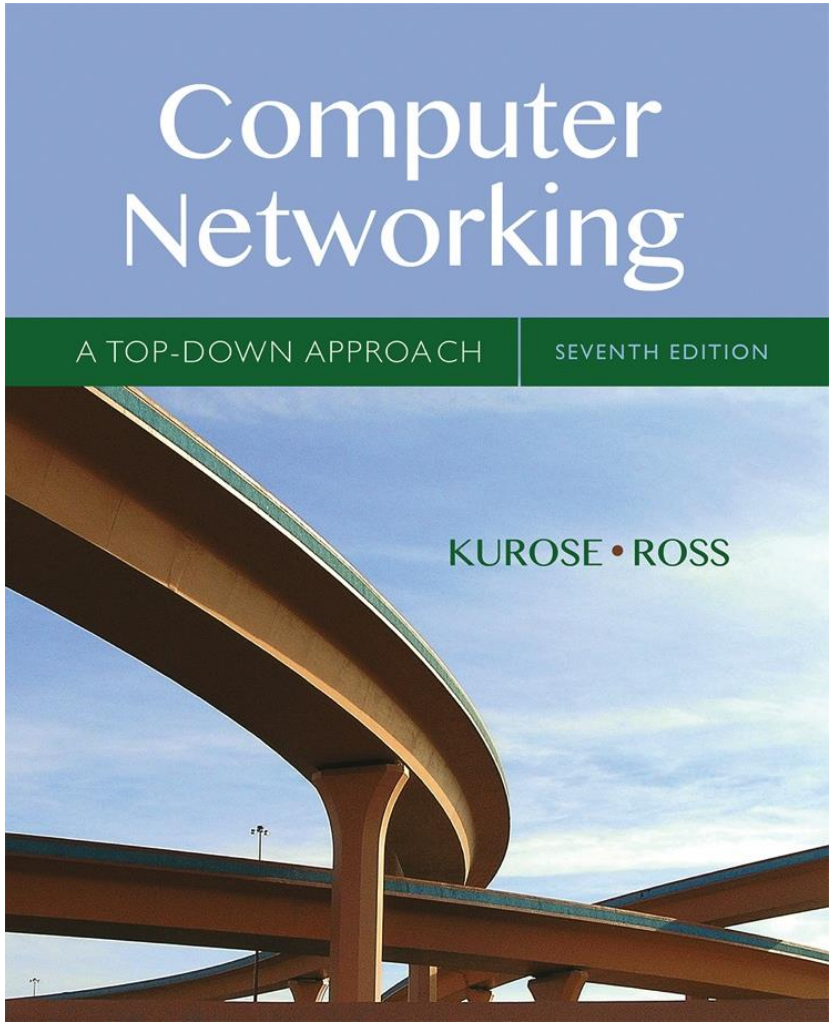
Recommendation

Try to borrow (or buy) this book:

Computer Networking: A Top Down Approach

7th edition. Jim Kurose, Keith Ross, Pearson, 2019.

It is very good to understand!



NetSec

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

- 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

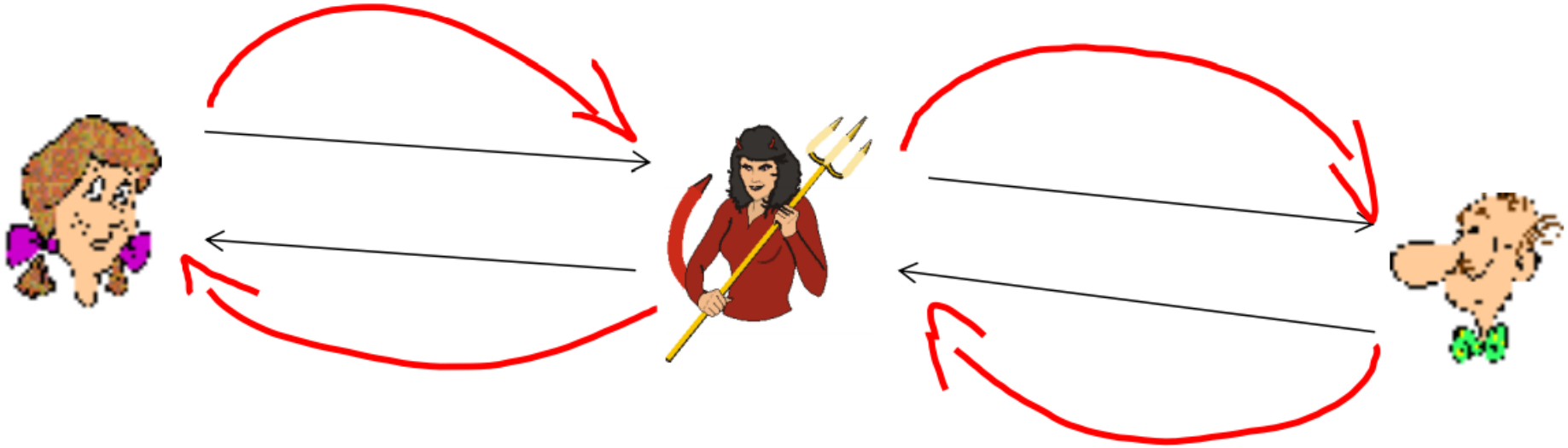
Cryptography

- Q2: 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, DiffieHellman

Authentication

- Q3: 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.

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

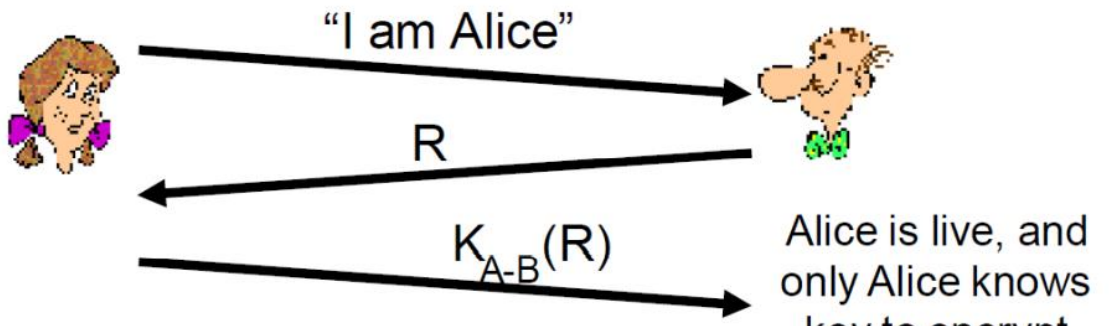
Nonces

- Q5: What is the purpose of a nonce in an endpoint 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?

Hashes

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

1. Every cryptographic hash function is a hash function. But not every hash function is a cryptographic hash.
2. A cryptographic hash function aims to guarantee a number of security properties.
3. Non cryptographic hash functions just try to avoid collisions for non malicious input.

Authenticate Big Messages

- Q7: Alice wants to send a big message (~ 1Gb) to Bob. Explain how she can authenticate herself. Is there a more efficient way to do it?

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

Secure Big Messages

- Q8: Alice wants to send a big message (~ 1Gb) to Bob. She wants to send the message in a confidential way. How can she do that? With the techniques explained during class, please explain how it would be possible to do it in a more efficient way

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

    Alice: $K^+_B(K_S) \rightarrow$ Bob: $K^-_B(K_S)$

    2. Send big message using shared symmetric K_S

    Alice: $M_C=K_S(M) \rightarrow$ Bob: $K_S(M_C)$

Any Questions?

Mail us:

Yachao Shao: yachao.shao@cs.uni-goettingen.de
Fabian Wölk: fabian.woelk@cs.uni-goettingen.de