Computer Networks WS20/21

Exercise 12

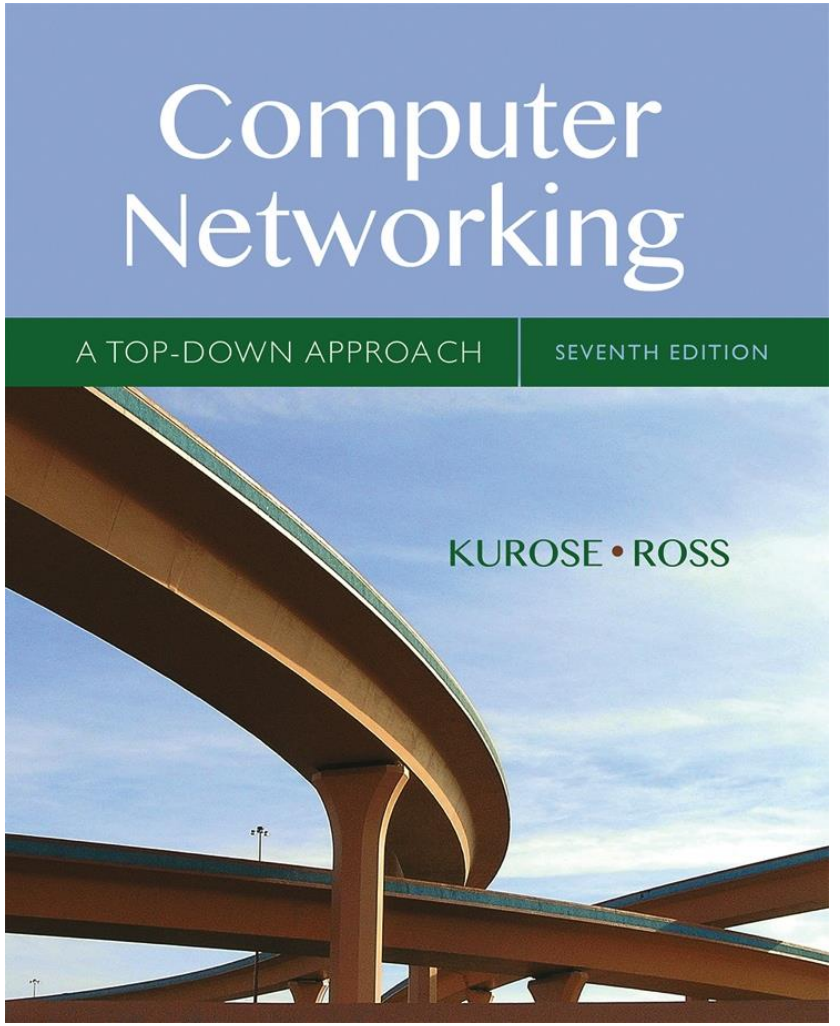
Recommendation

Try to borrow (or buy) this book:

Computer Networking: A Top Down Approach

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

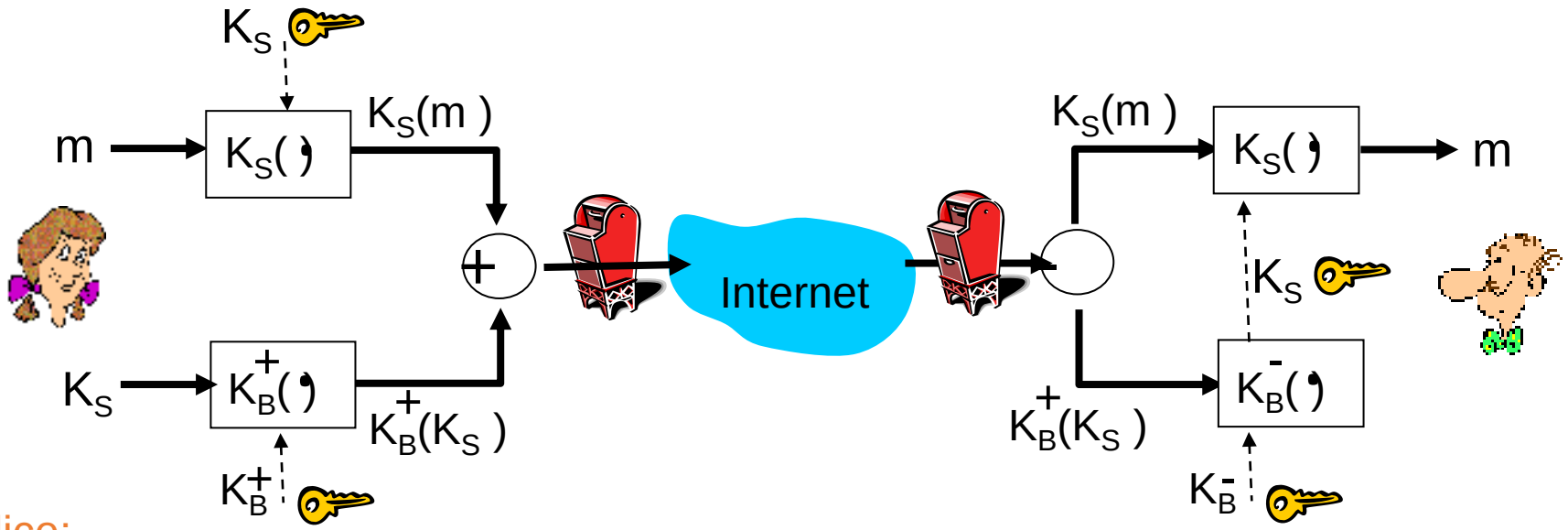
It is very good to understand!



Secure E-Mail

- Q1: Illustrate how Alice can send a confidential email to Bob using public/private keying.

Secure E-Mail



Alice:

- generates random *symmetric* private key, K_S.
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

Bob: uses his private key to decrypt and recover K_S

- uses K_S to decrypt $K_S(m)$ to recover m

Symmetric keys

- Q2: Why is a symmetric key used in most protocols to encrypt a data payload (the message etc.), even if a public/private key infrastructure exists?

- Public/Private keying more costly
- Minimal use of public/private key minimizes the key exposure
  - Symmetric key can be generated each time on the fly and is therefore always fresh
  - Public/Private key is always the same. Encrypting large amounts of data could compromise the key... (although no efficient algorithm is known yet)

PGP E-Mail signature

- Q3: Please explain in your own words the structure of the following PGP signed message (especially: how does the signature work?)

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1
Bob: My husband is out of town tonight.Passionately yours, Alice
---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

PGP E-Mail signature

Verification: Bob decrypts the PGP signature and obtains H(m). Additionally he computes H(m) for the message himself and computes it with the H(m) Alice computed.

SSL

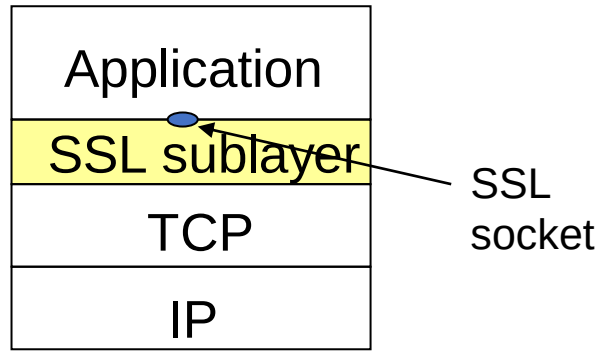
- Q4: What are the three main phases of SSL?

1. Handshake (TCP connection, authentication + master secret generation)
2. Key derivation
3. Data transfer

SSL

- Q5: On what layer does SSL reside and why is that advantageous?

- Provides transport layer security to any TCP-based application using SSL services.



TCP enhanced with SSL

IPsec

- Q6: Please sketch one typical scenario, where IPsec is used today.

- VPN gateway at company or university. E.g. 134.76.22.1 is the VPN Gateway for the GWDG

IPSec protocols

- Q7: What are the two main protocols used in IPsec and what is their primary difference with respect to security properties?

- Authentication Header (AH): Ensures authentication and data integrity. No encryption! Incompatible with NAT-traversal
- Encapsulated Security Payload (ESP): Ensures authentication, data integrity and encryption, compatible with NAT-traversal

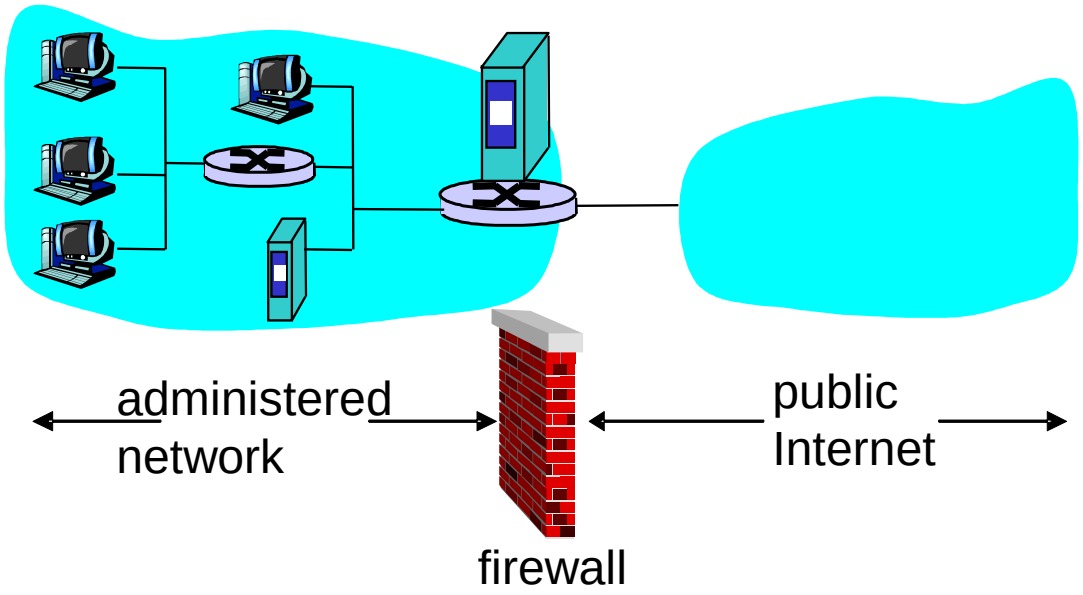
802.11i

- Q8: Who is handling the authentication information in an 802.11i scenario?

- Using TLS-EAP (Extensible Authentication Protocol over Transport Layer Security) to contact an AAA (Authentication, Authorization, Accounting) Server

Firewalls

- Q9: Explain the difference between stateless and stateful firewall.
  - Firewall: Isolation of organization's internal network from internet!



Filter rules

- The firewall can be configured to only let certain packets pass. An administrator might be interested in setting up rules like:
  - No telnet connections to hosts behind the FW
  - Prevent outside machines to connect to inside machines, but still inside machines can connect to outsiders
  - Prevent web radios
  - Many more…

Stateless & Stateful Firewalls

- Def A: a *stateless firewall* filters packets on a per-packet basis; the decision does not depend on previous packets and no state is saved on past packets
  - Pro: simpler HW
  - Cons: cannot check TCP flows
- *Def B:* a *stateful firewall* filters packets on a per-flow basis. It tracks status of every TCP connection
  - Pro: check TCP flows
  - Cons: more complex HW

Application Gateways

- Q10: Explain why Application Gateways are introduced and how they work.

- Def: an *Application Gateway* can perform packet filtering on IP/TCP/UDP fields such as a firewall. Additionally, it can perform packet filtering based on application data.
  - Pro: more granular control compared to firewalls
  - Cons: an application gateway for each application, whereas firewalls are shared among applications

Any Questions?

Mail us:

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