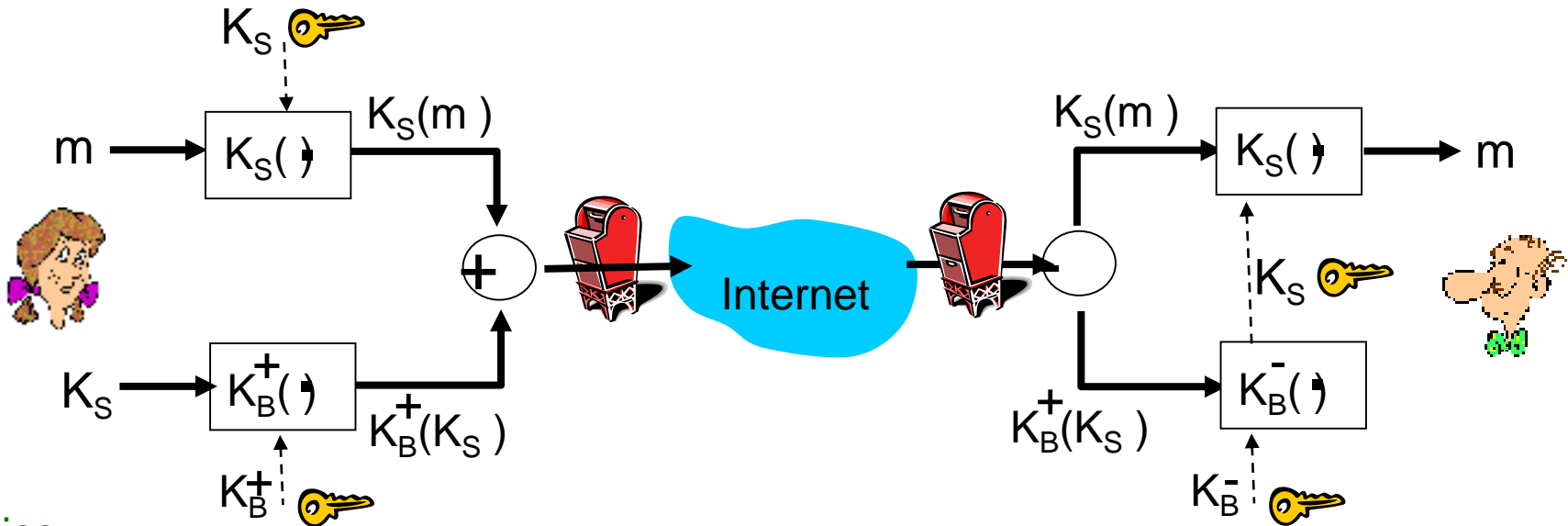# Computer Networks

Yachao Shao

yshao@gwdg.de

# 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

# Q2

o 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?

# Why symmetric keys?

o Public/Private keying more costly

o Minimal use of public/private key minimizes the key exposure

  o Symmetric key can be generated each time on the fly and is therefore always fresh

  o Public/Private key is always the same. Encrypting large amounts of data could compromise the key... (although no efficient algorithm is known yet)

# Q3

o 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

```
---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+lo8gE4vB3mqJ
   hFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Used crypto hash

Message m that is hashed with SHA1

Real signature: This is the hash of the message (H(m)) encrypted with Alice's private key.

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.

# Q4

o   What are the three main phases of SSL?

# SSL

o What are the three main phases of SSL?

   o 1. Handshake (TCP connection, authentication + master secret generation)

   o 2. Key derivation

   o 3. Data transfer

# SSL

o On what layer does SSL reside and why is that advantageous?

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

| Application |
| SSL sublayer |
| TCP |
| IP |

SSL socket
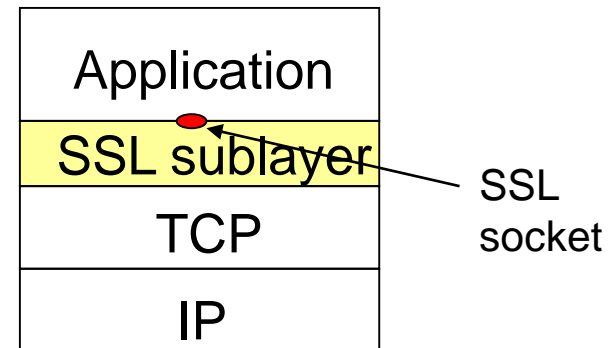
TCP enhanced with SSL

# Q6

○ 6. Please sketch one typical scenario, where IPsec is used today.

# IPsec

o Please sketch one typical scenario, where IPsec is used today.

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

# Q7

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

  o Authentication Header (AH): Ensures authentication and data integrity. No encryption!

  o Encapsulated Security Payload (ESP): Ensures authentication, data integrity and encryption.

# Q7.a

- o AH incompatible with NAT-traversal

- o ESP compatible with NAT-traversal

- o UDP Encapsulation

# 802.11i

o Who is handling the authentication information in an 802.11i scenario?

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

# Firewalls

o What is the purpose of a firewall and what are filter rules?

    o Isolation of organization's internal  network from internet!



administered network      public Internet
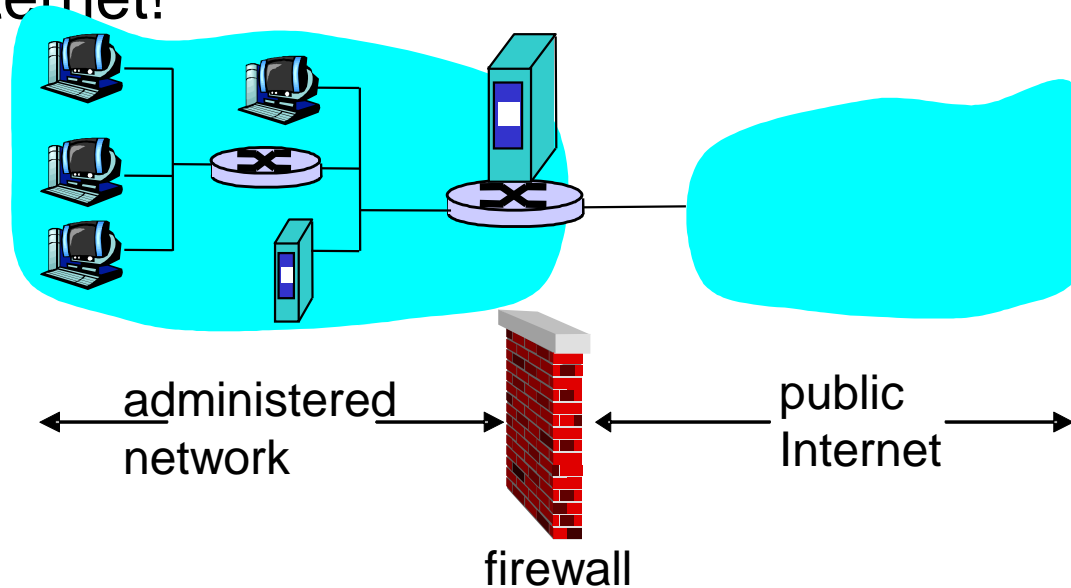
firewall

# Filter rules

o The firewall can be configured to only let certain packets pass. An administrator might be interested in setting up rules like:

  o No telnet connections to hosts behind the FW

  o Prevent outside machines to connect to inside machines, but still inside machines can connect to outsiders

  o Prevent web radios

  o Many more…

# 9 – Stateless & Stateful Firewalls

o 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

- o Pro: simpler HW
- o Cons: cannot check TCP flows

o Def B: a stateful firewall filters packets on a per-flow basis. It tracks status of every TCP connection

- o Pro: check TCP flows
- o Cons: more complex HW

# 10 – Application Gateways

○ 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

# Exam in general

- Time: 14:00-16:00  Feb. 6   2020
- Room:  MN08
- Deadline in FlexNow!
- 90 minutes, no notes allowed
- No calculator needed, just a blue or black ballpen, paper will be provided
- We start at 14:15, be there at around 14:00
- Check out old exams on website

# Exam hints

o No need to learn exact structure of packet (IP, TCP, UDP, …) headers

o No need to perform RSA (hard without calculator anyway ;))

o Be prepared to execute a routing algorithm

o Exercise questions often similar to exam questions

# The networking lab

o Put what you've learned in theory now into practice.

o 5 ECTS practical course with dedicated lab hardware

o Teamwork (teams of 2 students)

o Check our wiki for more details

# Thank you

Any questions?