

Computer Networks

January 25th , 2018

Prof. Xiaoming Fu

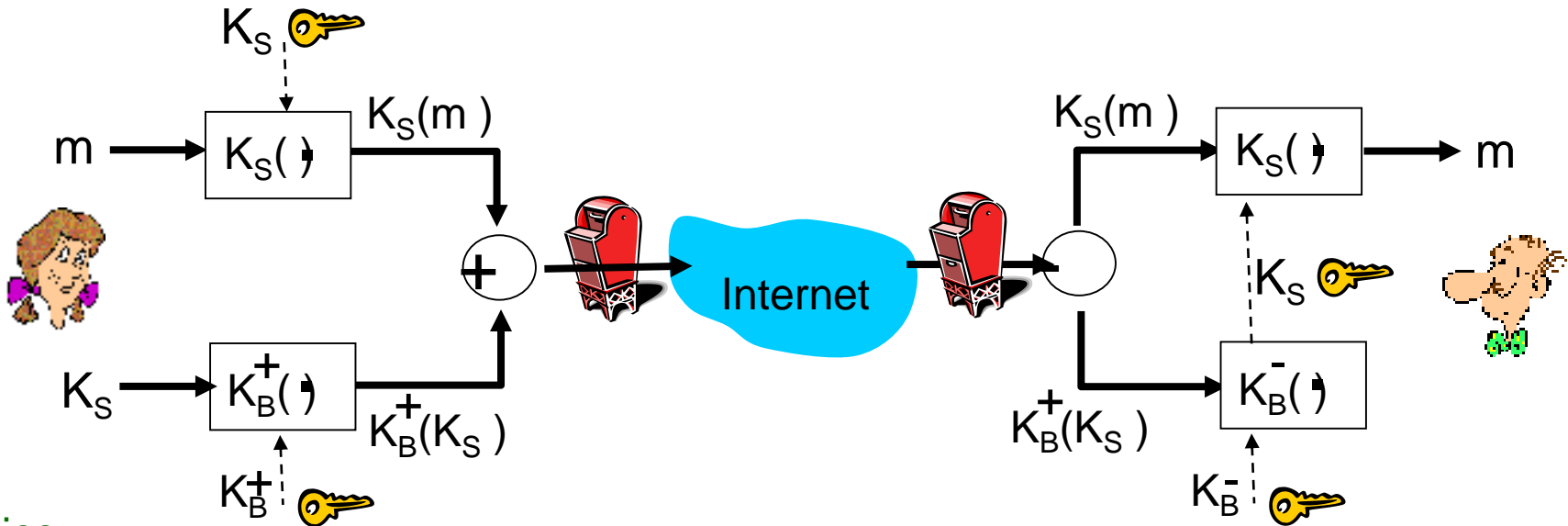
Assistant: **Alessio Silvestro (NEC Laboratories Europe)**

Email: Alessi.Silvestro@gmail.com

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

- 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?

- 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)

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  
yhHJRHhGJGhg/12EpJ+1o8gE4vB3mqJhFEvZP9t6n7G6m5Gw2  
---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+1o8gE4vB3mqJ
```

```
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 compares it with the $H(m)$ Alice computed.

Q4

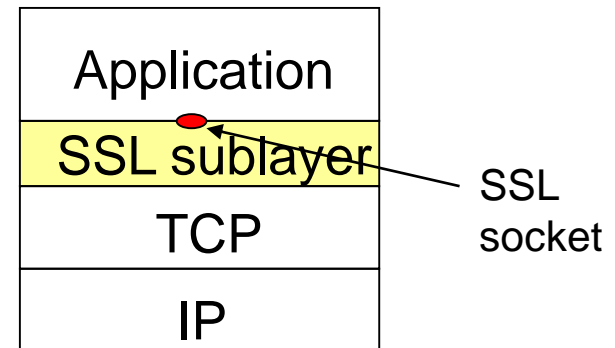
- What are the three main phases of SSL?

SSL

- What are the three main phases of SSL?
 - 1. Handshake (TCP connection, authentication + master secret generation)
 - 2. Key derivation
 - 3. Data transfer

SSL

- 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

Q6

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

IPsec

- 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

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

Q7.a

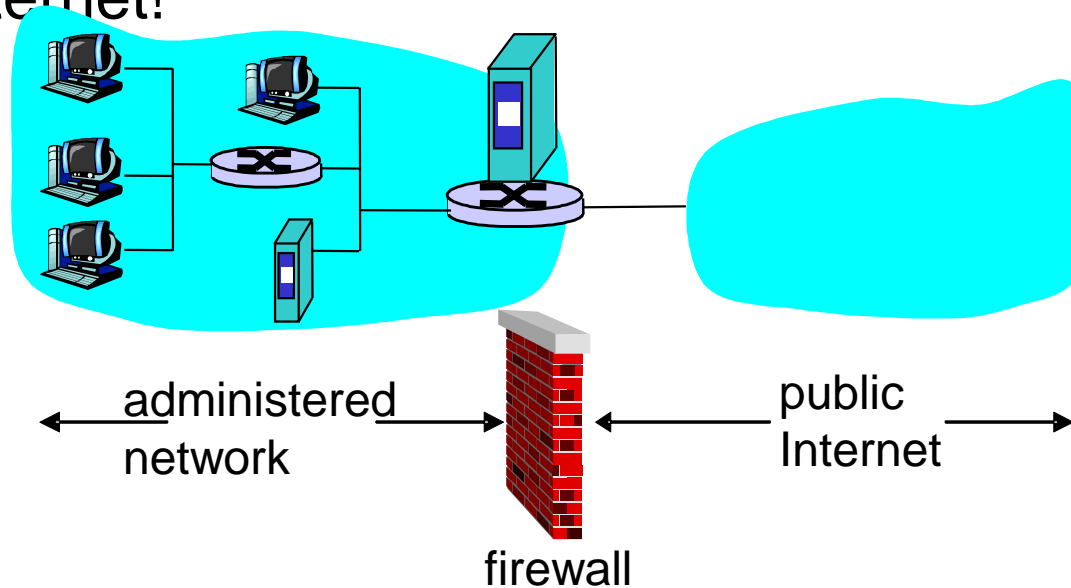
- AH incompatible with NAT-traversal
- ESP compatible with NAT-traversal
- UDP Encapsulation

802.11i

- 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

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

9 – 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

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

- Deadline in FlexNow!
- 90 minutes, no notes allowed
- No calculator needed, just a blue or black ballpen, paper will be provided
- We start at 12:15, be there at around 12:00
- Check out old exams on website, style will be similar

Exam hints

- No need to learn exact structure of packet (IP, TCP, UDP, ...) headers
- No need to perform RSA (hard without calculator anyway ;))
- Be prepared to execute a routing algorithm
- Exercise questions often similar to exam questions

The networking lab

- Put what you've learned in theory now into practice.
- 5 ECTS practical course with dedicated lab hardware
- Teamwork (teams of 2 students)
- Check our wiki for more details

Thank you

Any questions?