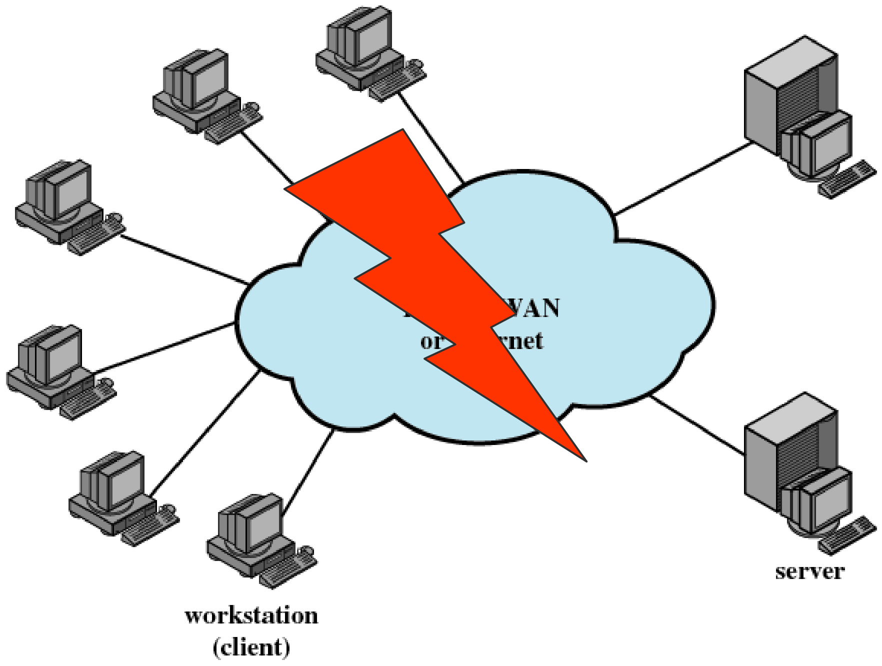
TI III: Operating Systems & Computer Networks
Network Security

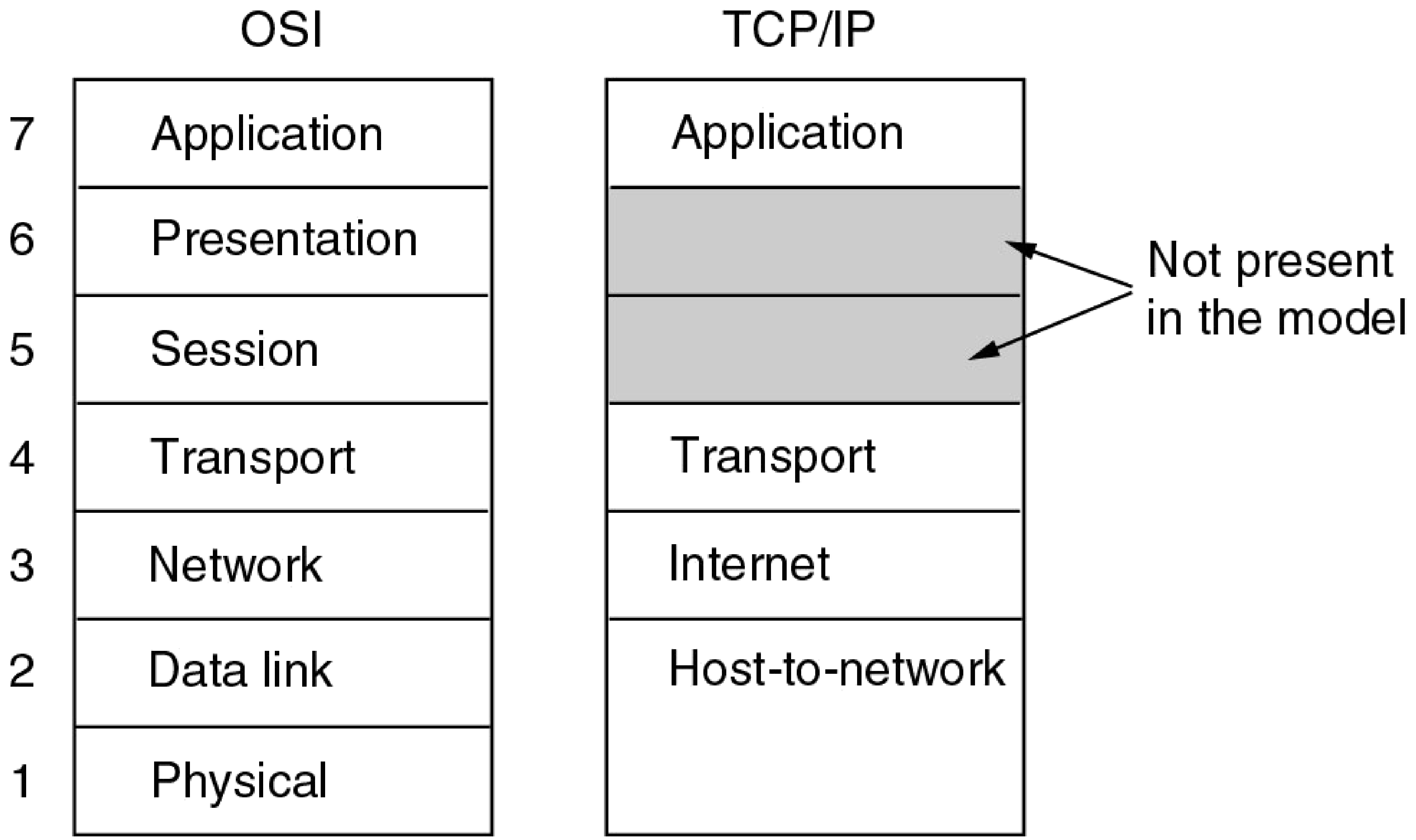
Prof. Dr.-Ing. Jochen Schiller
Computer Systems & Telematics
Freie Universität Berlin, Germany



Content

Freie Universität Berlin

Network Security



Threats in a Communication Network

Abstract definition:

- A *threat* in a communication network is any possible event or sequence of actions that might lead to a violation of one or more *security goals*.
- The actual realization of a threat is called an *attack*.

Examples:

- A hacker breaking into a corporate computer
- Disclosure of emails in transit
- Someone changing financial accounting data
- A hacker temporarily shutting down a website
- Someone using services or ordering goods in the name of others

➢ One attack may facilitate another, more serious one

Security Goals Technically Defined

Confidentiality
- Data transmitted or stored should only be revealed to an intended audience
- Confidentiality of entities is also referred to as anonymity

Data Integrity
- It should be possible to detect any modification of data
- This requires to be able to identify the creator of some data
  - Checksums are insufficient, as they could be manipulated, too

Accountability
- It should be possible to identify the entity responsible for any communication event

Availability
- Services should be available and function correctly

Controlled Access
- Only authorized entities should be able to access certain services or information

Threats Technically Defined

Masquerade
- An entity claims to be another entity, e.g. address spoofing

Eavesdropping
- An entity reads information it is not intended to read

Authorization violation
- An entity uses a service or resources it is not intended to use

Loss or modification of (transmitted) information
- Data is being altered or destroyed, e.g. files or packets

Denial of communication acts (repudiation)
- An entity falsely denies its participation in a communication act

Forgery of information
- An entity creates new information in the name of another entity

Sabotage
- Any action that aims to reduce the availability and / or correct functioning of services or systems

Threats and Technical Security Goals

Technical Security Goals	General Threats						
	Masquer-ade	Eaves-dropping	Authori-sation Violation	Loss or Mo-dification of (transmitted) information	Denial of Communi-cation acts	Forgery of Infor-mation	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x
Controlled Access	x		x			x	

➢ Threats are often combined in order to perform an attack

Communications Security – Terminology

Security Service

- Abstract service that seeks to ensure a specific *security goal*
- Can be implemented with the help of cryptographic algorithms and protocols as well as with conventional means

➢ Example: One can keep an electronic document on a USB stick confidential by storing it on the stick in an encrypted format as well as locking away the stick in a safe

  - Combination of cryptographic and other means usually most effective

Cryptographic Algorithm

- Mathematical transformation of input data (e.g. confidential data, key) to output data that suffices certain properties (e.g. collision resistant – hard to find two inputs that results in same output)
- Cryptographic algorithms are used in cryptographic protocols

Cryptographic Protocol

- Series of steps and message exchanges between multiple entities in order to achieve a specific *security objective*
- Not tied to a particular algorithm, rather classes of algorithms as components (e.g. cryptographic hash, symmetrical encryption)

Basic Security Services

Authentication

- Most fundamental security service which ensures, that an entity has in fact the identity it claims to have

Access Control

- Controls that each identity accesses only those services and information it is entitled to

Confidentiality

- Most popular security service, ensuring secrecy of protected data

Integrity

- Ensures, that data created by specific entities may not be modified without detection
- In some way, “little brother” of authentication service

Non-repudiation

- Protects against entities participating in communication exchange can later falsely deny that the exchange occurred

Cryptology – Definition / Terminology

Cryptology

- Science concerned with communications in secure and usually secret form
- Term is derived from the Greek kryptós (hidden) and lógos (word)
- Cryptology encompasses:
  - Cryptography (gráphein = to write): Study of principles and techniques by which information can be concealed in ciphertext and later revealed to legitimate users by employing a secret key
  - Cryptanalysis (analýein = to loosen, to untie): Science (and art) of recovering information from ciphers without knowledge of the key

Cipher

- One class of cryptographic algorithms
  - Others classes: Hash functions, pseudo-random number generators, ...
- Method of transforming a message (plaintext) to conceal its meaning
  - Transformation usually takes message and a (secret) key as input
- Also used as synonym for the concealed messages (ciphertext)

Source: Encyclopaedia Britannica

Cryptographic Algorithms

For network security, two main applications of cryptographic algorithms are of principal interest

- Encryption of data: Transforms plaintext data into ciphertext in order to conceal its meaning
- Signing of data: Computes a check value or digital signature to a given plain- or ciphertext that can be verified by some or all entities being able to access the signed data
- Some cryptographic algorithms can be used for both purposes; some are only secure and/or efficient for one of them

Principal categories of cryptographic algorithms:

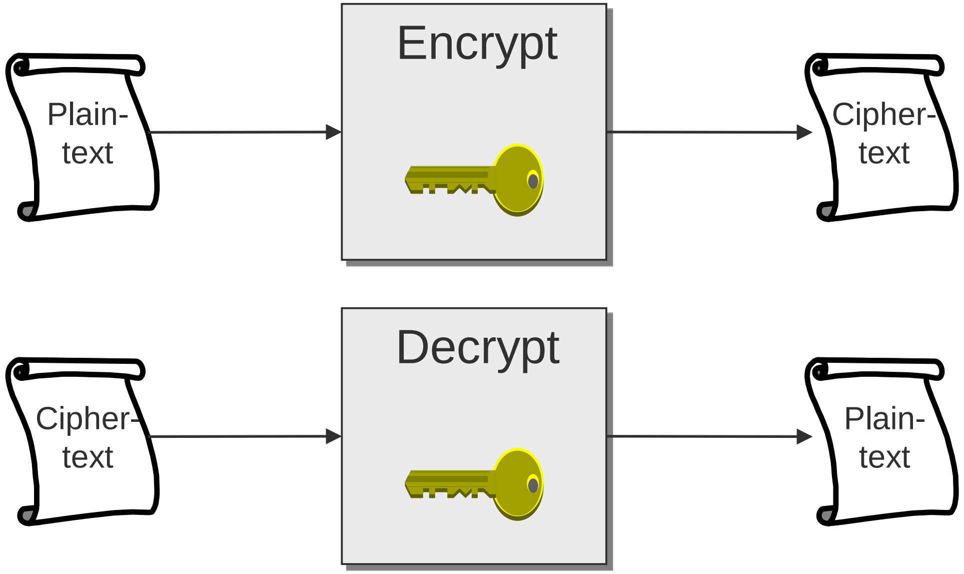
- Symmetric cryptography using one key for en-/decryption or signing/checking
- Asymmetric cryptography using two different keys for en-/decryption or signing/checking
- Cryptographic hash functions (using no keys)
    - "Key" is not an input, but may be "appended" to or "mixed" with data

Questions & Tasks

- How is user authentication often implemented? Does this really authenticate a user? Alternatives?
- Why is non-repudiation important in a business context?
- Which security goal(s) cannot be achieved via cryptography?

Symmetric Encryption

Same key $K_{A,B}$ is used for enciphering and deciphering of messages between entities A and B



Notation for plaintext message *P*:

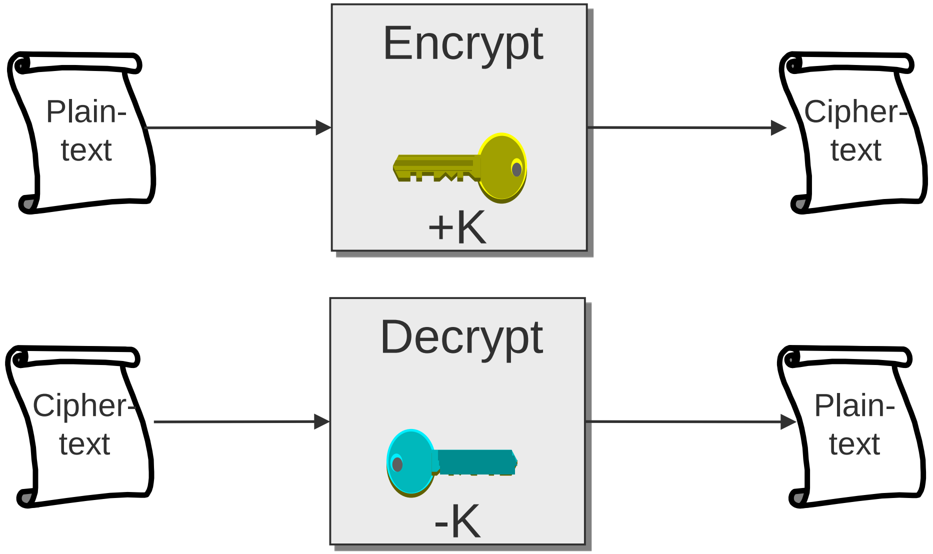
- $E(K_{A,B}, P)$ denotes ciphertext
- $D(K_{A,B}, E(K_{A,B}, P)) = P$ holds

Pro: Short key size, efficient implementations; Contra: Key distribution

➢Examples: Data Encryption Standard (DES), 3DES, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), ...

Asymmetric Encryption

Use two different keys +K and -K for encryption and decryption
- Key -K is only known to entity A and is called A's private key $-K_A$
- Key +K can be publicly announced and is called A's public key $+K_A$



Given a random ciphertext c = E(+K, m) and +K, it should be infeasible to compute m = D(-K, c) = D(-K, E(+K, m))
- ➢Hence, it should be infeasible to compute -K when given +K

Pro: (Partially) solves key distribution problem; Contra: Large key size, inefficient implementation

➢Examples: RSA, ElGamal, Elliptic curves, ...

Asymmetric/Public-key Cryptography

Applications:

- Encryption – If B encrypts a message with A's public key $+K_A$, she can be sure that only A can decrypt it using $-K_A$
- Signing – If A encrypts a message (or hash of a message) with his own private key $-K_A$, everyone can verify this signature by decrypting it with A's public key $+K_A$

➢ It is *crucial* that everyone can verify that s/he really knows A's public key and not the key of an adversary!

Practical considerations:

- Asymmetric cryptographic operations are about magnitudes slower than symmetric ones
  - ➢ Only rarely used for encrypting/signing bulk data
- Symmetric techniques are used to encrypt/compute a cryptographic hash value and asymmetric cryptography is just used to encrypt key/hash value
- Public Key Infrastructure (PKI) or web of trust (e.g. PGP) needed

Example: Classical E-Mail protection via PGP

Encryption and authentication of emails:

MD5 (Message Digest 5) calculates hash value of message

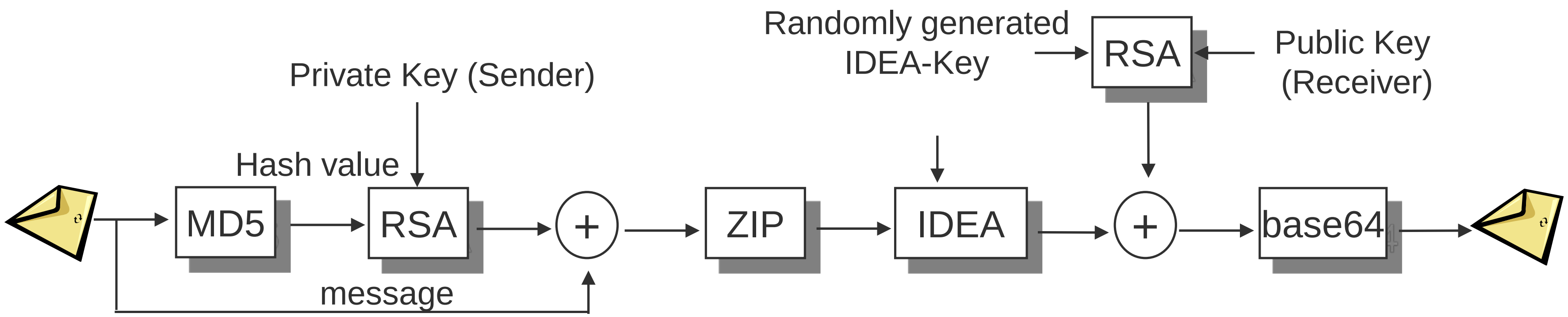
- ➢No message resulting in same hash value should be constructible within reasonable time

RSA (Rivest, Shamir, Adelman) authenticates sender and receiver:

- Each user has a known public and a private key
- Sender uses its private key to encrypt the MD5 hash value
  - ➢Authentication of sender possible
- Public key of the receiver is used to encrypt IDEA key
  - ➢Authentication of receiver

IDEA (International Data Encryption Standard) conceals message:

- ➢Message and hash encrypted using IDEA random key

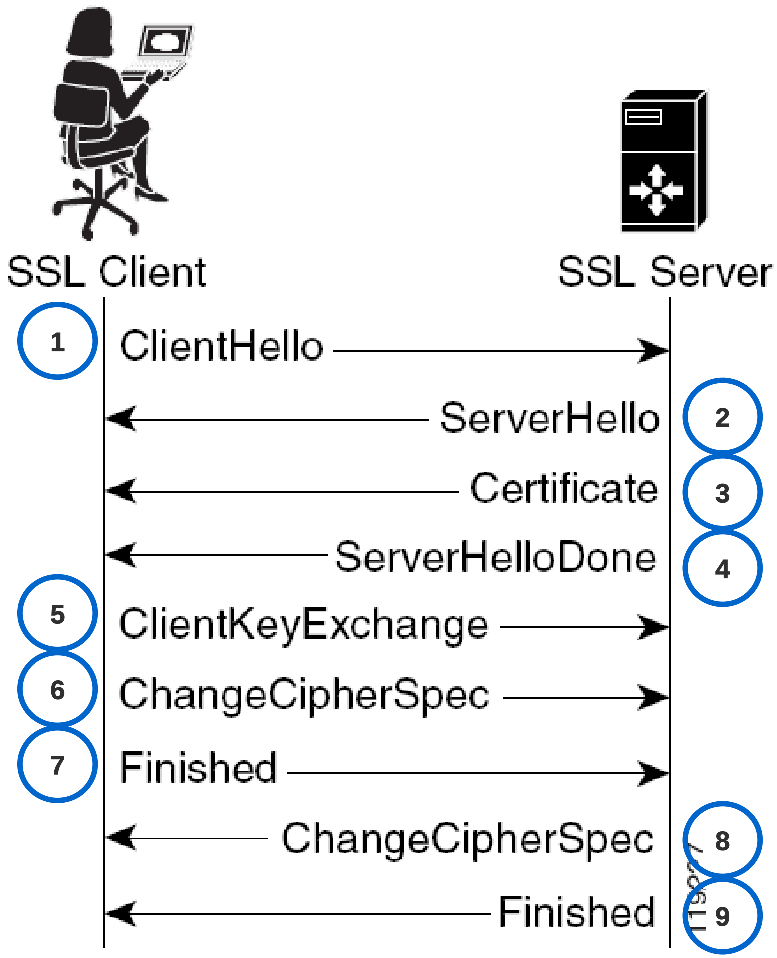


Example: HTTP over TLS/SSL

HTTPS authenticates server and establishes secure connection:

1) Propose SSL parameters, send random number
2) Agree to parameters, send random number
3) Send public key certificate
4) Conclude handshake negotiation
5) Send random number encrypted with server's public key
   - Client and server derive session key from all three random numbers
6) Activate negotiated parameters
7) Send encrypted hash over previous messages
   - Server decrypts and verifies message
8) Activate negotiated parameters
9) Send encrypted hash over previous messages
   - Client decrypts and verifies message

➢ Proceed to exchange regular HTTP data over secure channel

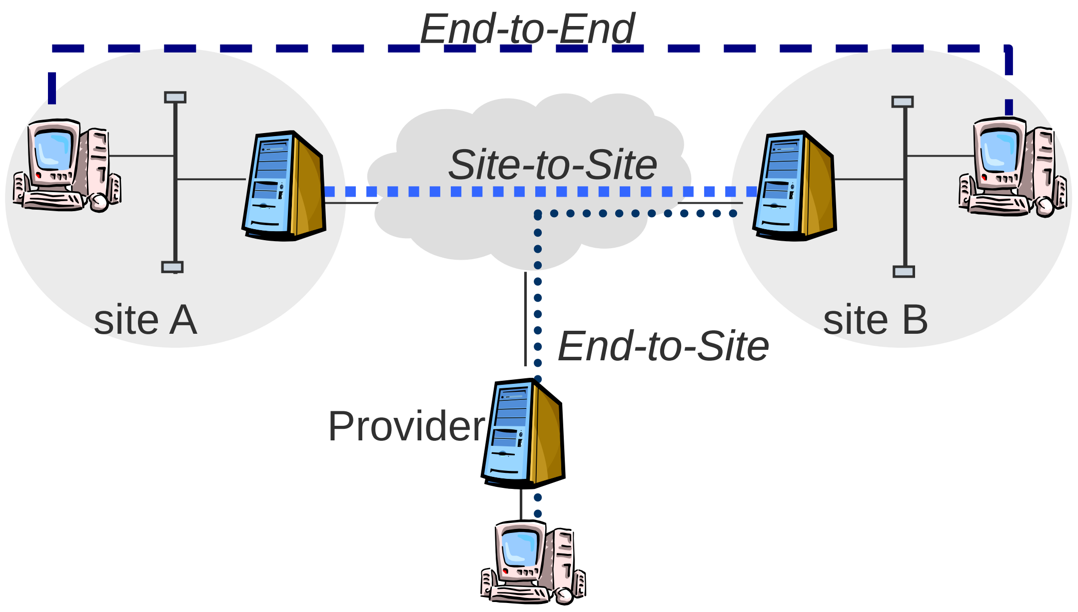


Source: Cisco Systems. Application Control Engine Module SSL Configuration Guide

Network Security – VPNs

VPN – Virtual Private Network

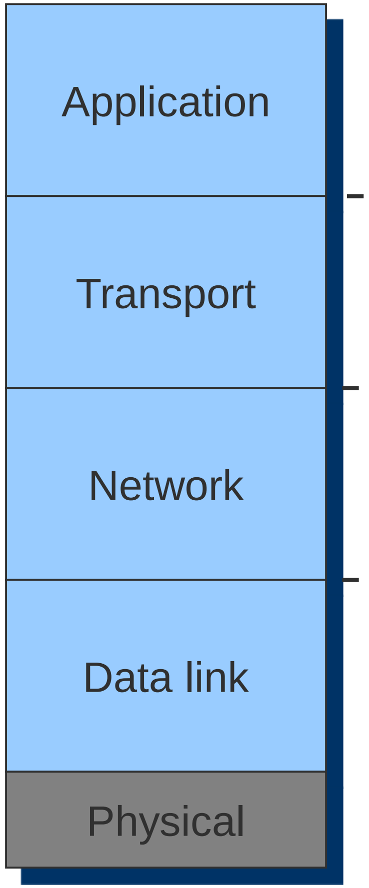
Goal: Offer secure data exchange between remote communication partners via potentially insecure transit networks, e.g. the Internet



Implemented using authentication and encryption services

Different kinds of VPNs: Host-to-host, host-to-net, net-to-net (VLAN)

VPNs in the Internet



Protection of single application layer protocols, e.g. Pretty Good Privacy (PGP), Transport Layer Security (TLS/SSL)

Protection of TCP and UDP by modification of layer 4 in end systems (mostly proprietary)

Protection of IP packets by modification of IP stack, e.g. IPSec

Protection of user data on link layer, e.g. Point-to-Point-Tunneling-Protocol (PPTP), Layer-2-Tunneling-Protocol (L2TP)

Example: IP Security (IPsec)

Operation modes:

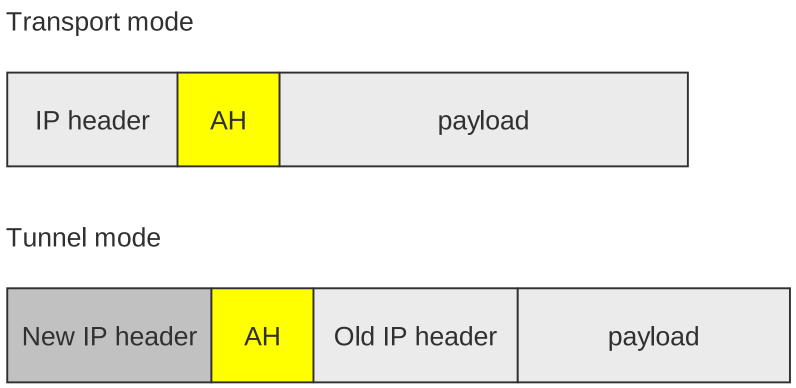
- Transport mode: No change in addresses (direct communication)
- Tunnel mode: New IP addresses between tunnel endpoints

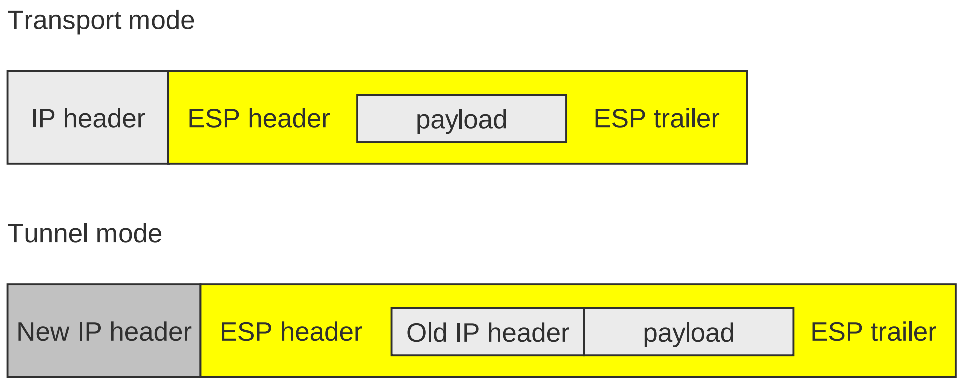
Authentication Header (AH)

- Authentication, data integrity

Encapsulating Security Payload (ESP)

- Authentication, data integrity, confidentiality





Questions & Tasks

- What are the pros and cons of symmetric/asymmetric encryption?
- Why does asymmetric encryption only partially solve the key distribution problem?
- What is the difference between a PKI and a web of trust?
- How is the exchange of the symmetric key solved in PGP?
- What is the basic idea of a VPN? On which layer can it operate?

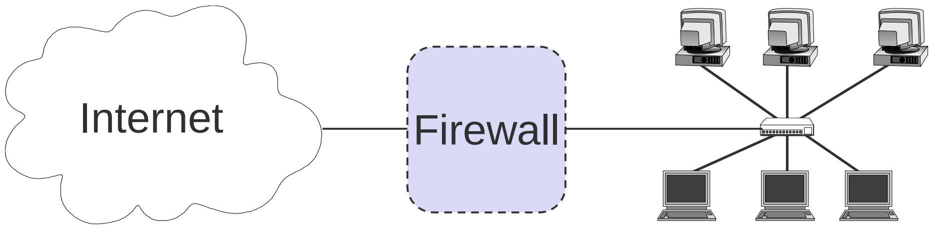
Network Security: Internet Firewalls

Network firewall can be compared to a castle moat

- Restricts people to entering at one carefully controlled point
- Prevents attackers from getting close to other defenses
- Restricts people to leaving at one carefully controlled point

Usually, firewall is installed at point where protected subnetwork is connected to a less trusted network

➢ Example: Connection of corporate local area network to the Internet



Some firewalls also implement access control on subnetwork level

Firewalls: Terminology (1)

Firewall:

- Component or a set of components that restricts access between a protected network and the Internet or between other networks

Bastion Host:

- Computer that must be highly secured because it is more vulnerable to attacks than other hosts on a subnetwork
- Bastion host in a firewall is usually the main point of contact for
  - User processes of hosts of internal networks, and
  - Processes of external hosts

Dual-homed host:

- General purpose computer with at least two network interfaces connected to different networks

Perimeter Network / De-Militarized Zone (DMZ):

- Subnetwork added between external and internal network, in order to provide an additional layer of security

Firewalls: Terminology (2)

Packet Filtering (“Screening”):

- Action a device takes to selectively control flow of data to and from a network
- Important technique to implement access control on subnetwork-level for packet oriented networks, e.g. the Internet

Network Address Translation (NAT):

- Procedure by which a router changes data in packets to modify network addresses
- Allows to conceal internal network addresses (even though NAT is not actually a security technique)
- Example: use of private IP addresses in home networks and for mobile phones

Proxy:

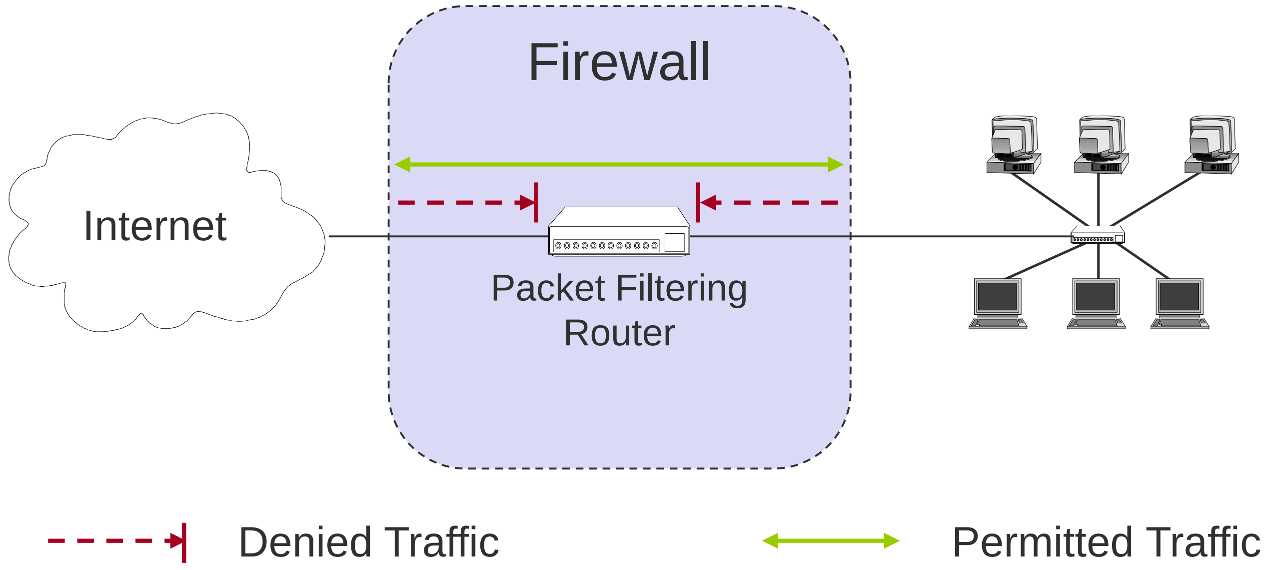
- Program that deals with external servers on behalf of internal clients
- Relays approved client requests to real servers and also relay the servers’ answers back to clients

Firewalls Architecture: Packet Filter

Simple architecture consists of a packet filtering router

Implementation options:

- Standard workstation (e.g. Linux PC) with at least two network interfaces plus routing and filtering software
- Dedicated router device, which usually also offers filtering capabilities



Requires forwarding and filtering rules to operate

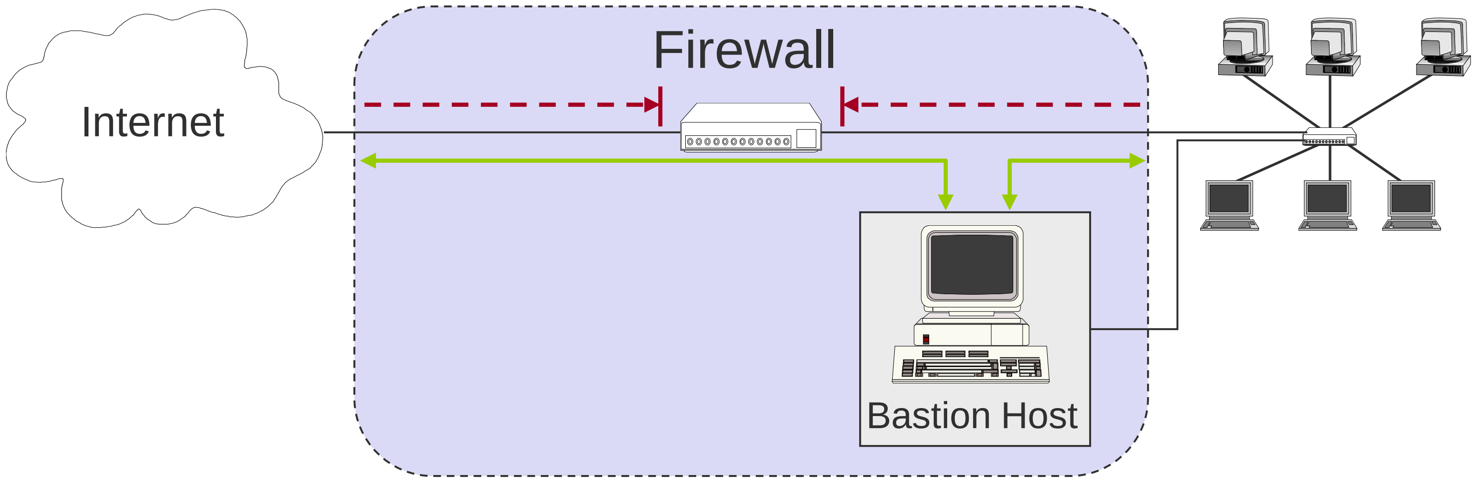
Firewall Architecture: Screened Host

Packet filter ...

- allows permitted IP traffic between screened host and the Internet
- blocks all direct traffic between other internal hosts and the Internet

Screened host provides proxy services

➢ Despite partial protection by packet filter, screened host acts as bastion host



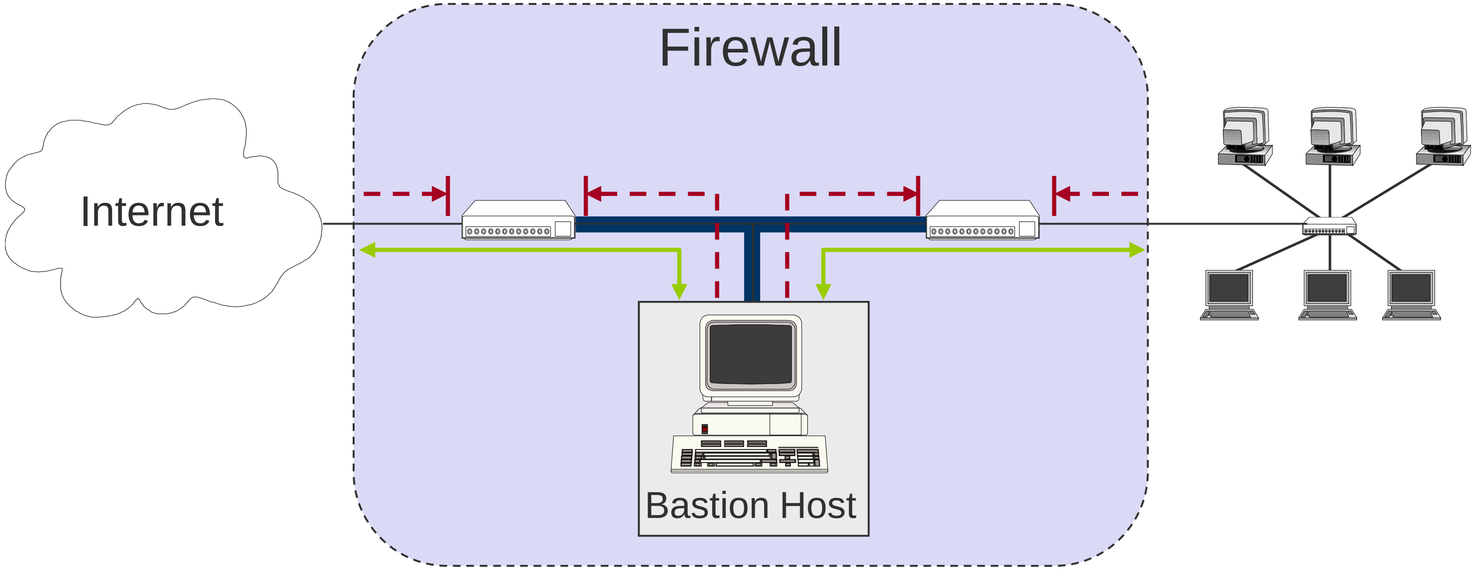
Firewall Architecture: Screened Subnet

DMZ between two packet filters

Inner packet filter serves as additional protection in case bastion host is compromised

- Avoids that compromised bastion host sniffs internal traffic

Perimeter network is also a good place to host publicly accessible information server, e.g. a WWW server



Firewalls: Packet Filtering

What can be done with packet filtering?

- Theoretically speaking “everything”
  - All information exchanged in a communication relation is transported via packets
- In practice, efficiency tradeoffs against proxy approaches have to be considered
  - Deep packet inspection is expensive; comes at cost of routing efficiency (but can be done!)

Basic packet filtering allows to control data transfers based on:

- Source/destination IP address
- Transport protocol
- Source / destination application port
- Specific protocol flags:
  - No TCP SYNs from exterior network
  - No TCP SYN/ACKs from exterior network, unless prior and related SYN from interior network (stateful packet filtering)
- Network interface a packet has been received on

Example: Packet Filtering Rule Set

This rule set specifies that incoming and outgoing email is the only allowed traffic into and out of a protected network:

- Email is relayed between two servers by transferring it to an SMTP daemon on the target server (server port 25, client port > 1023)
- Rule A allows incoming email to flow to the bastion host and rule B allows the bastion host's acknowledgements to exit the network
- Rules C and D are analogous for outgoing email
- Rule E denies all other traffic

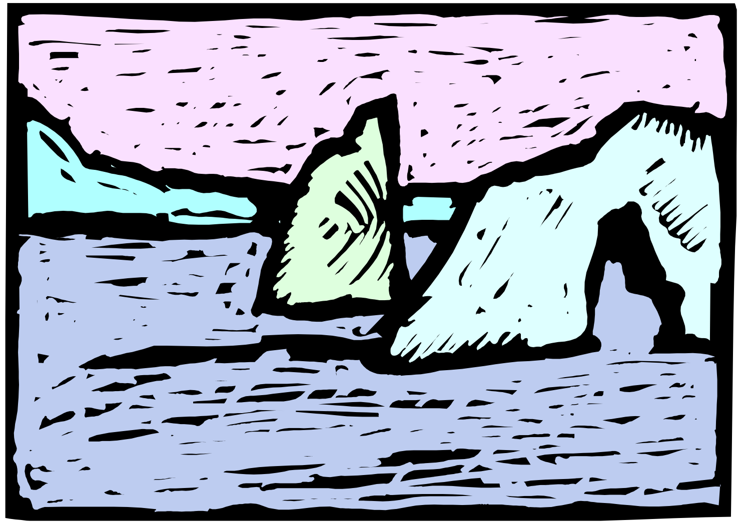
Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Bastion	TCP	>1023	25	Any	Permit
B	Outbound	Bastion	External	TCP	25	>1023	Yes	Permit
C	Outbound	Bastion	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Bastion	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

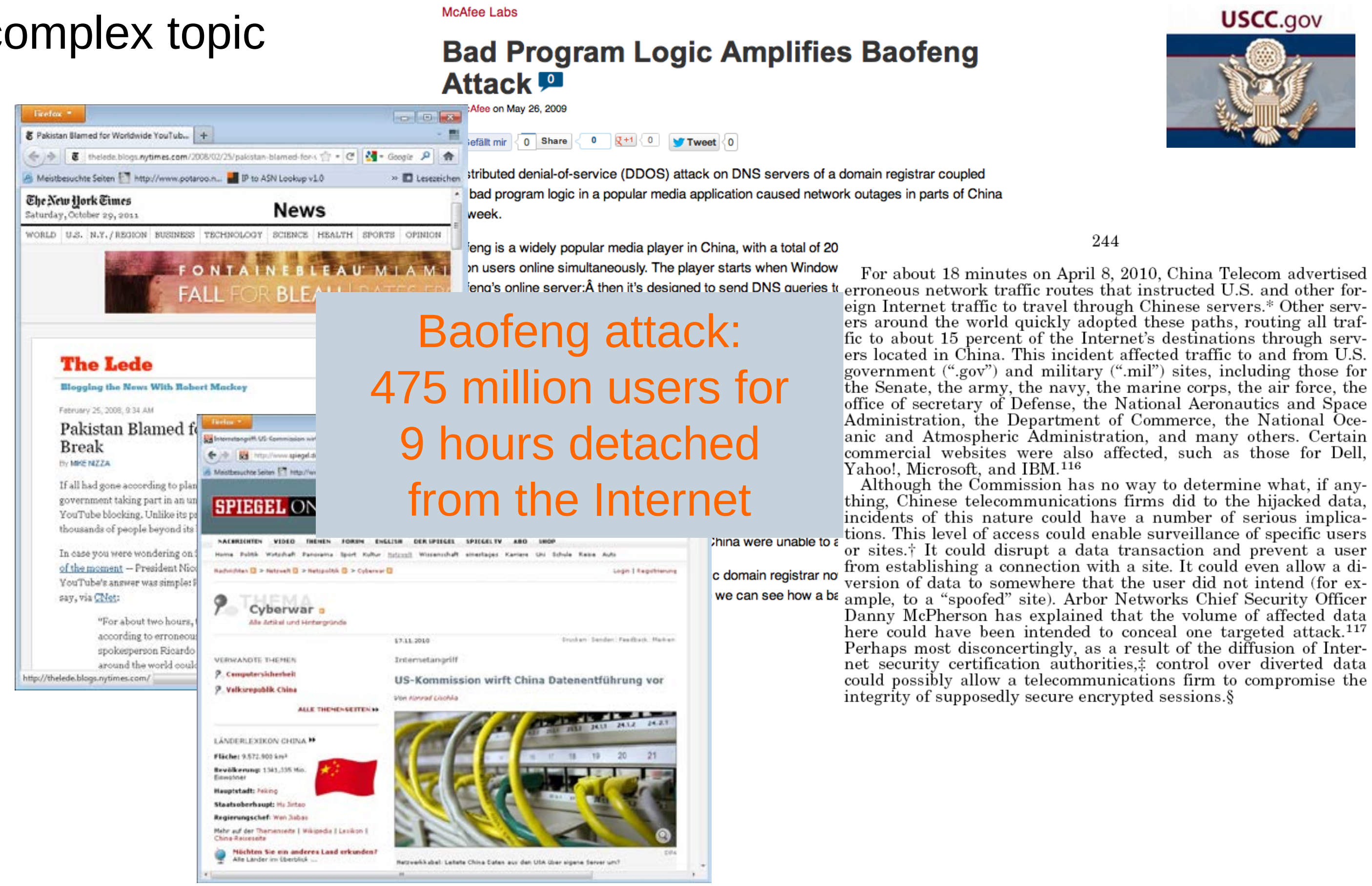
Conclusion

Network security is an important, but extremely complex topic

Unfair by definition:

- Attacker only needs to find one hole
- Defender must close all holes





Baofeng attack:
475 million users for
9 hours detached
from the Internet

We have not even scratched the surface, we just know that there is an iceberg out there…

Content

8. Networked Computer & Internet

9. Host-to-Network

10. Internetworking

11. Transport Layer

12. Applications

13. Network Security

14. Example

Questions & Tasks

- On which layers can a firewall operate?
- What is the idea of a DMZ?
- What is packet filtering? What does deep packet inspection mean?
- Where is your firewall at home? Check the settings!
- Why do we have cyber security problems at all?