VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE | DEPARTMENT OF COMPUTER SCIENCE

Basics of Computer Networks Security

Computer Networks
Lecture 7

The Process of Securing Computer Network (1)

- Security is not about installing a „big security box“, but about definition of a process of secure usage of the network and its enforcement
  - Incorporates company's security policy
    - that should include penalties for violation of the security rules
- Security rules are always restricting to the users
  - It is necessary to find a compromise between users' comfort and network security

The Process of Securing Computer Network (2)

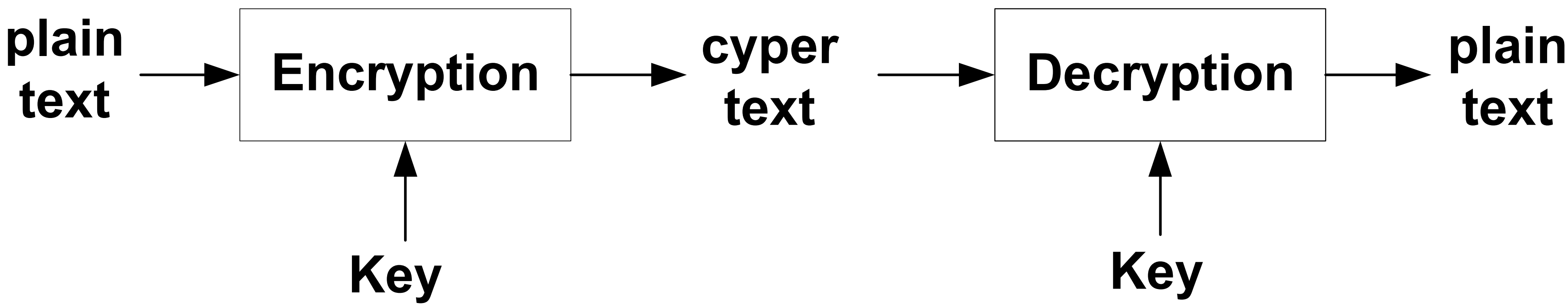
- Covers both the network infrastructure and OS of the user stations
  - Including protection against viruses
    - Infected stations may attack to the network infrastructure

Basic Terminology and Mechanisms of Network Security and Cryptography

Authentication and Encryption

- Confidentiality
  - unauthorized listener cannot understand data meaning
  - implemented by encryption
- Data Integrity
  - verification that data were not modified during transport
- Availability
  - the information must be available when it is needed.
- Non-repudiation
  - data source cannot repudiate that it sent particular piece of data
    - (i.e. it signed it)
- Authentication
  - verification of data sender identity

General Cryptographic System



Implementation options

- Conceal encryption/decryption algorithm
  - If the algorithm is revealed, implementation is useless
- Conceal keys
  - Keys used to parameterize (known) algorithm
  - Enough possible keys have to be available

Symmetric Cryptosystem

Properties of Symmetric Cryptosystem

- Shared secret key
- Effective algorithm implementations
    - speed, relative simplicity
    - possible to implement in hardware
    - DES, 3DES, AES, …
- Problem with secure secret key distribution

Authentication in Symmetric Cryptosystem

- Sender encrypts username using shared key, receiver decrypts using the same key and tests username validity
  - Requires database of valid usernames
- Alternative validity check implementation:
  - Sender appends username hash behind username, then encrypts whole block with shared key
  - Receiver decrypts [username+hash] with shared key, computes username hash and compares with received hash
  - Does not require to maintain username database

Combines authentication with data integrity check

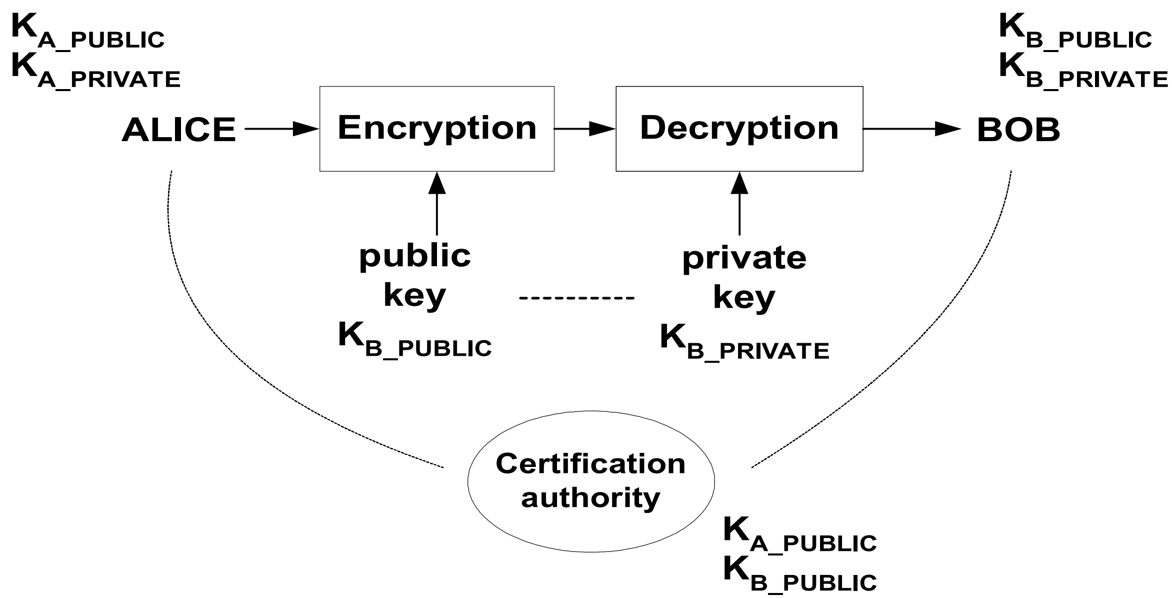
Data Integrity Check Implementation

- [message+shared secret key]->hash
- message+hash is sent
- receiver appends shared secret key behind received message, calculates hash by itself and compares with received hash

Combines origin authentication and data integrity check

Asymmetric Cryptosystem

Public and Private Keys



- Keys generated as pair – public and private key
- One key of pair used for encryption, second one for decryption
  - no matter which one for what
  - uses identical or complementary algorithms for encryption and decryption

Features of Asymmetric Cryptosystem

- More calculations comparing to symmetric algorithm => slower
  - RSA, El-Gammal
- Problem of secure public key distribution
  - no need to conceal them, but we need a mechanism to protect public keys against modification during transport
  - certification authority digitally signs public keys packed together with owner information
    - (so called “certificates”)

Usages of Asymmetric Cryptosystem

- Digital signatures
  - No problem with secret key distribution
- Exchange of keys for symmetric system
  - Often generated dynamically keys with limited lifetime

Certification Authority (1)

- Trusted entity
- Digitally signs public keys packed together with owner information - **certificates**
- First contact with CA must be personal
  - obtaining of private+public key pair
    - private key + signed certificate (better to just give CA publ.)
- There are ways how to deliver encrypted private key + certificate (containing signed public key) without physical contact from the CA
  - need to authenticate certificate request
  - uses password pre-negotiated between user and CA to encrypt private key and certificate before sending it to user
    - usage of LDAP password etc.
  - private+public key generation may take place in client OS
    - Only client keeps private key and sends public key for signing to CA using HTTPS

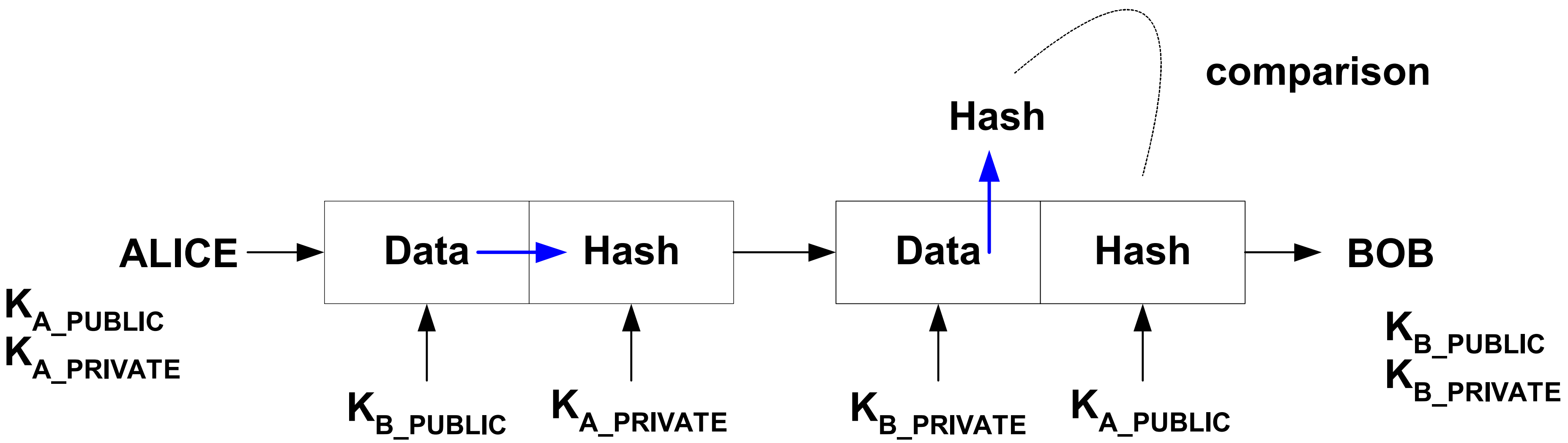
Certification Authority (2)

- Public key of CA needed by communicating parties to verify certificates of other communicating peers

- Public key of CA has to be inserted into every system by some trustworthy manner
  - built-in into OS/WWW browser installation files, …

Advantage: only one public key (CA certificate) has to be pre-configured manually

Authentication and Data Integrity Check in Asymmetric System



Options of Securing the Data Transferred over the Network

Security on Individual Layers of OSI-RM

- L2
  - hop-by-hop, inefficient
- L3
  - Independent both on the network topology and the application
  - IPSec
- L4
  - Transport Layer Security (TLS) - only for TCP
    - Equivalents for UDP exists
- L7
  - Security solved by particular applications
  - e.g. S/MIME

Traffic Filtering

- Stateless (packet filters)
  - Decides whether individual packet will be passed through or discarded
  - Decision made only based on data contained in the packet
  - Problem with inspection of L4+ in case of fragmented packets
- Stateful (transparent or proxy server)
  - Reconstructs and inspects data flows
  - Needs to maintain state for each flows
    - Limited scalability

Packet Filtering

Access Control Lists – ACL

- Applied most often on router interfaces
  - sometimes also on switch interfaces
- Filters traffic coming to or going out of the interface
- Packets/frames are filtered according to L3 and L4 header information
  - Sometimes also according to L2 headers fields

ACL Definition

- ACL is a sequence of entries that permit or deny traffic that matches criteria defined for a given entry
- ACL is looked up sequentially (top-down) until an entry that matches the inspected packet is found
  - The packet is passed through or discarded according to the action specified by the entry
  - After a match is found, the following ACL entries are ignored
- If no matching entry is found, the packet is implicitly denied
  - any traffic not listed in ACL is implicitly denied

How to Implement Packet Filtering using ACL

Network administrator needs to define

- The interface on which the ACL will be applied
  - A separate ACL for every interface may be defined
- The direction of traffic to be filtered by ACL
  - One inbound and at one outbound ACL may be assigned to the interface
- Criteria to pass/deny traffic through the ACL (ACL entries)

ACL – The Common Mistake

It is necessary not to forget to permit the returning traffic

- Normally, we need to create “hole” in ACLs that filter the ingoing and outgoing traffic
- Numbers of the source and destination port have to be swapped for the returning traffic

Implementation Example: Usage of ACLs on Cisco IOS

Syntax of ACL Entry Definition

**access-list <acl_number> {permit | deny}
<PROTOCOL>
<source-IP-addr> <source-addr-wildcard>
[<source-port>] <destination-IP-addr>
<destination-addr-wildcard> [<destination-port>]
[protocol-dependent-options]**

- Wildcard mask defines which bits will be compared
  - 0=must match, 1=don't care
  - May be treated as an inverted subnet mask

Example of ACL Definition (1)

```
Entries of ACL #101:
access-list 101 permit udp 200.1.1.100
  0.0.0.0 eq 53 158.196.135.0 0.0.0.255
```

- **Permit UDP from port 200.1.1.100/32:53 to network 158.196.135.0/24**

```
access-list 101 permit icmp 0.0.0.0
  255.255.255.255 158.196.135.0 0.0.0.255
  echo-reply
```

- **Permit ICMP Echo Reply from anywhere to network 158.196.135.0/24**

```
access-list 101 deny ip 100.1.1.0 0.0.0.255
  158.196.135.0 0.0.0.255
```

- **Deny IP (and thus all protocols carried in IP packets) from network 100.1.1.0/24 to network 158.196.135.0/24**

Example of ACL Definition (2)

```
access-list 101 permit tcp 0.0.0.0
  255.255.255.255 eq 80 158.196.135.101 0.0.0.0
  established
```

- **Permit TCP from anywhere from source port 80 to machine 158.196.135.101, but only already existing connections (discards TCP segments with SYN=1, `ACK`=0**

Syntactic Shortcuts

- any
  - = any IP address
  - + wildcard mask 255.255.255.255
- host X.X.X.X
  - = IP address X.X.X.X + wildcard mask 0.0.0.0

Example

```
permit tcp host 158.196.100.100 any eq 80
```

Assigning of ACL to an Interface

```
interface s0
 ip access-group 101 in
```

- Assigns an a particular ACL to an interface
  - in = filters inbound traffic (coming to the router)
  - out = filters outgoing traffic (going out of the router)

Time-based ACLs

- Individual ACL entries(permit/deny) may be valid only during specified time intervals
- Usage example:
  - Disallow Internet browsing during working hours

Reflective ACLs

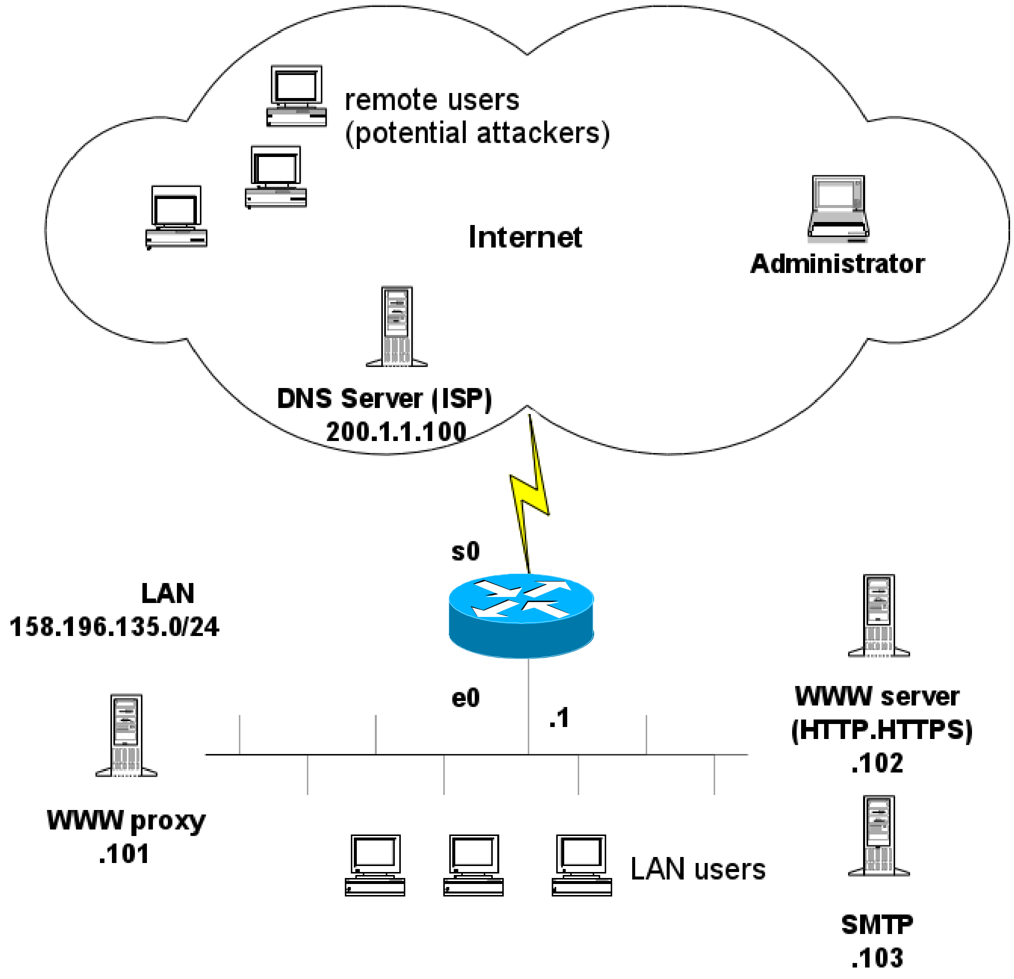
- Automatically permits inbound traffic that matches the allowed outbound traffic
  - Allowed outgoing traffic is defined manually (by ACL for outgoing direction)
  - The ACL for incoming traffic implicitly denies everything
  - When a traffic is permitted by ACL in the outgoing direction, the corresponding „permit“ entry is automatically created for the returning traffic in the inbound ACL
    - source and destination addresses/ports will be swapped
- The ACL entry for returning traffic is valid only during the existence of outgoing traffic flow
  - until the TCP connection is closed (FIN/RST) or inactivity timeout expires for UDP sessions

Steps to Implement Packet Filtering in the Network

- Analyze the applications
  - What applications do we support in our network ?
  - What protocol and which ports are used by protocol of each application ?
    - Does the application use dynamic ports ?
- Decide the interface to apply the ACL
  - Typically we use one ACL for incoming and (different) one for outgoing traffic
  - It is desirable to avoid routing of packets that will be discarded due on the outgoing interface
- Define entries of individual ACLs
  - Don't forget to permit the returning traffic !

ACL Case Study

The Example Scenario



Network Services Requirements

- The company operates its own SMTP server (158.196.135.103) accessible from the Internet.
- The company operates its own WWW server (158.196.135.102) accessible from the Internet using both HTTP and HTTPS.
- Local clients access WWW servers on the Internet (HTTP/HTTPS) through proxy server on 158.196.135.101.
- The clients on the corporate LAN may only open SSH connections to the Internet.
- DNS servers that performs recursive lookup for all clients of the corporate LAN is operated by ISP on 200.1.1.100.
- Clients on corporate LAN may ping machines on the Internet, but the opposite direction is prohibited
- The remote administration may access the corporate WWW server from anywhere in the Internet using SSH

The traffic not listed explicitly here is prohibited

Analysis of Applications

Service (L7 protocol)	L3/L4 protocol	Port
HTTP	TCP	80
HTTPS	TCP	443
SMTP	TCP	25
DNS	UDP	53
-	ICMP	Echo Request & Echo Reply messages

None of the required applications use the dynamically assigned ports

Specification of Interfaces to apply ACLs on

ACL ID	Interface	Direction
101	s0	in
102	e0	in

- The traffic coming from the Internet to the s0 interface will be filtered by ACL 101 before it will be routed
- The traffic coming from the corporate network to e0 interface will be filtered by ACL 102 before it will be routed

Entries of ACL 101 (s0, in)

Order	Permit/ deny	L3/4 Prot.	Source IP	Source port	Destination IP	Dest. port
1	D	IP	158.196.135.0/24		*	
2	P	TCP	*	*	158.196.135.103	25
3	P	TCP	*	*	158.196.135.102	80
4	P	TCP	*	*	158.196.135.102	443
5	P	TCP	*	*	158.196.135.102	22
6	P	UDP	200.1.1.100	53	158.196.135.0/24	*
7	P	ICMP	*		158.196.135.0/24	E. reply+
8	P	TCP	*	80	158.196.135.101	*
9	P	TCP	*	443	158.196.135.101	*
10	P	TCP	*	22	158.196.135.0/24	*
11	D	IP	*		*	

Note:
Echo Reply is a specification of ICMP message type, not the port number (placed to destination port column just to save space)

Entries of ACL 102 (e0, in)

Order	Permit/ deny	L3/L4 prot.	Source IP	SRC port	Destination IP	DST port
1	P	TCP	158.196.135.101	*	*	80
2	P	TCP	158.196.135.101	*	*	443
3	P	TCP	158.196.135.0/24	*	*	22
4	P	UDP	158.196.135.0/24	*	200.1.1.100	53
5	P	ICMP	158.196.135.0/24		*	E. request+
6	P	TCP	158.196.135.103	25	*	*
7	P	TCP	158.196.135.102	80	*	*
8	P	TCP	158.196.135.102	443	*	*
9	P	TCP	158.196.135.102	22	*	*
10	D	IP	*		*	

Note:
Echo Request is a specification of ICMP message type, not the port number (placed to destination port column just to save space)

Configuration and Application of ACL 101 in Cisco IOS

```
access-list 101 deny ip 158.196.135.0 0.0.0.255 any
access-list 101 permit tcp any  host 158.196.135.103 eq 25
access-list 101 permit tcp any  host 158.196.135.102 eq 80
access-list 101 permit tcp any  host 158.196.135.102 eq 443
access-list 101 permit tcp any  host 158.196.135.102 eq 22
access-list 101 permit udp host 200.1.1.100 eq 53 158.196.135.0 0.0.0.255
access-list 101 permit icmp any 158.196.135.0 0.0.0.255 echo-reply
access-list 101 permit tcp any eq 80 host 158.196.135.101 established
access-list 101 permit tcp any eq 443 host 158.196.135.101 established
access-list 101 permit tcp any eq 22 158.196.135.101 0.0.0.255 established

interface s0
 ip access-group 101 in
```

Configuration and Application of ACL 101 in Cisco IOS

```
access-list 102 permit tcp host 158.196.135.101 any eq 80
access-list 102 permit tcp host 158.196.135.101 any eq 443
access-list 102 permit tcp 158.196.135.0 0.0.0.255 any eq 22
access-list 102 permit udp 158.196.135.0 0.0.0.255 host 200.1.1.100 eq 53
access-list 102 permit icmp 158.196.135.0 0.0.0.255 any echo
access-list 102 permit tcp host 158.196.135.103 eq 25 any established
access-list 102 permit tcp host 158.196.135.102 eq 80 any established
access-list 102 permit tcp host 158.196.135.102 eq 443 any established
access-list 102 permit tcp host 158.196.135.102 eq 22 any established

interface e0
 ip access-group 102 in
```

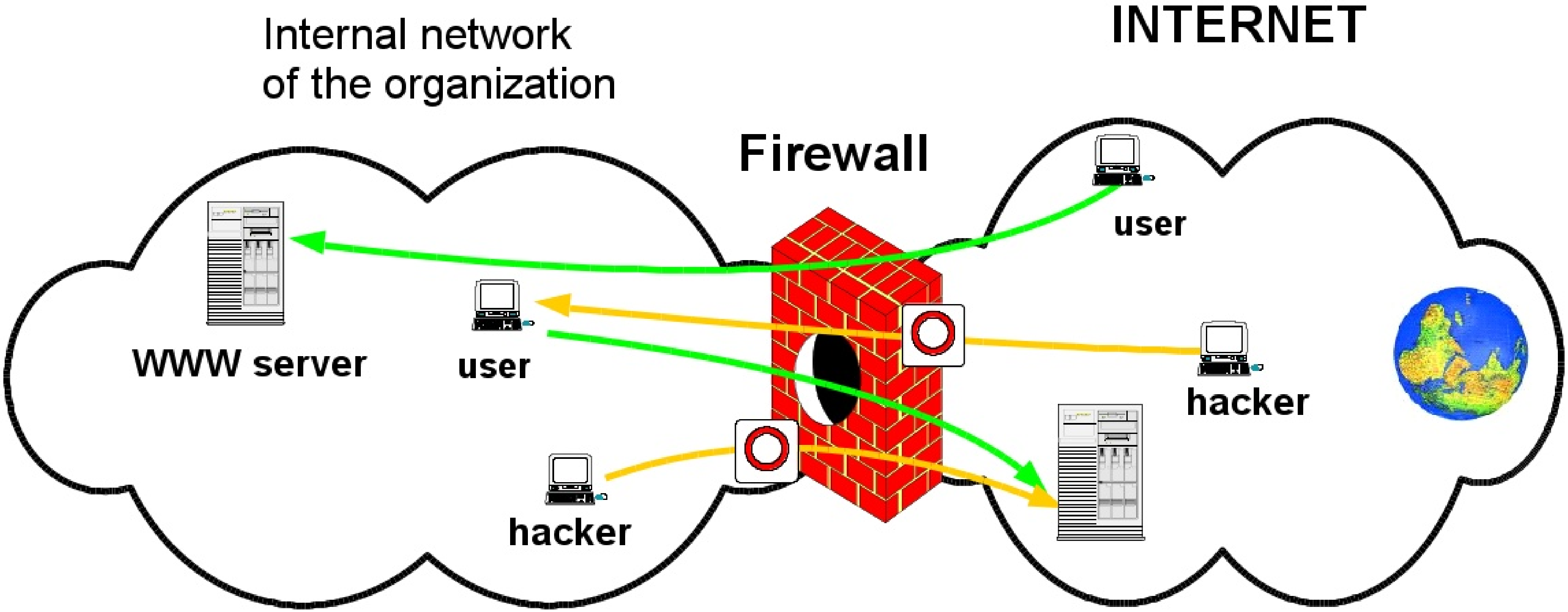
Stateful Traffic Inspection

Firewalls

Separate the trusted (internal) an untrusted (external) network

- Sometimes also attaches the the Demilitarized Zone (DMZ)
  - DMZ contains server exposed to the external network
    - „bastion hosts“ servers with well-secured OS
    - Mutual communication between DMZ servers and from DMZ servers to internal network is limited
  - Hosts on the internal network are not accessible from the external network

Operation of the Firewall



Firewall Types

- Transparent to the permitted traffic
  - behaves as router or bridge
- Proxy server(s) for various L7 protocols

Implementations of Stateful Firewalls

- Hardware-based
  - e.g. Cisco PIX/ASA, Juniper firewall, …
  - Details of internal OS implementation are not published
    - considered more secure by some people
- Software-based
  - Linux – iptables
    - limited support for stateleful filtering
  - NetBSD
    - very flexible, easily-readable config files
  - Checkpoint, …

Context-Based Access Control:
Cisco IOS with Firewall Feature Set

- Inspect the control channel of selected application protocols and opens dynamic ports for data channels accordingly (FTP, IP telephony, …)
  - Opens temporary holes in the inbound ACL for returning traffic that corresponds to a session initiated from the internal network
  - For unknown application protocols works with TCP/UDP session as the reflective ACL
- May also detect some known attacks (SYN flood, suspicious TCP sequence numbers, ...)
- May also handle/reset half-open connections

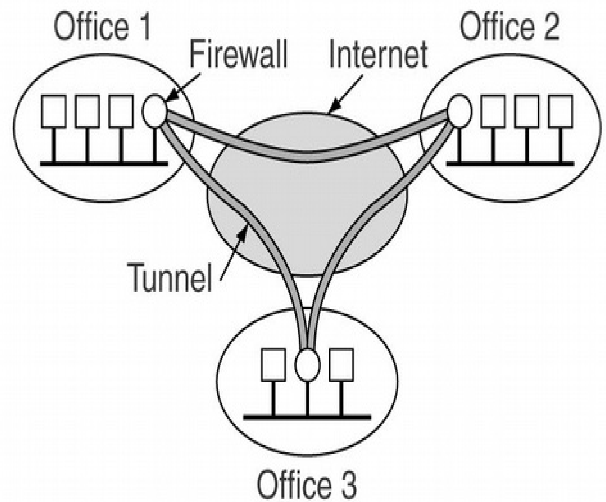
Network Security and NAT

Advantages of NAT for Securing the Network

- Hides the internal structure of the network
  - Only single address or a limited number of addresses are exposed
- Dynamic NAT
  - Inbound traffic is allowed only during the existence of the session initiated from the inside network
  - The same station is visible from the outside networks under different addresses during the time

Virtual Private Networks (VPN)

What is VPN ?



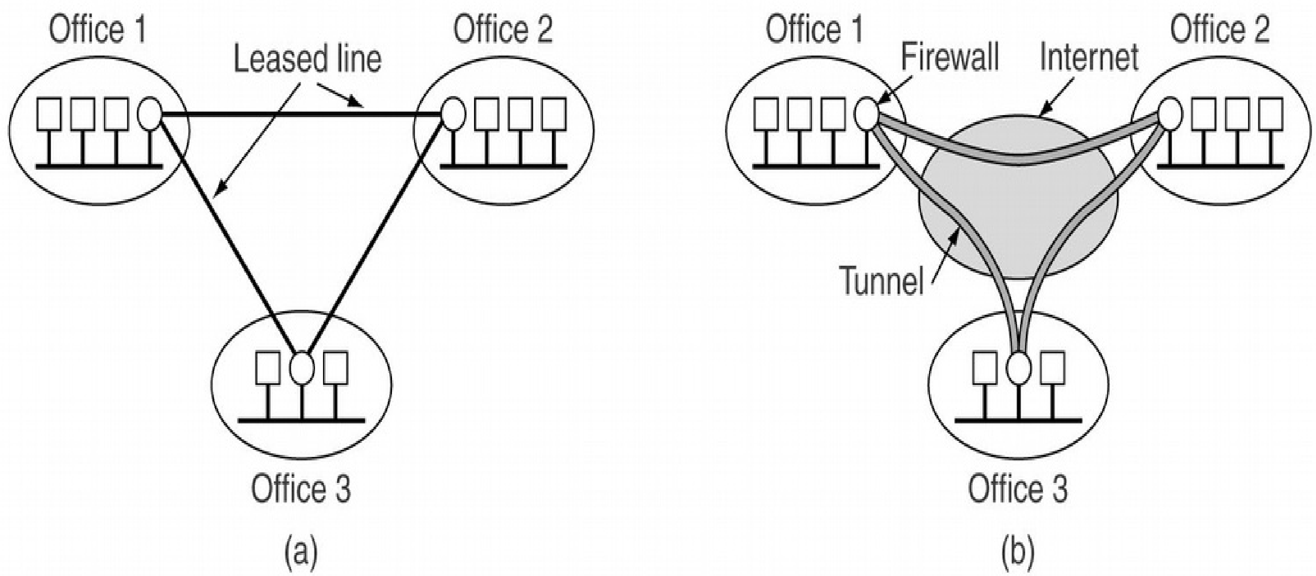
(b)

- VPN allow to build private WANs using public shared infrastructure with the same level of security and configuration options as with private infrastructure
- Uses tunneling and encryption methods
  - including authentication

Tunnel

- Virtual point-to-point connection over shared infrastructure
  - often authenticated and encrypted
- Carries packets of some protocol encapsulated in another protocol
  - sometimes in the same protocol (IP over IP)
  - tunnel can carry layer 2 frames also
  - allows other protocols to be carried over IP network
    - (even non-routable protocols such as NetBEUI etc.)

Comparison of VPN with Private Infrastructure



Advantages of VPNs over Physical Private WAN Infrastructure

- Lower cost
- Flexibility of (virtual) topology
  - topology defined purely by configuration
- No WAN link maintenance and management needed
  - provider (ISP) takes responsibility of infrastructure

No special contract with infrastructure provider is needed (we only need that ISP does not filter tunneling protocols)

Most Common VPN Implementation Options

Internetwork-wide VPNs → tunnels at or above layer 3

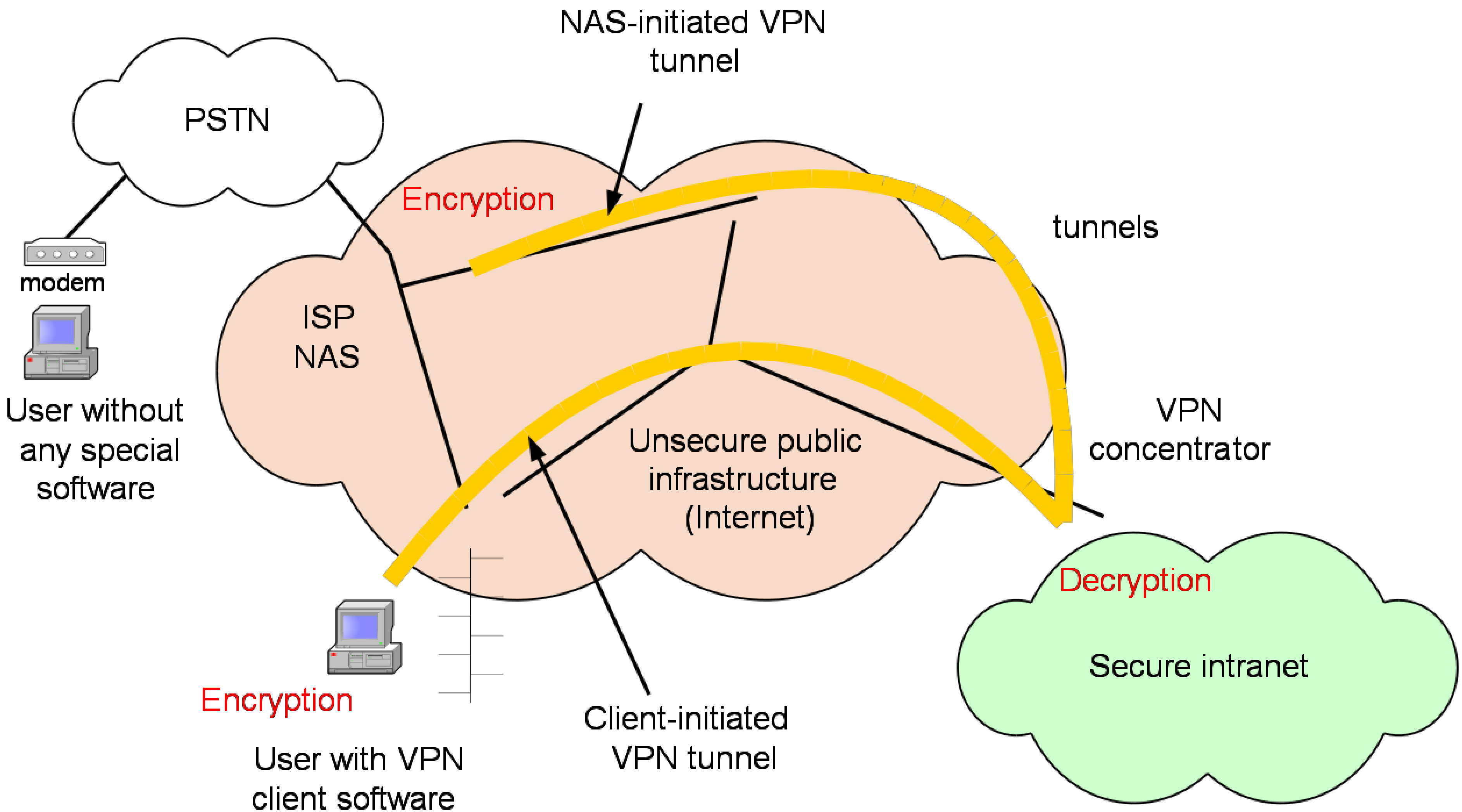
- Layer 3 VPN – IPSec
  - media independent (above hop-by-hop L2 security)
  - application independent
  - connectionless security
- Layer 4 VPN – commonly use SSL
  - but what to do with connectionless service (UDP) ?
- Layer 7 VPN – application level (WWW)

Most Common VPN Implementation Options

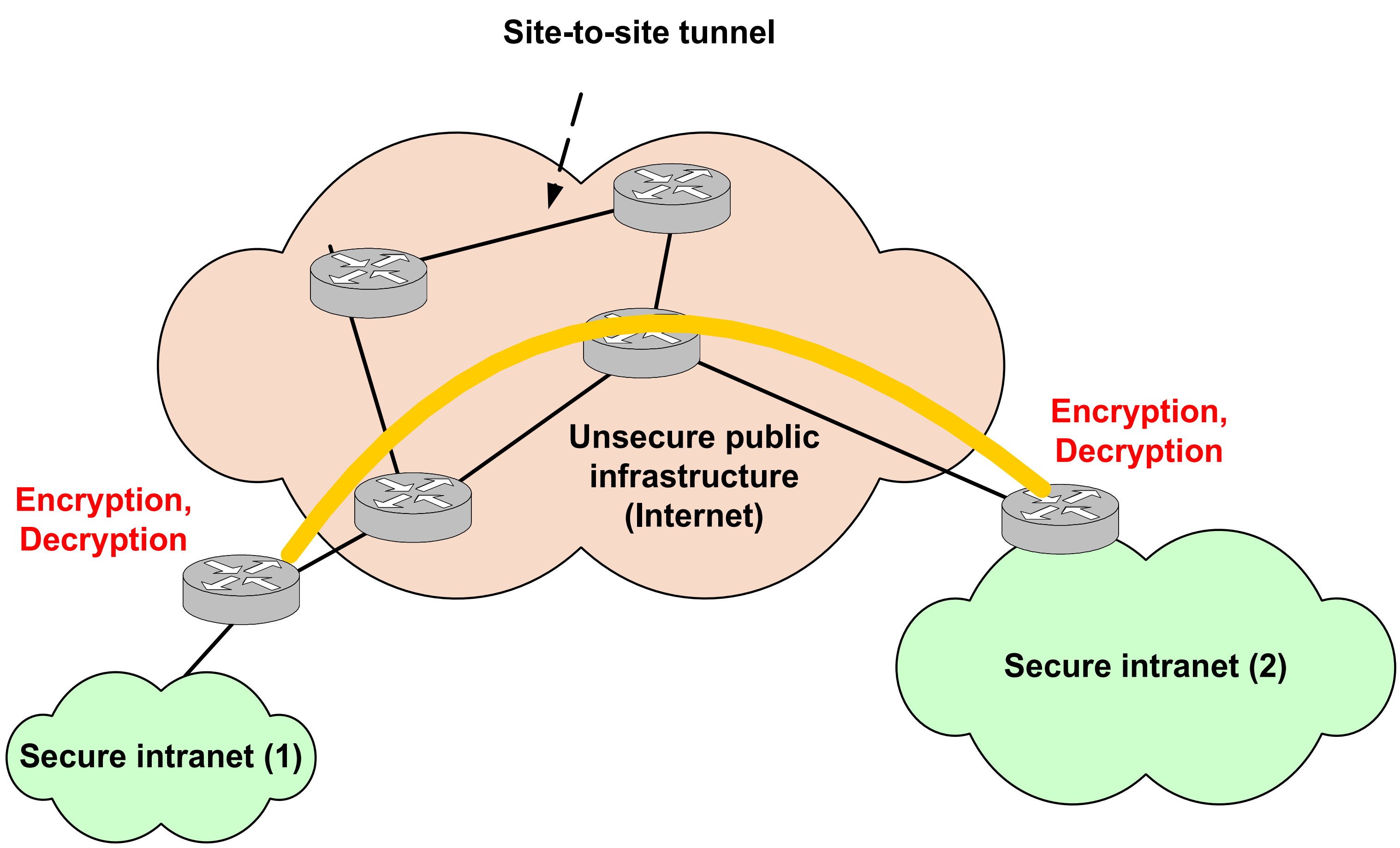
- Router-to-router (firewall)
  - Site-to-site VPNs
  - Single router may terminate multiple tunnels

- Remote User to VPN concentrator
  - Remote access VPNs
  - user has to have special encryption software installed (VPN client)

Remote Access VPN



Site-to-Site VPN



IPSec:
A Layer 3 VPN Implementation

- General architecture for implementation of dynamically negotiated VPN tunnels
- Provides authentication, data integrity and encryption
- General framework independent on utilized cryptographic algorithms
  - Algorithms are negotiated during tunnel establishment
    - Security Association with limited lifetime
- Only for IP (unicast) traffic
  - But other protocols and multicast traffic may be encapsulated into IP prior sending to the tunnel

Security of Selected LAN and WAN Technologies

ARP Security

- Fake ARP replies by attacking stations
  - forging of the default GW
- ARP requests with fake IP-to-MAC binding may be generated
  - and placed to ARP caches of all receiving stations
- May be solved by static records in the ARP cache

Security of Routing Protocol

Protection mechanism against fake routing information:

- Authentication of routing information sources (neighbors)
  - RIPv2, OSPF, EIGRP, BGP
  - Plain text password or MD5 hashes
- Filtering sources of the routing information by ACL
- Filtering of received and propagated routes

Security in Switched Networks

- Explicit list of MAC addresses allowed on the port
- Limitation of number of dynamic MAC addresses on the port
  - Protects against source-spoof DoS
    - The principle is to overfill the whole MAC address table that causes removal of regular entries (LRU) and frame flooding
- Filtering using ACLs on L2 ports
  - source/destination MAC address, sometimes L3/L4 info
- VLAN ACLs
- Restriction of mutual communication between clients ports
  - Traffic may pass to server and backbone ports
  - Avoids peer-to-peer communication (games etc.)

DNS Security

DNS replies may be forged

- Fake mapping of domain names to IP addresses
- Fake MX and SRV records

- Modification of the reply on the way
  - Man-in-the-middle attack
- Generating of (a fake) non-authoritative additional information
  - Most of DNS resolvers updates cache accordingly without further checking

A proposed solution: DNSSec

Protection of Spanning Tree

- BPDU Guard
  - filter eventual BPDUs from ports where clients stations are expected
- Root Guard
  - Does not allow the unauthorized device to become Spanning Tree root

Securing of Network Devices' Management

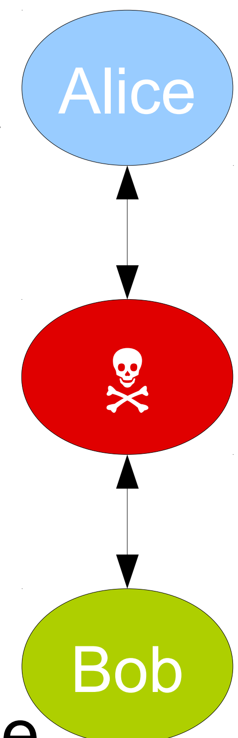
- Secure administrator's password
  - Telnet, SSH, WWW, SNMP - RO/RW communities
- Idle timeout for inactive administrator sessions
- Explicit listing of permitted management stations (ACL)
- Separate management VLAN

Securing of the physical access to the network devices must not be underestimated

Network Attacks

Man-in-the-Middle

- Listens to A & B communication in both directions A → B a B → A (the traffic may be redirected instead of the attacker being between A & B)
- The direct channel between A & B is broken for each side it emulates the second partner
  - may just listen but also change the data
- Results:
  - Hard to detect for unencrypted communication
  - May force weaker authentication
  - If the attacker provides a “reputable” identity when impersonating second side (e.g. CA whose root CA is trusted), encrypted channel may be attacked as well.



Denial of Service (DoS) Attacks

- The aim of the attacker is to deplete victim servers' or network infrastructure's resources and bring the system down or modify its behavior
  - memory, CPU, bandwidth
- Traffic commonly sourced from fake source address(es) to get through the the filters
  - Source IP spoofing
- Very dangerous in distributed version (DDoS)
  - The administrator cannot react to the changes of the attacking traffic quickly enough

Examples of DoS Attacks

- TCP SYN flood
- ping flood or packets destined to non-existent network
  - Some routers allows to limit the rate of generated ICMP messages
    - ICMP Unreachables in this case
  - It may be efficient to forge the source address so that it also belongs to the destination network
- Non-authorized routing change
  - ICMP redirects, fake routing information

Intrusion Detection System (IDS) Intrusion Prevention System (IPS)

- Identifies suspicious communication patterns
  - operates on various OSI RM layers
- Classifies attack risks, informs network administrator (IDS) or automatically adapts filters (IPS)
  - Implementation of IPS brings a risk of false positives

Authentication and Authorization of Network Access

Accounting (Logging) of User Activities

Authorization of Network Users' Activities

- Users should be authenticated before allowing to access the network resources
- Users have to be authorized to use particular service
  - Users actions should be logged (Syslog)
- The same is valid for network administrators
- Centralized management of user account and user rights is desirable
  - RADIUS, TACACS, ...