b

UNIVERSITÄT
BERN

b
UNIVERSITÄT
BERN

Network Security

XII. Network Endpoint Security

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 16.05.2022 – 23.05.2022

Network Endpoint Security

Table of Contents

1. Firewalls
2. Intrusion Detection Systems
3. Malicious Software
4. Denial of Service Attacks
5. The Onion Routing

1. Firewalls

1. Introduction

- important complement to host-based security services such as intrusion detection systems.
- typically inserted between the premises network and the Internet to establish a controlled link and to build an outer security wall or perimeter.
- provides an additional layer of defense
- insulates internal systems from external networks or other parts of the internal network.

1. Firewalls

2. Design Goals

- All traffic in both directions must pass through the firewall.
  This is achieved by blocking all access to the local network except via the firewall.
- Only authorized traffic,
  as defined by the local security policy,
  will be allowed to pass.
- Firewall itself is immune to penetration.
  This implies the use of a hardened system with a secured operating system.
  Trusted computer systems are suitable for hosting a firewall.

1. Firewalls

3. Techniques

- **Service control**
  - determines the types of Internet services that can be accessed, inbound or outbound.
  - Firewall may
    - filter traffic on the basis of IP address, protocol, or port number.
    - provide proxy software that receives and interprets each service request
    - host the server software itself, such as a Web or mail service.
- **Direction control**
  - determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.
- **User control**
  - controls access to a service according to which user is attempting to access it.
  - typically applied to users inside the firewall perimeter (local users).
  - may also be applied to incoming traffic from external users; this requires some form of secure authentication, e.g., IPsec.
- **Behaviour control**
  - controls how particular services are used, e.g., firewall may filter email to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

1. Firewalls

4. Capabilities

Firewall

- defines a single choke point that keeps unauthorized users out of the protected network.
- prohibits potentially vulnerable services from entering or leaving the network.
- provides protection from various kinds of IP spoofing and routing attacks.
- simplifies security management because security capabilities are consolidated on a single system or set of systems.
- provides a location for monitoring security-related events. Audits and alarms can be implemented on firewall.
- is a convenient platform for several Internet functions that are not security related, e.g., Network Address Translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.
- can serve as the platform for implementing virtual private networks.

1. Firewalls

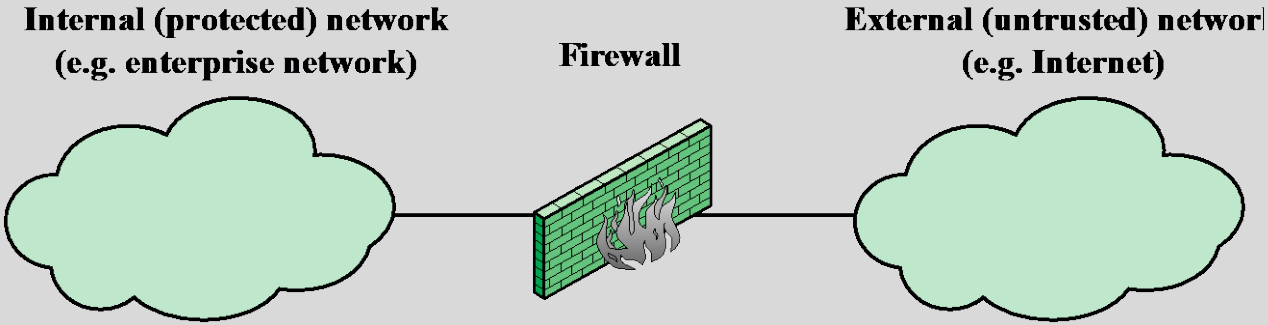
5. Limitations

Firewall

- cannot protect against attacks that bypass the firewall.
- may not protect fully against internal threats, such as a misbehaving employees
- An improperly secured wireless LAN may be accessed from outside the organization.
- Mobile devices may be used and infected outside the corporate network, and then connected and used internally.

1. Firewalls

6. General Model

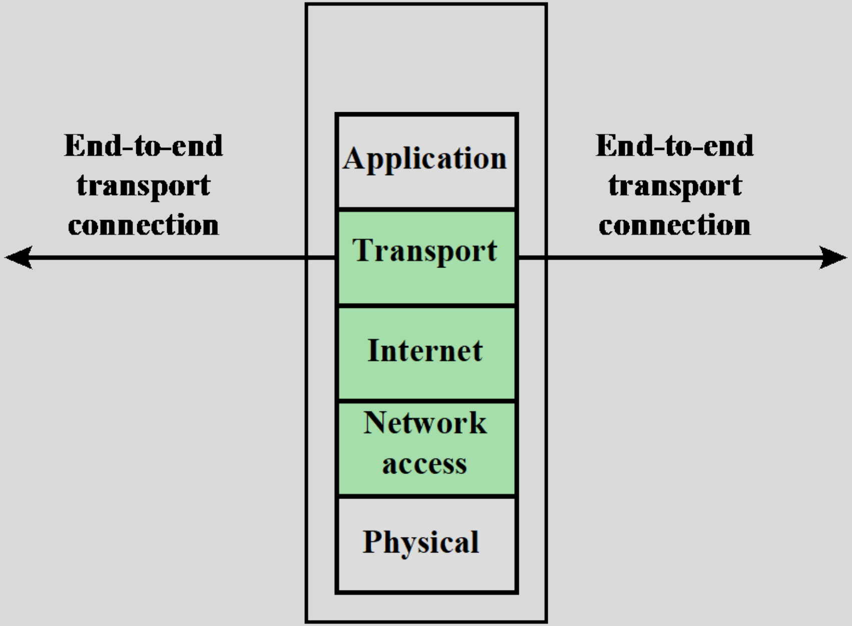

Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) networ
(e.g. Internet)

Types

- Packet Filtering Firewall
- Stateful Inspection Firewall
- Application Proxy Firewall
- Circuit-level Proxy Firewall

1. Firewalls

7.1 Packet Filtering Firewall


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

- Filtering Rules
  - Source and destination IP address
  - Source and destination transport-level address (port number)
  - IP protocol field
  - Interface
- List of rules based on matches to fields in the IP or TCP header; default: discard / forward

1. Firewalls

7.2 Packet Filtering Example

a) Inbound mail is allowed (port 25 is for SMTP incoming), but only to a gateway host. Packets from a particular external host, SPIGOT, are blocked.

b) explicit statement of the default policy

c) Any inside host can send mail to the outside. A TCP packet with a destination port of 25 is routed to the SMTP server on the destination machine. problem: use of port 25 for SMTP is only a default. An outside machine could be configured to have some other application linked to port 25.

d) addresses problem in c): Once a connection is set up, the ACK flag of a TCP segment is set to acknowledge segments sent from the other side. It allows IP packets where the source IP address is one of a list of designated internal hosts and the destination TCP port number is 25. It allows incoming packets with a source port number of 25 that include the ACK flag in the TCP segment.

e) Approach to handle FTP connections. FTP uses 2 TCP connections: a control and a data connection. Data connection uses a different port number dynamically assigned. Most servers use low-numbered ports; most outgoing calls tend to use a higher-numbered port > 1023. Thus, this rule set allows
   - Packets that originate internally
   - Reply packets to a connection initiated by an internal machine
   - Packets destined for a high-numbered port on an internal machine

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

1. Firewalls

7.3 Weaknesses

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.
- Logging functionality in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source/destination address, traffic type).
- Most packet filter firewalls do not support advanced user authentication schemes, mostly due to the lack of upper-layer functionality by firewall.
- Packet filter firewalls are generally vulnerable to attacks that take advantage of problems within the TCP/IP specification and protocol stack, such as *network layer address spoofing*. Many packet filter firewalls cannot detect a network packet in which IP addressing information has been altered.
- Due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

1. Firewalls

7.4 Attacks and Countermeasures

- **IP address spoofing**

  → discard packets with an inside source address if the packet arrives on an external interface.

- **Source routing attacks**
  - Source station specifies the route that a packet should take as it crosses the Internet, in the hope that this will bypass security measures that do not analyse source routing information.

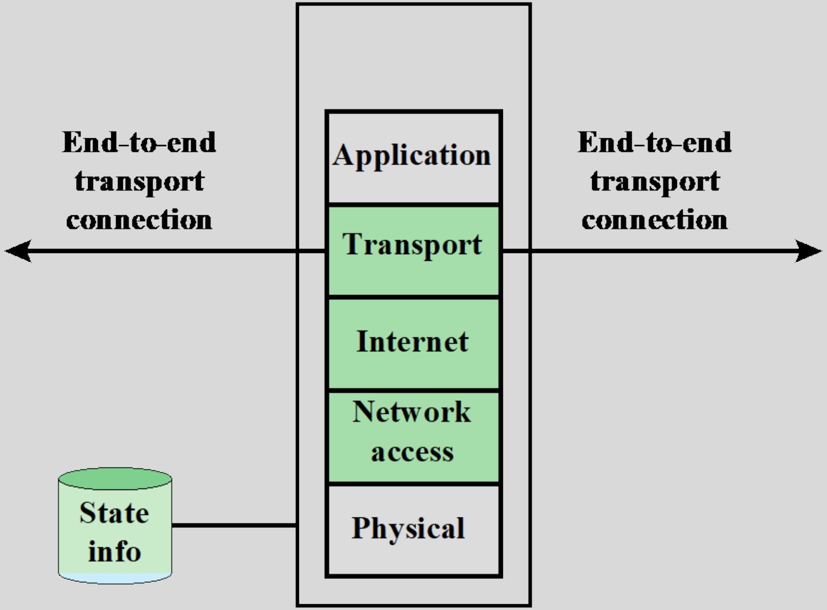
  → discard all packets using this option

- **Tiny fragment attacks:**
  - Attacker uses IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment.
  - This circumvents filtering rules that depend on TCP header information.
  - Attacker hopes that the filtering firewall examines only the first fragment and that the remaining fragments are passed through.

  → enforce a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header. If the first fragment is rejected, the filter can remember the packet and discard all subsequent fragments.

1. Firewalls

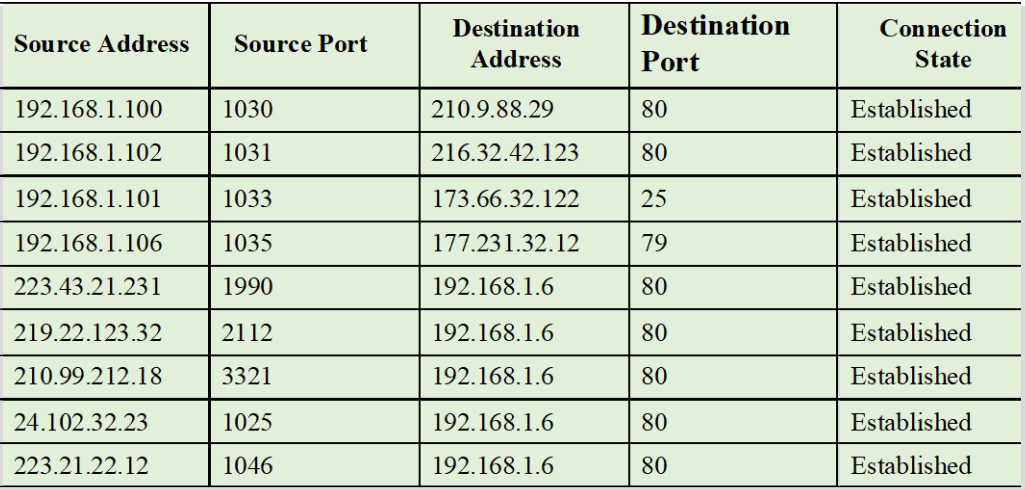
8.1 Stateful Inspection Firewall


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

- A traditional packet filter makes filtering decisions on an individual packet basis and does not consider any higher-layer context.
- Most applications that run on top of TCP follow a client/server model, e.g., SMTP. Typically, servers use lower-numbered well-known ports and clients use high-numbered ports.
- A simple packet filtering firewall must permit inbound network traffic on all high-numbered ports for TCP-based traffic to occur. This creates a vulnerability that can be exploited by unauthorized users.
- A stateful inspection packet firewall defines rules for TCP traffic by creating a directory of outbound TCP connections.

1. Firewalls

8.2 Example Stateful Firewall Connection State Table

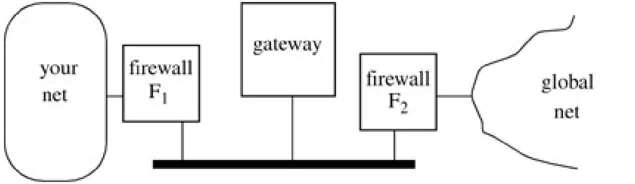


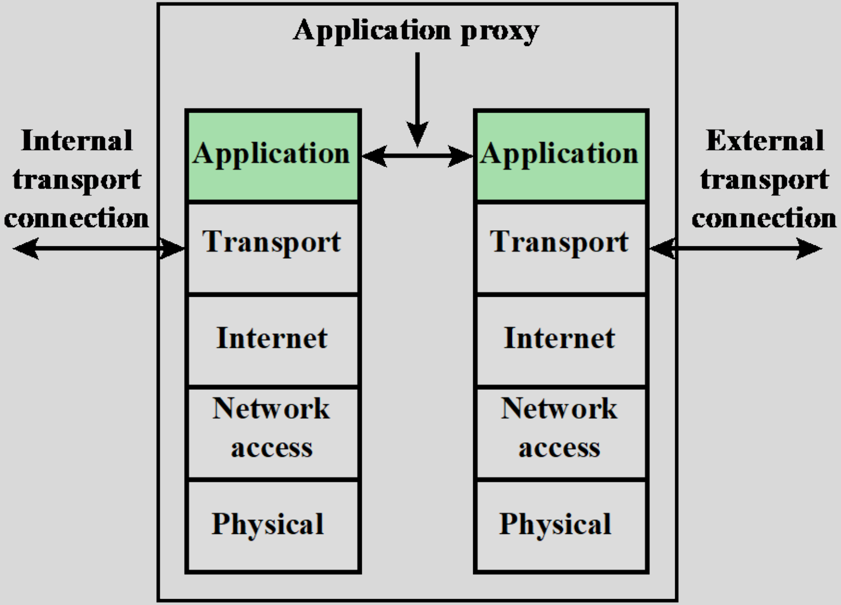
Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

- Table entries for each currently established connection.
- Packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory.
- Stateful packet inspection firewall reviews same packet information as a packet filtering firewall, but also records information about TCP connections.
- Some stateful firewalls keep track of TCP sequence numbers to prevent attacks that depend on the sequence number, e.g., session hijacking.
- Some inspect limited amounts of application data for some well-known protocols like FTP in order to identify and track related connections.

1. Firewalls

9. Application Proxy Firewalls

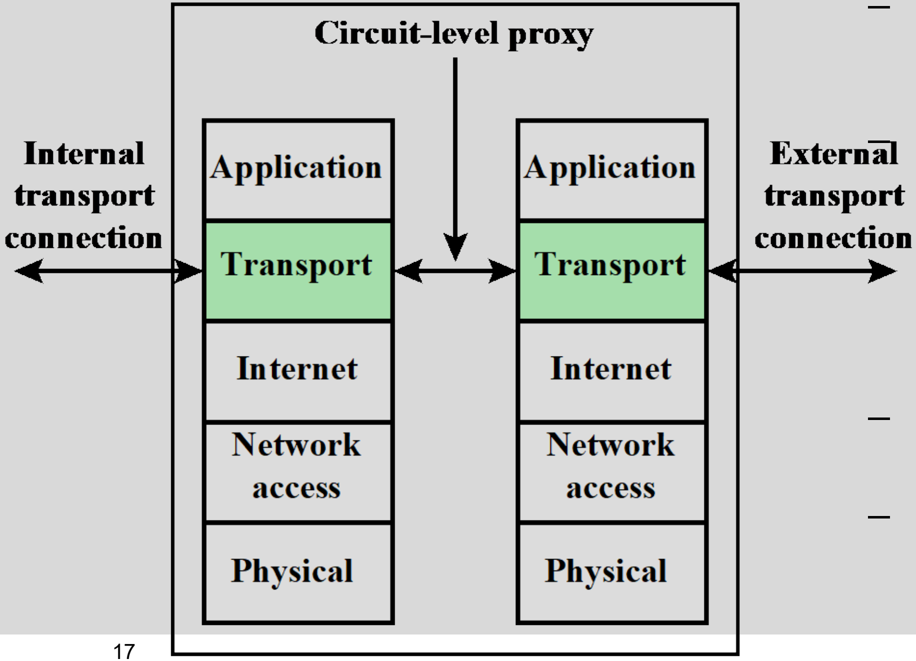




- An application-level gateway, also called application proxy acts as a relay of application-level traffic.
- User contacts gateway using an application, e.g., Telnet, FTP; gateway asks user for name of remote host to be accessed.
- When the user provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments with application data between the endpoints.
- If the gateway does not implement the proxy code for a specific application, the service is not supported.
- Advantages:
  - Approach tends to be more secure than packet filters.
  - Application-level gateway needs to check few applications.
- Disadvantages:
  - additional processing overhead on each connection
  - two spliced bi-directional connections

1. Firewalls

10. Circuit-level Proxy Firewall

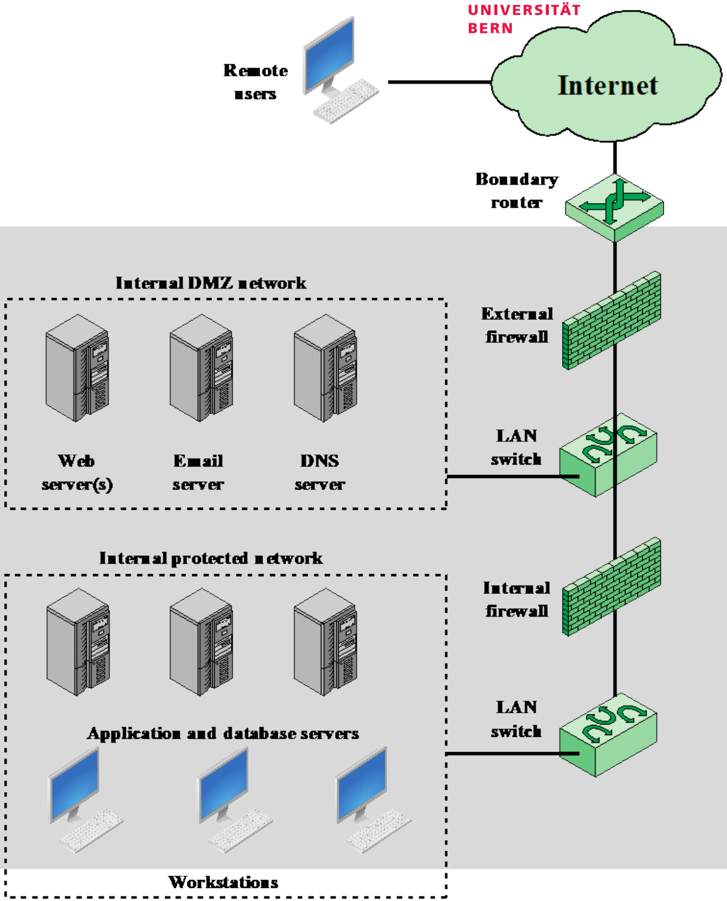


- Stand-alone system or a specialized function performed by an application-level gateway for certain applications.
- As with an application gateway, a circuit-level gateway sets up two TCP connections. Once the two connections are established, the gateway relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.
- Typical use when system administrator trusts internal users.
- The gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections.

1. Firewalls

11. Demilitarized Zone Networks

- External firewall is placed at the edge of a local or enterprise network.
- One or more internal firewalls protect the enterprise network.
- Between internal and external firewalls there are one or more networked devices in a region called demilitarized zone network, e.g., for systems that are externally accessible but need some protections like corporate web server, email server.



2. Intrusion Detection Systems

1. Terms

Intrusion

- Violations of security policy, usually characterized as attempts to affect the confidentiality, integrity, or availability of a computer or network by external attackers or authorized users trying to overstep their legitimate authorization levels

Intrusion Detection

- The process of collecting information about events occurring in a computer system or network and analyzing them for signs of intrusions

Intrusion Detection System

- Hardware or software that gather and analyze information from various areas within a computer or a network for the purpose of finding, and providing real-time or near-real-time warning of attempts to access system resources in an unauthorized manner

2. Intrusion Detection Systems

2. Classification

Host-based IDS

- monitors the characteristics of a single host and the events occurring within that host for suspicious activity

Network-based IDS

- monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity

2. Intrusion Detection Systems

3. Components

Sensors

- are responsible for collecting data.
- The input for a sensor may be any part of a system that could contain evidence of an intrusion, e.g., network packets, log files, and system call traces.
- collect and forward this information to the analyzer.

Analyzers

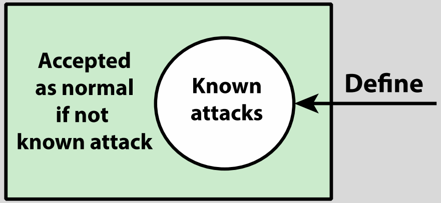
- receive input from one or more sensors or from other analyzers.
- are responsible for determining if an intrusion has occurred. The output of this component is an indication that an intrusion has occurred. The output may include evidence supporting the conclusion that an intrusion occurred.
- may provide guidance about what actions to take as a result of the intrusion.

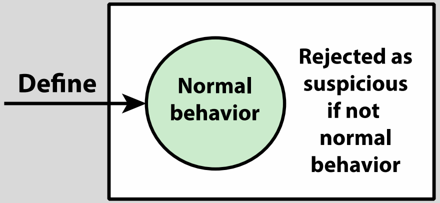
User interface

- enables a user to view output from the system or control the behavior of the system.
- may equate to a manager, director, or console component.

2. Intrusion Detection Systems

4.1 Misuse and Anomaly Detection





Misuse detection

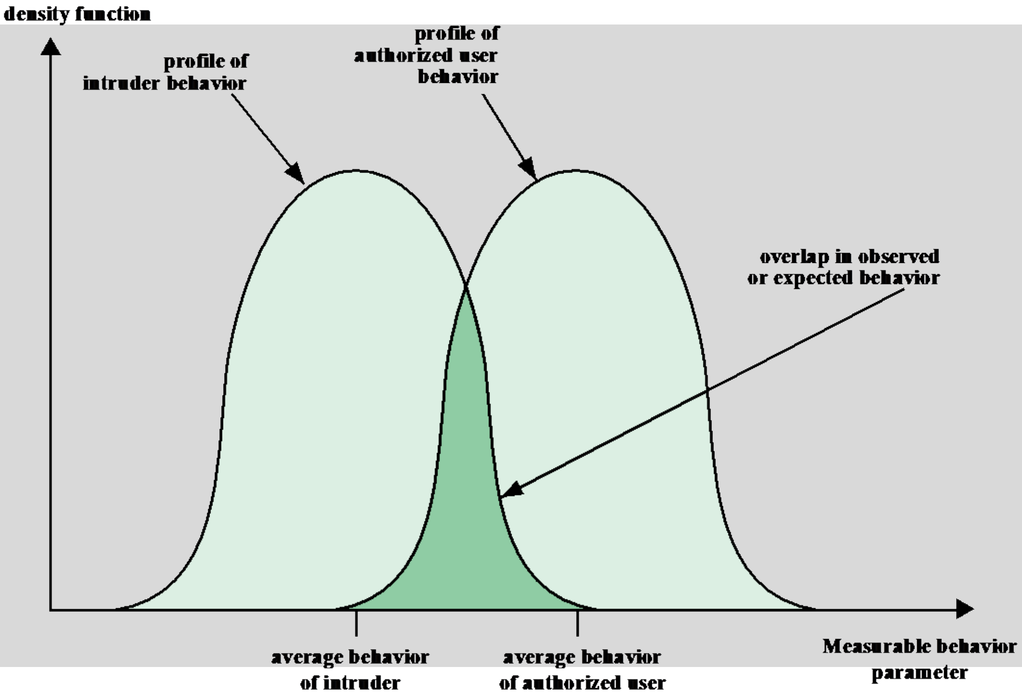
- is based on rules that specify system events, sequences of events, or observable properties of a system that are believed to be symptomatic of security incidents.
- uses various pattern-matching algorithms, operating on large databases of attack patterns, or signatures.
- Advantage: accurate and few false alarms.
- Disadvantage: difficult to detect novel or unknown attacks.

Anomaly detection

- searches for activity that is different from the normal behaviour of system entities and system resources.
- Advantage: able to detect previously unknown attacks based on an audit of activity.
- Disadvantage: significant trade-off between false positives and false negatives.

2. Intrusion Detection Systems

4.2 Behaviour of Intruders and Authorized Users


density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

2. Intrusion Detection Systems

5. Host-Based IDS

- add a specialized layer of security software to vulnerable or sensitive systems, e.g., database server
- monitor activity on the system in a variety of ways to detect suspicious behavior
- sometimes can halt an attack before any damage is done
- primary purpose: to detect intrusions, log suspicious events, and send alerts
- can detect external and internal intrusions
- use one or a combination of anomaly and misuse protection, anomaly detection strategies:
  - Threshold detection
  - Profile based

2. Intrusion Detection Systems

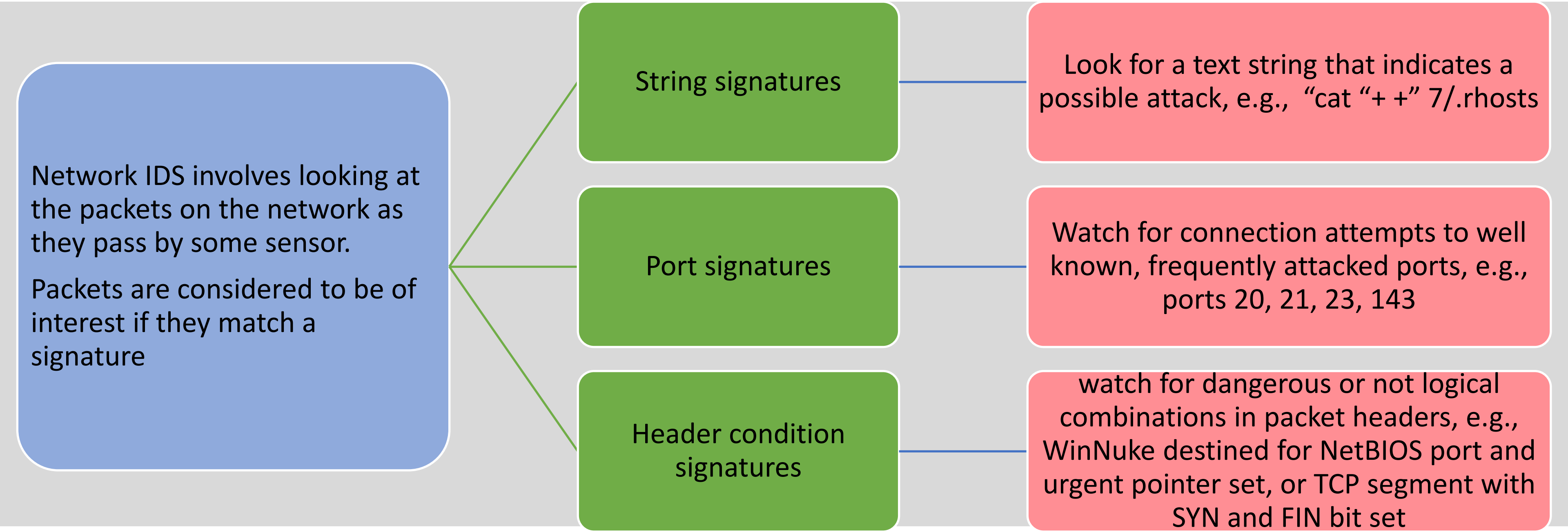
6.1 Network IDS

- monitors the traffic on its network segment as a data source.

- accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment.

2. Intrusion Detection Systems

6.2 Network IDS Function



Network IDS involves looking at the packets on the network as they pass by some sensor.

Packets are considered to be of interest if they match a signature

String signatures

Look for a text string that indicates a possible attack, e.g., “cat “+ +” 7/.rhosts

Port signatures

Watch for connection attempts to well known, frequently attacked ports, e.g., ports 20, 21, 23, 143

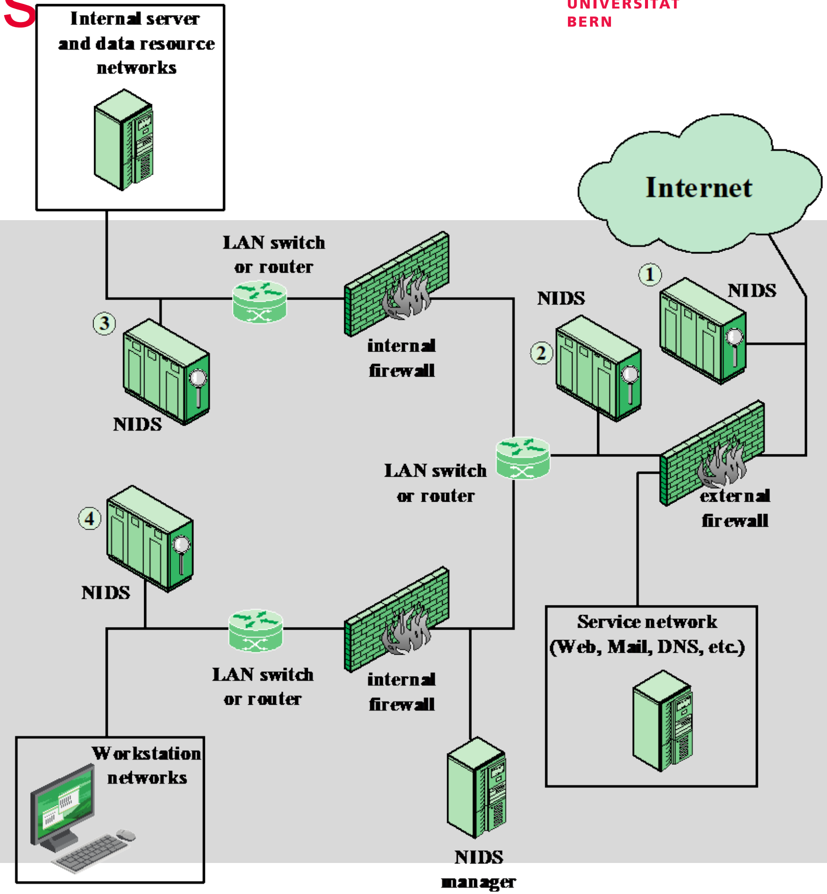
Header condition signatures

watch for dangerous or not logical combinations in packet headers, e.g., WinNuke destined for NetBIOS port and urgent pointer set, or TCP segment with SYN and FIN bit set

2. Intrusion Detection Systems

6.3 Network IDS Locations

1. Outside the main enterprise firewall: useful for establishing the level of threat for a given enterprise network
2. In the network DMZ: to monitor for penetration attempts that target web and other services generally open to outsiders.
3. Behind internal firewalls: to monitor major backbone networks, such as those that support internal servers and database resources.
4. Behind internal firewalls: to monitor LANs that support user workstations and servers specific to a single department.



3. Malicious Software

1. Definition and Types

- NIST SP 800-83 Definition:
  - “a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system”
- Malware can
  - pose a threat to application programs, to utility programs, and to kernel-level programs
  - be used on compromised or malicious Web sites and servers, or in especially crafted spam emails or other messages

Malware types

- Virus
- Worm
- Trojan Horse
- Spyware
- Rootkit
- Backdoor
- Mobile code
- Bot

3. Malicious Software

2. Malware Defense

		Area of Vulnerability		
		Network	Payload	Endpoint
Time Scale	Real-Time/ Near-Real-Time	Network Traffic Analysis	Payload Analysis	Endpoint Behavior Analysis
	Post-compromise (days/weeks)	Incident Management and Forensics		

4. Denial-of-Service Attacks

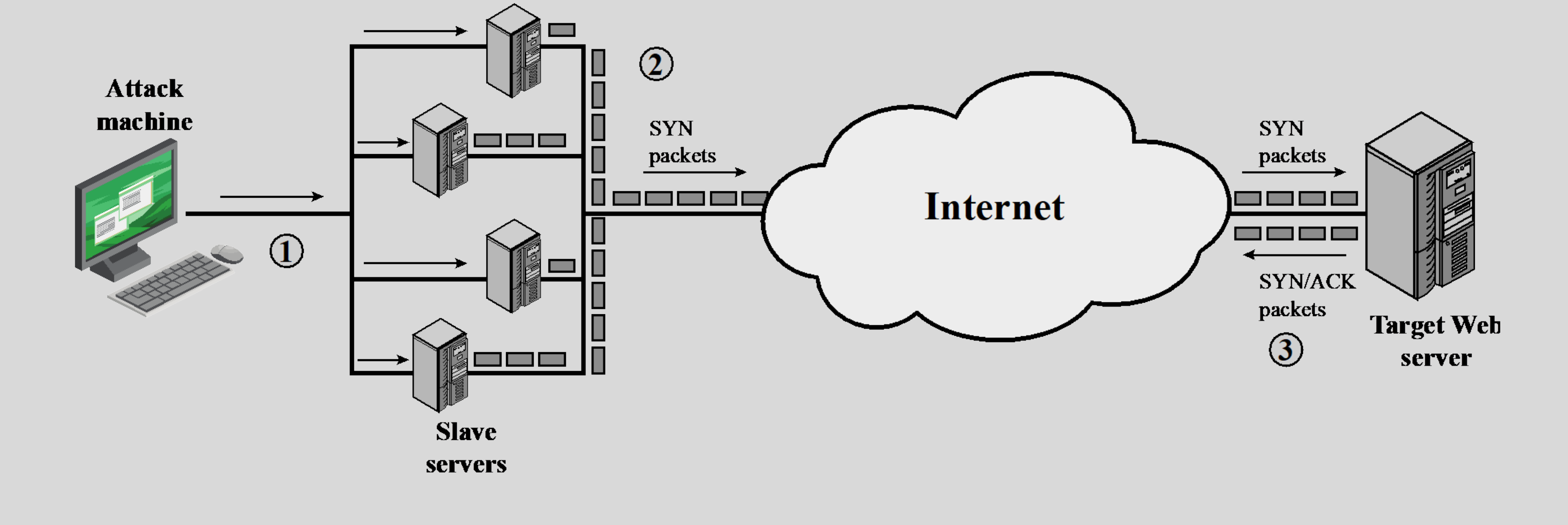
1. Overview

- Attempt to prevent legitimate users of a service from using that service
- When the attack comes from a single host or network node, then it is simply referred to as a DoS attack
- More serious threats by a Distributed Denial-of-Service attack; in a typical DDoS attack, many compromised hosts send useless packets

- (D)DoS attacks make computer systems inaccessible by flooding servers, networks, or even end-user systems with useless traffic so that legitimate users can no longer gain access to those resources.

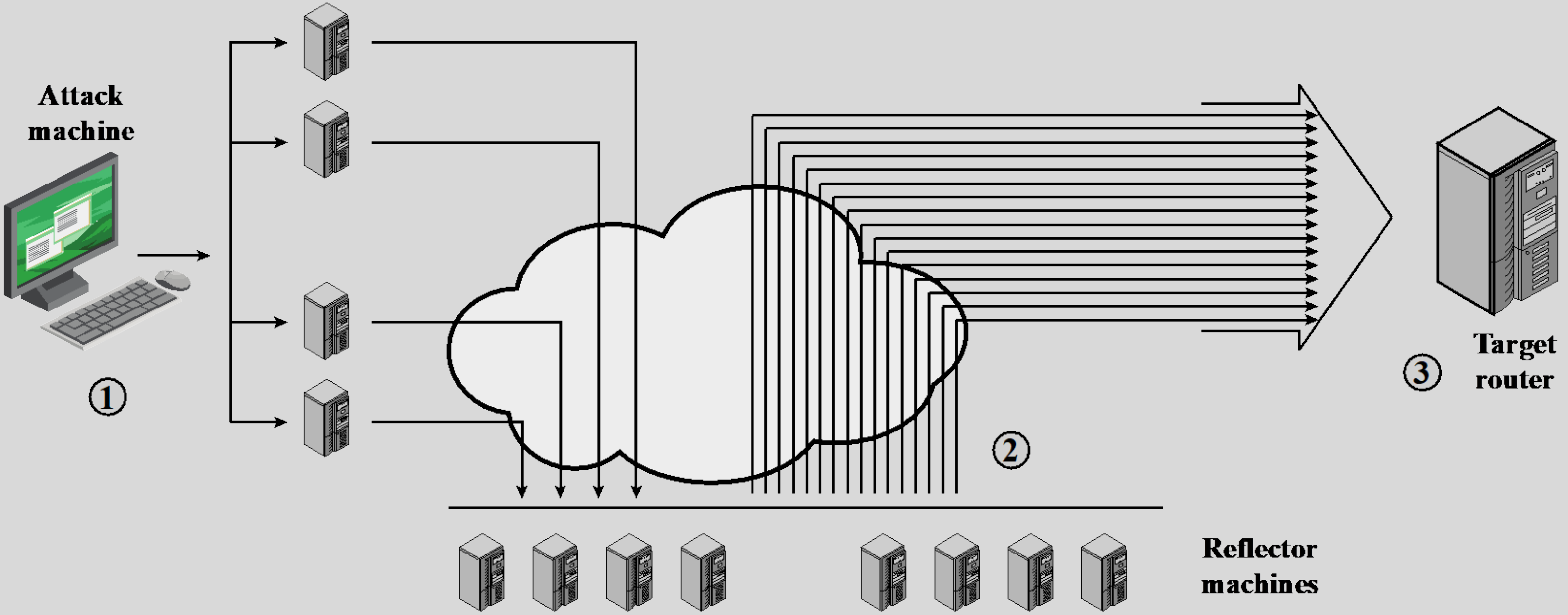
4. Denial-of-Service Attacks

2.1 DDoS Example: Distributed SYN Flood Attack



4. Denial-of-Service Attacks

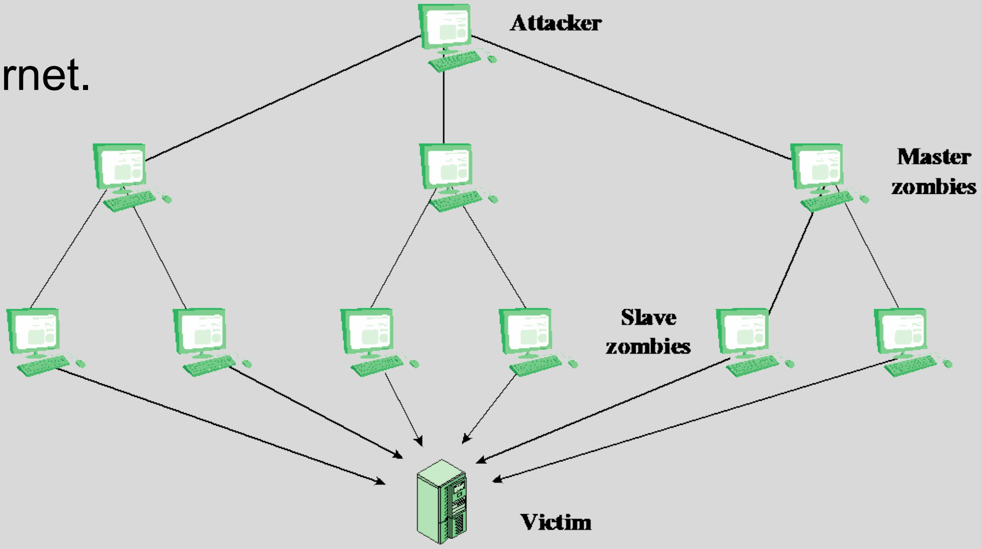
2.2 DDoS Example: Distributed ICMP Attack



4. Denial-of-Service Attacks

3.1 Direct DDoS Attack

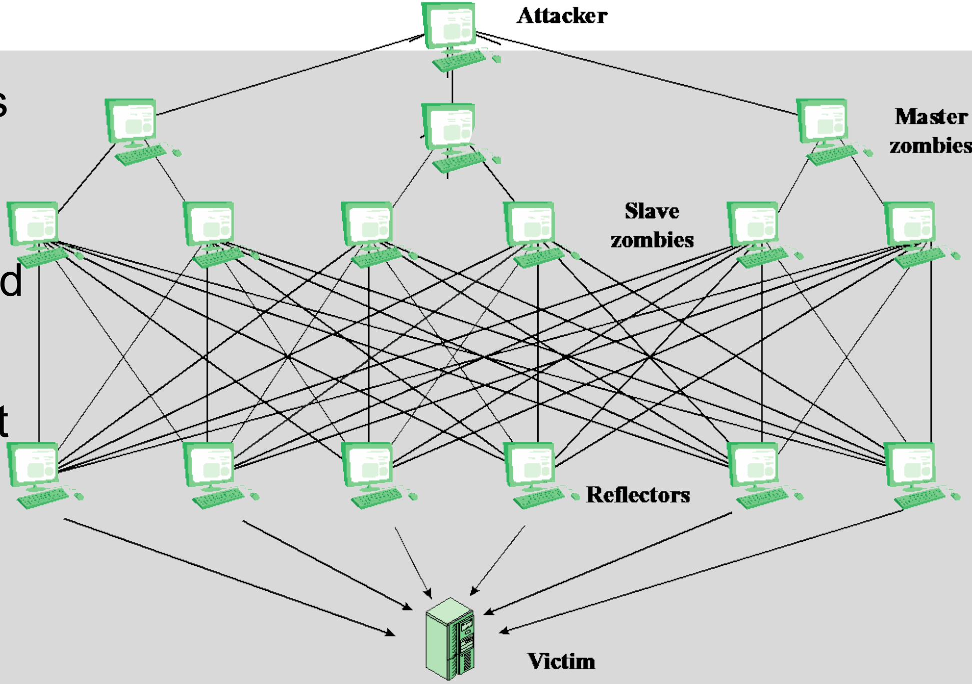
- Attacker can implant zombie software on several sites distributed throughout the Internet.
- Often, two levels of zombie machines: master zombies and slave zombies, both infected with malicious code.
- Attacker coordinates and triggers the master zombies, which in turn co-ordinate and trigger the slave zombies.
- The use of two levels of zombies makes it more difficult to trace the attack back to its source and provides for a more resilient network of attackers.



4. Denial-of-Service Attacks

3.2 Reflector DDoS Attack

- Slave zombies construct packets requiring a response that contain the target’s IP address as the source IP address in the packet’s IP header.
- These packets are sent to uninfected machines known as reflectors, which respond with packets directed at the target machine.
- A reflector DDoS attack can easily involve more machines and more traffic than a direct DDoS attack and hence be more damaging.
- Tracing back the attack or filtering out the attack packets is more difficult because the attack comes from widely dispersed uninfected machines.



4. Denial-of-Service Attacks

4. DDoS Countermeasures

- **Attack prevention and preemption** (before attack):
  - Mechanisms enable the victim to endure attack attempts without denying service to legitimate clients
  - Techniques: enforcing policies for resource consumption and providing backup resources available on demand
  - Prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks

- **Attack detection and filtering** (during attack):
  - Mechanisms attempt to detect the attack as it begins and respond immediately.
  - Detection involves looking for suspicious patterns of behavior
  - Response involves filtering out packets likely to be part of the attack
- **Attack source traceback and identification** (during and after attack):
  - Attempt to identify the source of the attack as a first step in preventing future attacks.
  - typically, does not yield results fast enough, if at all, to mitigate an ongoing attack.

5. The Onion Routing

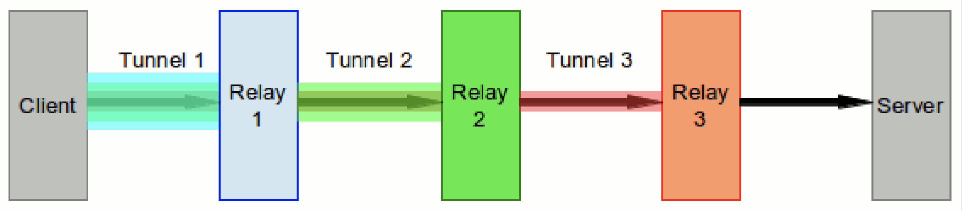
1. Overview

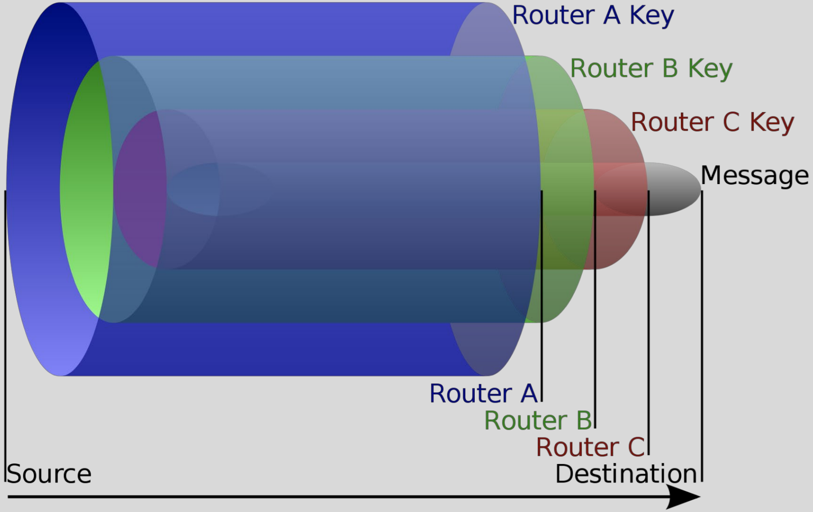
- most widely used anonymity network
- based on Onion Routing ideas
- First release in 2002

- integrated with a customized browser for better user experience and mitigate against side channel attacks
- provides anonymity for users and servers

5. The Onion Routing

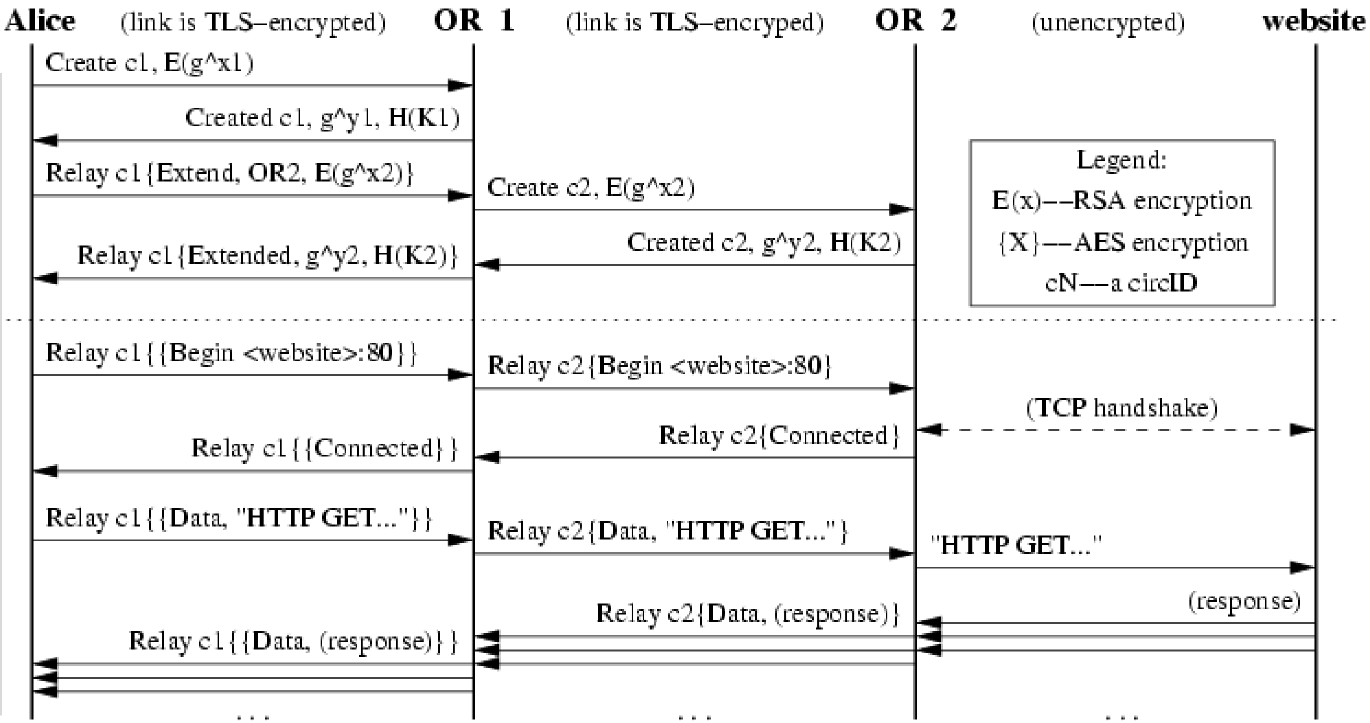
2. Tunneling





5. The Onion Routing

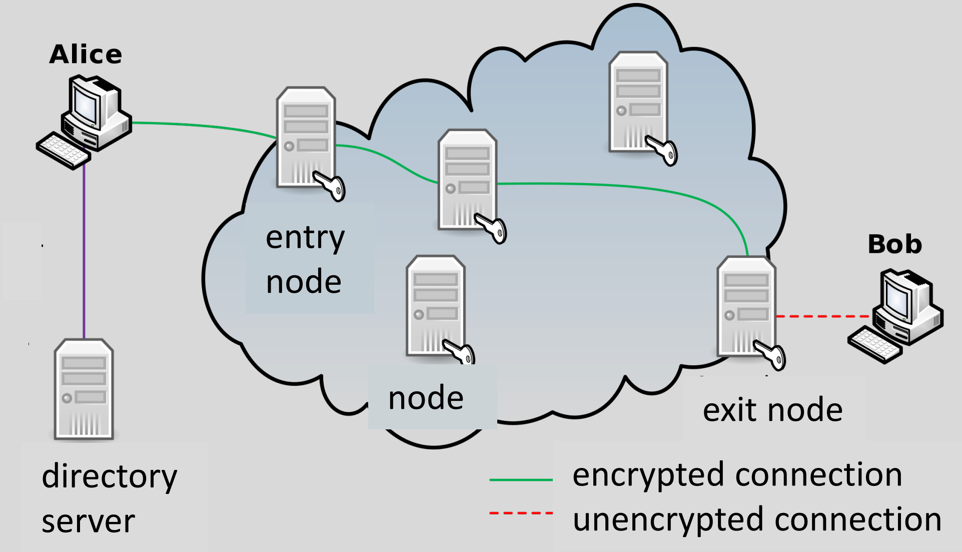
3. TLS Tunneling



5. The Onion Routing

4. Operation

1. User installs Tor-Proxy on his/her computer, which connects to Tor network. Download of available Tor servers (relays) from directory server (signed list)
2. Selection of random route via at least 3 Tor servers (trade-off delay and anonymity)
3. Setup of consecutive connections, each server knows successor and predecessor
4. Data transfer over these connections



5. The Onion Routing

5. Discussion

Advantages

- No Single Tor node is aware of the complete plan of Communication.
- the more Tor nodes the more anonymity added
- Tor builds anonymous paths for the client based on a list of bridge nodes.

Disadvantages

- Quality-of-Service and Performance
- Central directory server
- Dependence on DNS

Thanks a lot

for your Attentation

Prof. Dr. Torsten Braun, Institut für Informatik

Bern, 16.05.2022 – 23.05.2022