UNIVERSITY OF PLYMOUTH

Network Security

Learning outcome checklist

1. Explain the role of firewalls
2. See the difference between different firewall types: William Stallings, Network Security Essentials Application and Standard, 6th edition, section 12.3, p414
3. Understand when to set up DMZ: William Stallings, Network Security Essentials Application and Standard, 6th edition, section 12.5, p423
4. Explain the role of IDS/IPS

Session Content

Overview of Networking

Firewalls

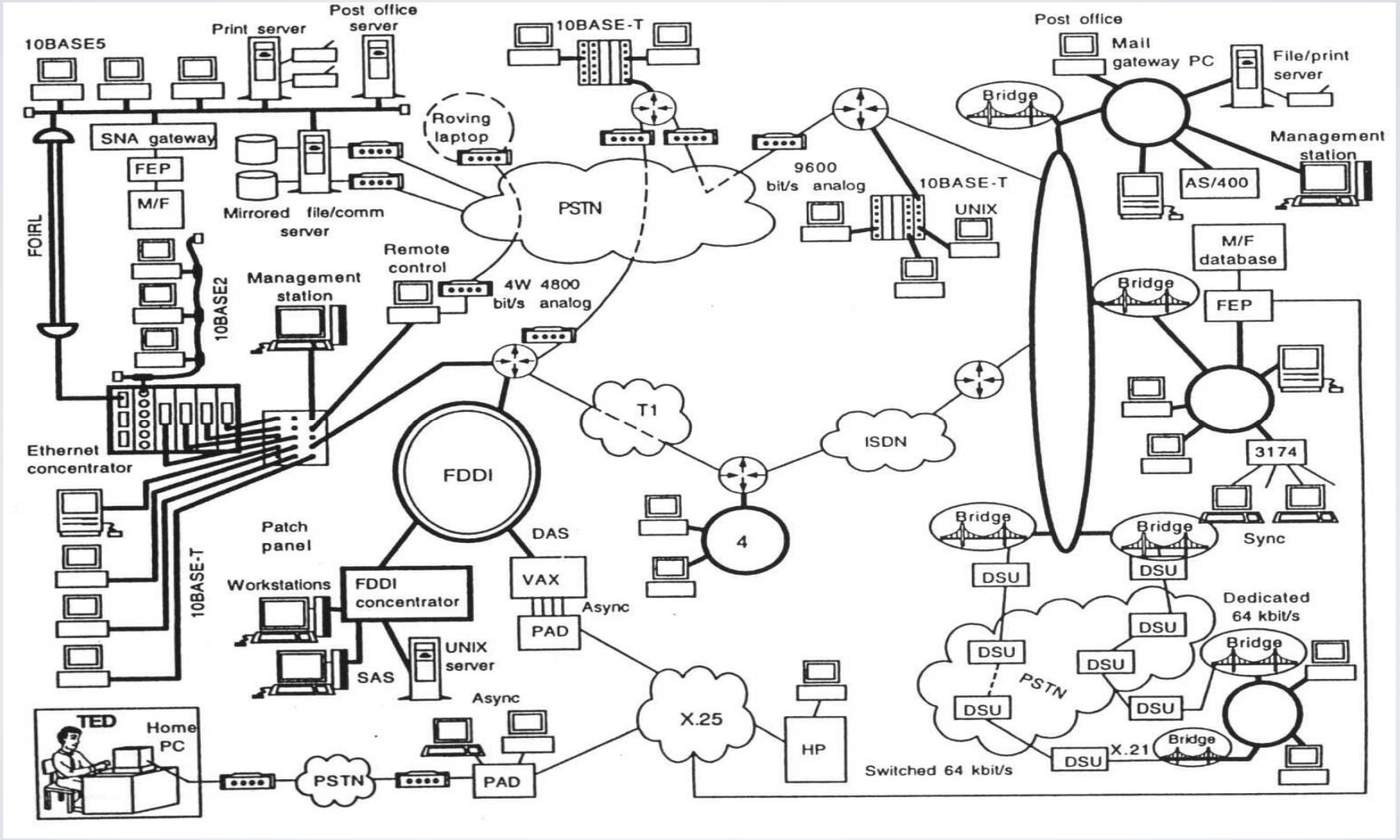
Demilitarised Zone

Intrusion Detection Systems

Conclusions

Overview of Networking

Networking

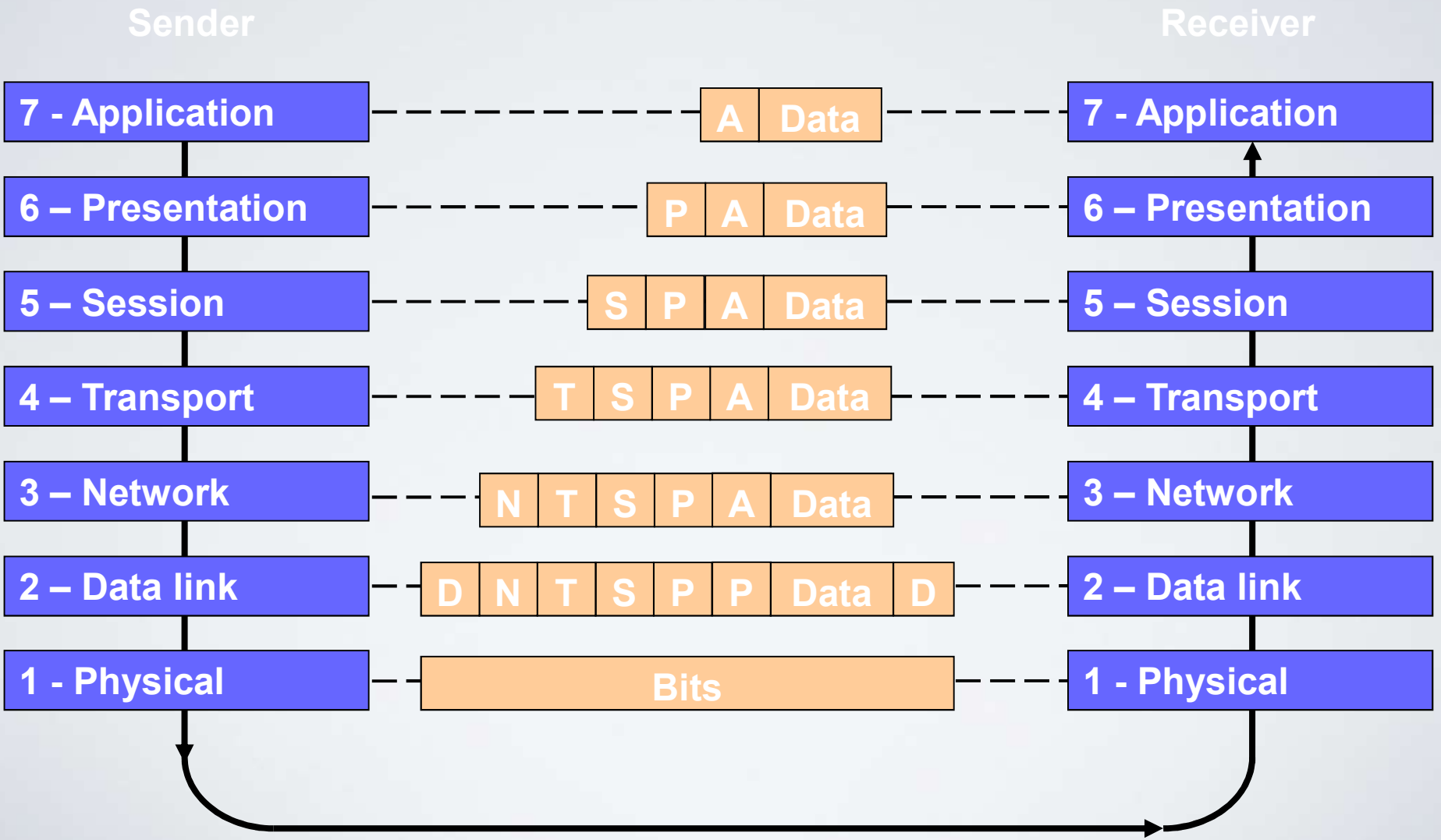

10BASE5
Print server
Post office server
10BASE-T
Post office
Mail gateway PC
File/print server
Bridge
Roving laptop
SNA gateway
FEP
M/F
FOIRL
Mirrored file/comm server
PSTN
9600 bit/s analog
10BASE-T
UNIX
Management station
AS/400
M/F database
Remote control
4W 4800 bit/s analog
Management station
10BASE2
Bridge
FEP
T1
ISDN
Ethernet concentrator
FDDI
3174
Patch panel
DAS
4
Bridge
Bridge
Sync
DSU
DSU
Workstations
FDDI concentrator
VAX
Async
PAD
Dedicated 64 kbit/s
DSU
DSU
Bridge
DSU
DSU
PSTN
DSU
DSU
UNIX server
SAS
Async
X.25
HP
TED
Home PC
PSTN
PAD
DSU
X.21
Bridge
Switched 64 kbit/s

Networking

Attributes of a network

- Environment
  - Anonymity
  - Automation
  - Distance
  - Opaqueness
  - Routing Diversity
- Shape and Size
  - Boundary
  - Ownership
  - Control
- Media
  - Cable
  - Optical Fiber
  - Wireless
  - Microwave

OSI Model – Data Flow



TCP/IP

- General network protocols are typically concerned with routing messages between a sender and a receiver, dealing with loss or corrupted data
- TCP/IP are good protocols: designed for friendly and co-operating users linked in an unreliable networks
- Not designed with security in mind!
- IPSEC
  - IP Authentication Header
  - IP Encapsulating Security Payload
  - Does not include mechanisms to prevent traffic analysis
- SSL/TLS
  - Provides strong cryptographic entity authentication, data integrity and confidentiality

Network– Why are they Vulnerable?

- Anonymity
  - Attacks can come from anywhere in the world and from the guy sitting next to you – difficult to establish origin, particularly when intermediate hosts are used to disguise an attack
- Many points of attack
  - Information is stored on a variety of systems – local machines and network servers
- Sharing
  - Many users using systems, with many sets of user credentials open to misuse
- Complexity of system
  - Organizational systems comprise of a variety of networks, of systems with differing OSs etc
- Unknown perimeter
  - Challenging to define in large and mobile organizations
- Unknown Path
  - Packet paths may pass into un-trusted systems

Attack surfaces

- Network attack surface: network protocol vulnerabilities, such as open ports on outward facing Web and other servers
- Software attack surface such as web server vulnerabilities
- Human attack surface. Example: an employee with access to sensitive information vulnerable to a social engineering atta

Threats

- Eavesdropping and wiretapping
  - Dependent upon mode of communication – wired, wireless, microwave etc
- Protocol flaws
- Impersonation
  - Authentication by brute-force guessing, Authentication thwarted by eavesdropping, session hijacking, man-in-the-middle attack
- Message confidentiality threats
  - Misdelivery, exposure, traffic flow analysis
- Message integrity threats
  - Falsification of messages, noise
- Format failures
  - Malformed packets, protocol failures and implementation flaws
- Website vulnerabilities
  - Defacement, buffer overflows, Dot-Dot-Slash, Application code errors, server-side include
- Denial of Service
  - Transmission failure, connection flooding – ping of death, syn flood, traffic redirection

Attack tree example

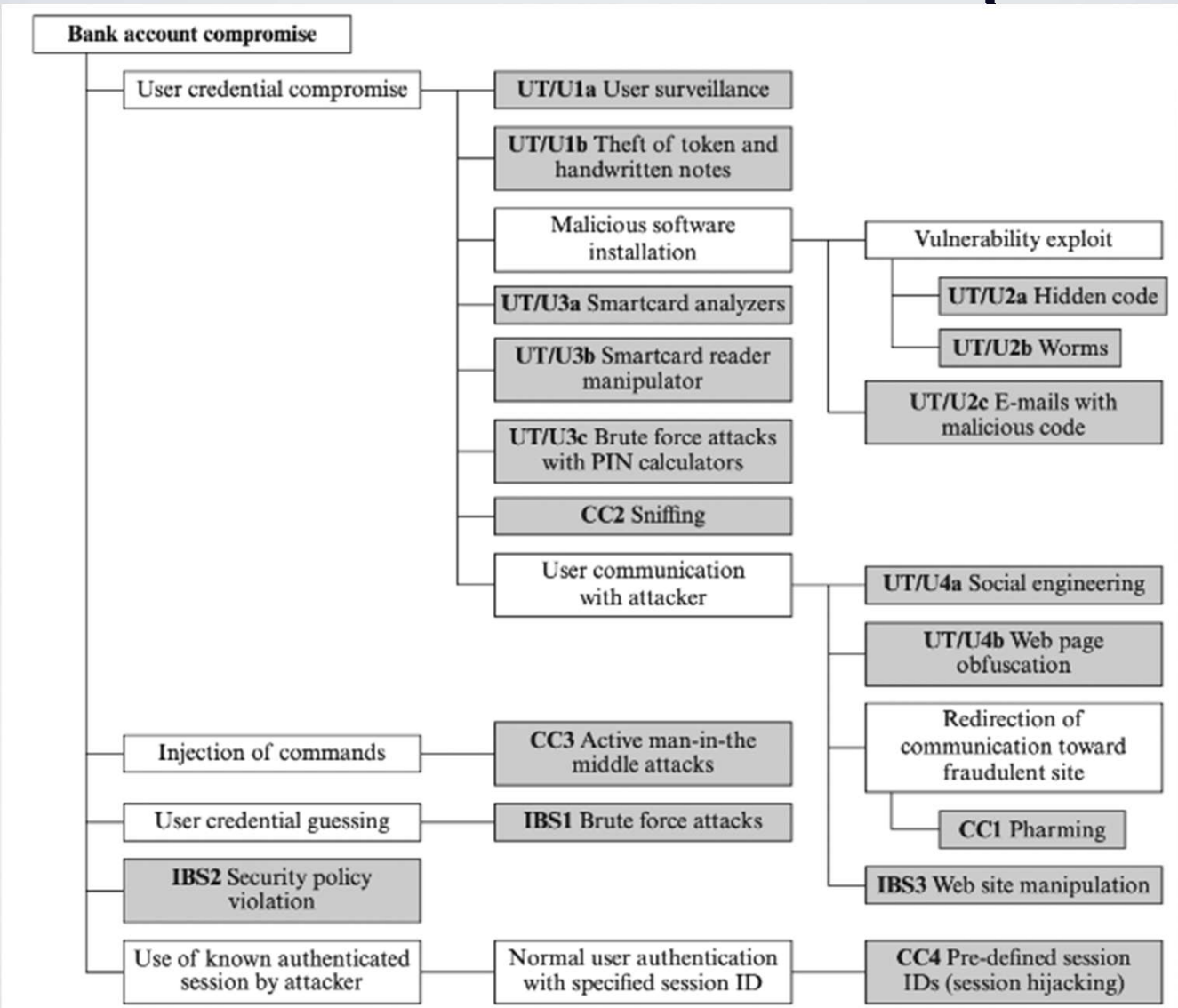
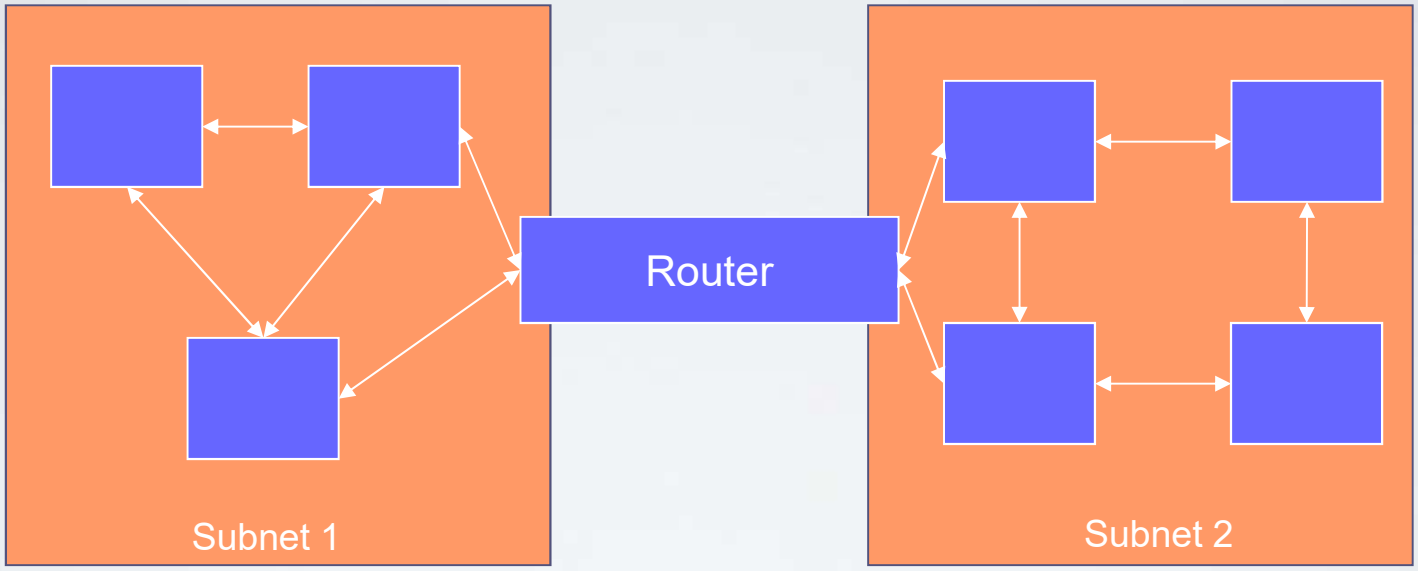


Figure 1.4 An Attack Tree for Internet Banking Authentication

Countermeasures – Network Boundaries



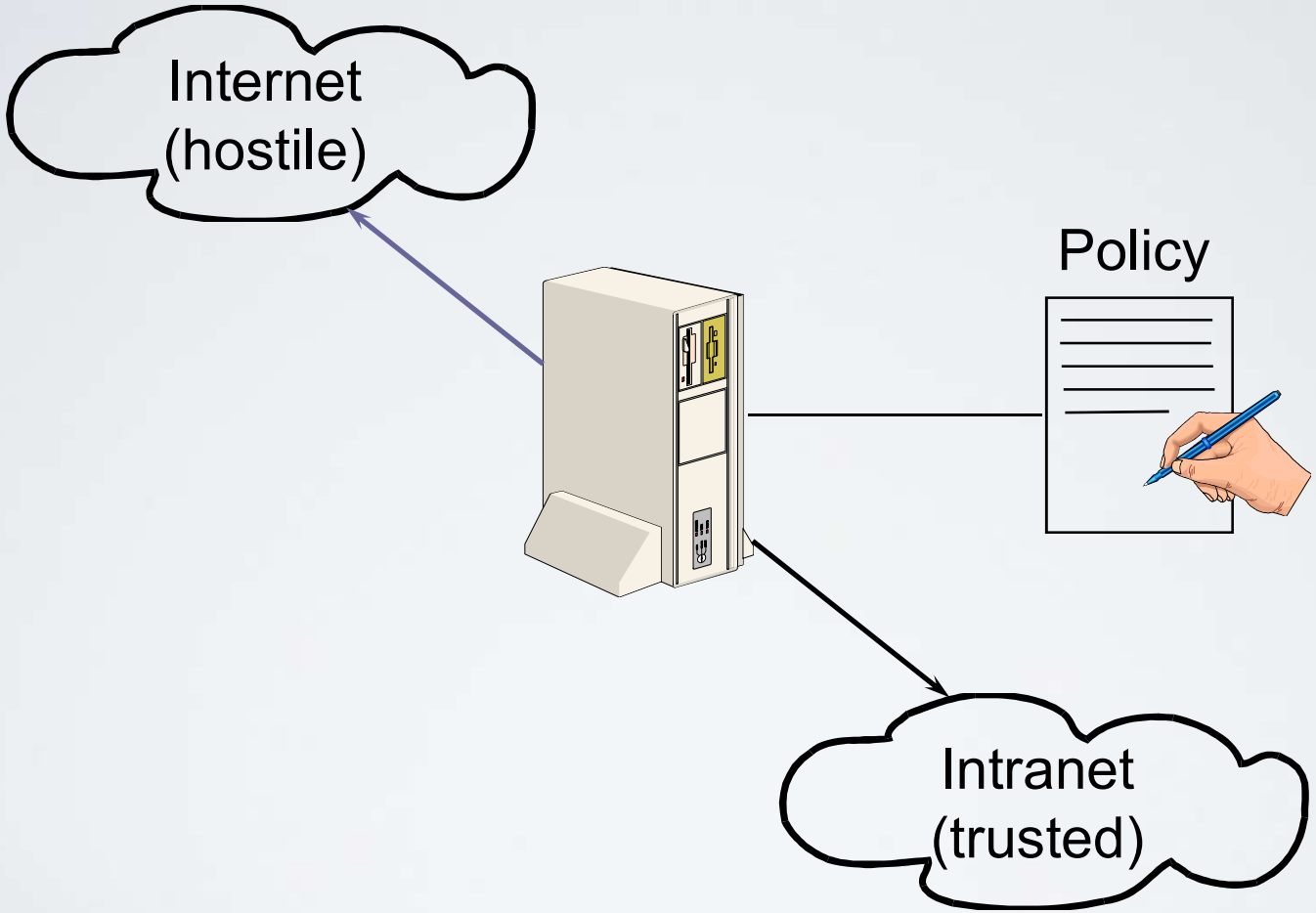
- Machines on a boundary:
  - Control access to the network
  - Add cryptographic protection on data leaving the network
  - Hide the internal structure of the network

Firewalls

Countermeasures - Firewalls

- A device that filters all traffic between networks – typically an insider and outside network
- Types of Firewall include:
  - Packet filtering gateways
  - Stateful inspection proxies
  - Application proxies
  - (Guards)
  - (Personal firewalls)

The Firewall Concept (cont.)



The need for Firewalls

- Traditionally rely on security of individual hosts

  - As number of hosts increases :
    - less manageable;
    - more chance of administrative mistakes / lapses.
  - reduced likelihood of uniform security
- Firewall helps to increase overall security of the subnetwork

Firewall Advantages

- Protection from vulnerable services
- Controlled access to site systems
- Concentrated security
- Enhance privacy
- Logging and statistics on network use
- Security policy enforcement

Packet Filtering Firewall

- Operates at **IP packet level**
- Filters packets as they pass between router interfaces
- A number of packet features may provide basis for filtering :
  - source / destination IP addresses
  - source / destination port numbers

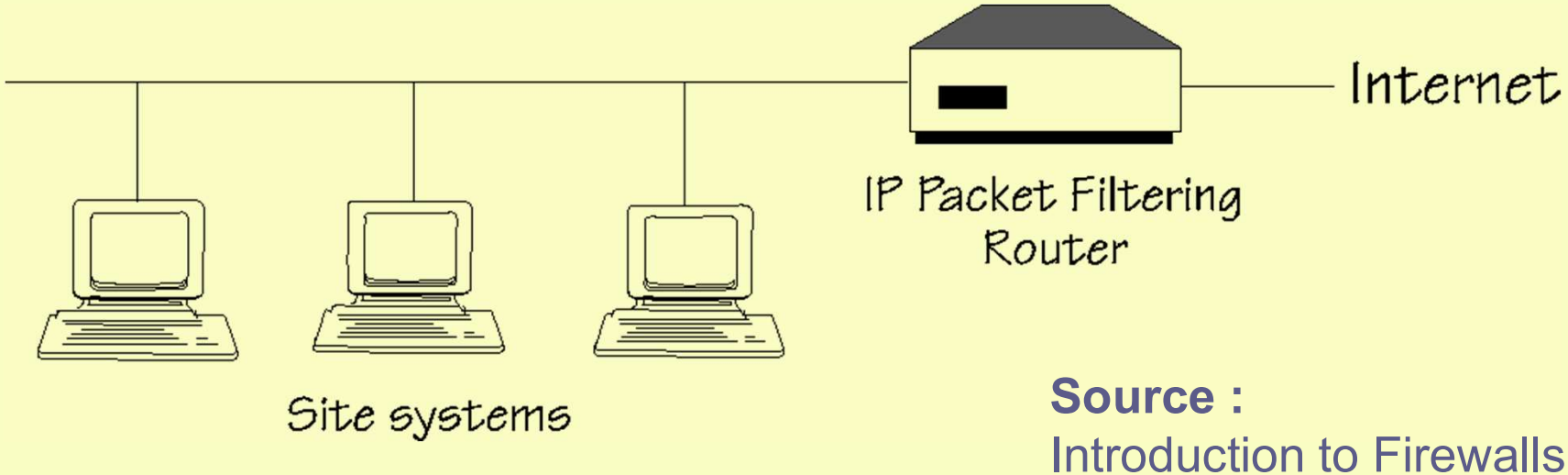
Packet Filtering Firewall

- Source IP address :
  - can control which machines on the internal network may access the Internet;
  - can control which machines from outside may access the internal network.
- Destination IP address :
  - on incoming packets, can filter what machines can be contacted for which services (e.g. WWW / email servers);
  - on outgoing packets, can control which sites internal users can access.

Packet Filtering Firewall (cont.)

- Source and Destination port numbers :
  - Many standard Internet services are offered via “well known” destination ports, e.g. :
    - HTTP = port 80;
    - SMTP = port 25;
    - FTP = port 21;
    - Telnet = port 23;
    - RPC = port 111.
  - Can control the accessibility of specific services.

Packet Filtering Firewall (cont.)



Source :
Introduction to Firewalls

Example

- Background: SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023.

Example

Rule	Direction	Source Address	Destination Address	Protocol	Destination Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

A. Inbound mail from an external source is allowed (port 25 is for SMTP incoming).
B. This rule is intended to allow a response to an inbound SMTP connection.
C. Outbound mail to an external source is allowed.
D. This rule is intended to allow a response to an outbound SMTP connection.
E. This is an explicit statement of the default policy. All rulesets include this rule implicitly as the last rule.

Exercise - Which connections are allowed?

- Your hosts in this example have IP address 172.16.1.1, 172.16.3.4.
- The remote host have IP addresses 192.168.3.4, 10.1.2.3

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Exercise – How to prevent attacks in packet 5, 6?

- In packets 5, 6: Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4), in order to carry out an attack.
- How would you modify the firewall rules to prevent such an attack?

Demo

- See video COMP1002-L6 demo-packet filtering firewall on DLE
- Local host: internal-Ubuntu. Remote machine: external-Ubuntu
- Add a firewall rule:

#	Direction	Src address	Dst address	Dst port	Action
1	In	Any	Any	80	Allow

1. On local host:
    1. Run web server on local host: sudo python3 -m http.server 80
    2. Enable firewall on local host: ufw enable; sudo ufw status
    3. Add rule to the firewall to allow connection to port 80: sudo ufw allow in 80/tcp; sudo ufw status
2. On remote machine:
    1. use browser to access the web server
    2. craft a packet to send to local host: sudo hping3 -V -S -p 80 –s 5050 IP_address_of_local

Packet Filtering Advantages

- Functionality is part of standard router configuration software
  - no special hardware / software required.
- Flexible
- Fast
- Installation requires no action on the part of users

Packet Filtering Disadvantages

- Filtering rules are complex to specify, especially when selective blocking of services required.
- Usually no testing facility to enable correctness of rules to be verified;
- Routers may not provide logging capability, so dangerous packets may not be detected until a break-in has occurred.

Packet Filtering Disadvantages

- May not be able to filter based upon TCP/UDP source port - may lead to holes in protection.
- Difficult to filter RPC services because the ports used are assigned randomly (therefore, cannot block RPC without potentially affecting other traffic).
- Some routers do not have the capability to filter according to the interface a packet arrived at (i.e. inbound / outbound), complicating the specification of rules.

Stateful Inspection Firewall

- Packet-level firewalls have no concept of “state” or “context”
  - Every packet needs to be examined against the rule-set
  - Very CPU intensive
- Stateful inspection firewall maintains state information
  - If the first packet of a connection has passed the rule-set then all packets associated to that connection are also ok – without needing to check each and every one.
- Updating the rule-set forces the state table to be flushed – increased processing until table is re-established.

Table 12.2 Example Stateful Firewall Connection State Table (SP 800-41-1)

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	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
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	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

Demo

See COMP1002-L6 demo-stateful inspection firewall on DLE

1. On local host
    1. Run web server on local host: sudo python3 -m http.server 80
    2. Enable firewall on local host: ufw enable; sudo ufw status
    3. Add stateful rule using iptables: sudo iptables -A INPUT –p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
2. On remote machine,
    1. use browser to access the web server
    2. craft a packet to send to local host: sudo hping3 -V -S -p 80 –s 5050 IP_address_of_local

Application Proxy

- Provides a *proxy* between external systems and hosts offering services on an internal network
  - users connect to the proxy as a *gateway* to the internal network;
  - no longer have direct connections to internal machines.
- Allows more fine-grain control of connections.
- Can be used in conjunction with packet filtering router
  - directs all permitted connections towards the application gateway machine.

Application Gateway Process

E.G. For establishing a TELNET connection :

- user TELNETs to application gateway an enters name of an internal host;
- gateway checks user's source IP address - accepts or rejects according to access criteria in place;
- user may need to authenticate him/herself;
- proxy creates TELNET connection between gateway and internal host;
- proxy service passes bytes between the 2 connections;
- application gateway logs the connection.

Application Gateway Advantages

- Allows through only those services for which there is a proxy
  - all other services completely blocked.
- Allows protocol to be filtered
  - e.g. allow FTP, but deny use of *put* command
- Information hiding
  - names of internal systems need not be known to outsiders. DNS only needs to know of application gateway

Application Gateway Advantages

- Robust authentication and logging
  - application traffic can be pre-authenticated before reaching internal hosts;
  - can be logged more effectively.
- Cost effectiveness
  - hardware / software for authentication and logging need only be located at the application gateway.
- Less complex filtering rules
  - packet filter need only allow application traffic destined for the gateway and reject the rest;
  - easier than filtering and directing to a number of specific systems.

Application Gateway Disadvantages

- Client-Server protocols (e.g. TELNET) require two steps for inbound and outbound connections.
- Requires modified user behavior or modified client
  - e.g. for TELNET, either :
    - user must connect (but not login) to firewall rather than direct to host; OR
    - use a modified TELNET client that deals with the firewall transparently.

Demo

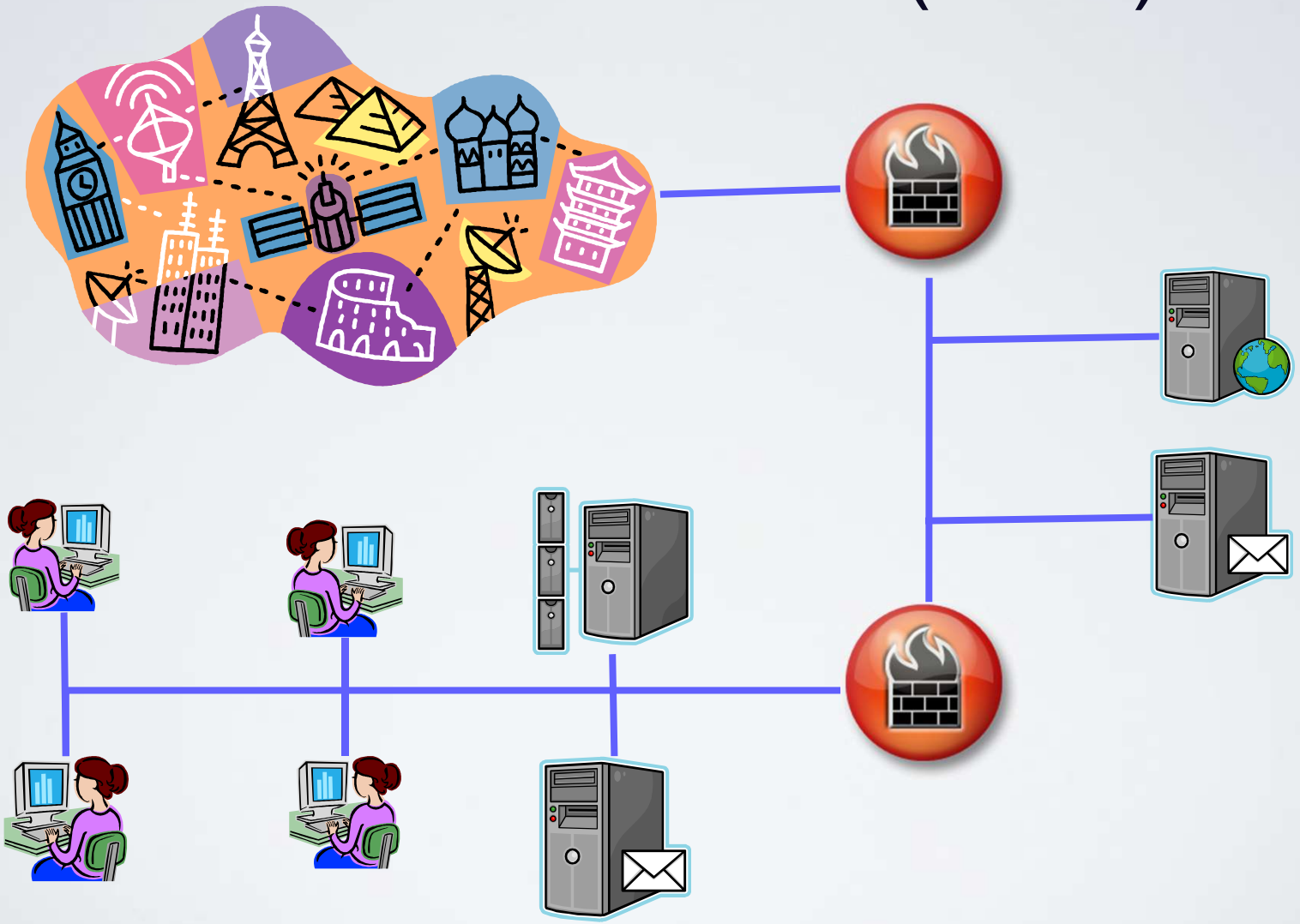
See the video “COMP1002-L6-demo-Application proxy” on DLE

Using squid proxy (Source: https://devopscube.com/setup-and-configure-proxy-server/)

1. Access facebook through the proxy: curl -x 127.0.0.1:3128 -I https://facebook.com
2. Edit /etc/squid/blocked_sites: add sites you would like to block
3. Restart squid: sudo systemctl restart squid
4. Access facebook through the proxy: curl -x 127.0.0.1:3128 -I https://facebook.com → 403 forbidden
5. Edit firefox to go through proxy
6. Try to access facebook with firefox

DMZ

Demilitarized Zone (DMZ)



Intrusion Detection Systems

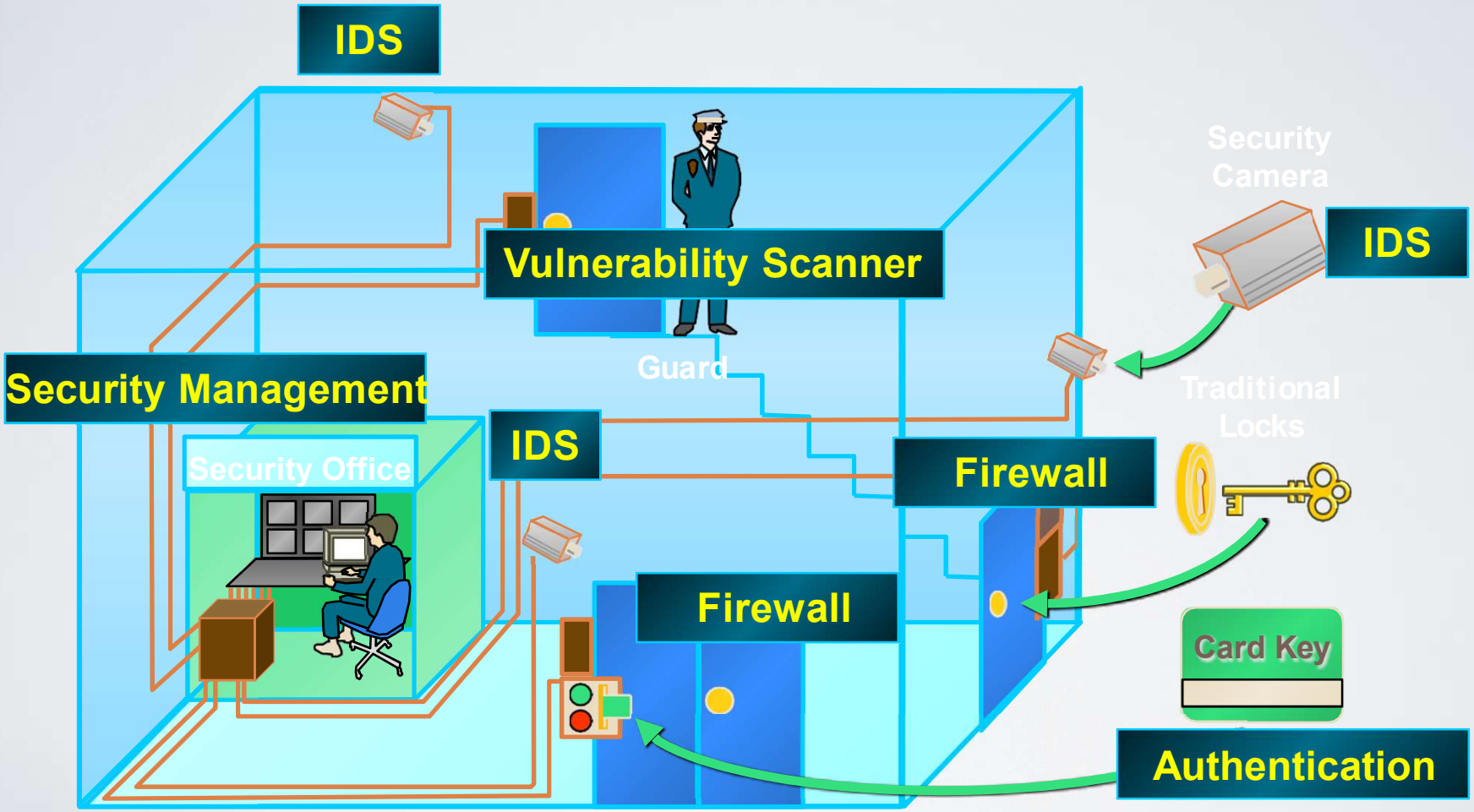
Intrusion Detection Systems

- Computer systems not under attack exhibit several characteristics:
  - User actions/processes conform to a statistical predictable pattern
  - User actions/processes do not include commands aimed at subverting the security policy
  - Actions of process conform to a set of specifications describing *what* the processes are allowed to do

Intrusion Detection Systems

- Goals of an IDS:
  - Detect a wide variety of intrusions
  - Detect intrusions in a timely fashion
  - Present analysis in a simple, easy-to-understand format
  - Be accurate! False positives reduce the confidence in the system

Network Security: An analogy



Intrusion Detection Systems

- IDS Models:

Anomaly Detection	Misuse Detection
Reports when user actions/processes deviate from those *expected* – based upon statistics	Sequence of user actions/processes being executed is *known* to violate the security policy

Misuse or anomaly detection

- Menti

Example 1: Suppose a particular user typically logs in around 10 a.m., reads mail, performs database transactions, takes a break between noon and 1 p.m., has very few file access errors, and so on. If the system notices that this same user logs in at 3 a.m., starts using compilers and debugging tools, and has numerous file access errors, it will flag this activity as suspicious.

Example 2: A system contains attack descriptions (or “signatures”) and match them against the audit data stream, looking for evidence of known attacks. One such attack, for example, would occur if someone created a symbolic link to a Unix system’s password file and executed a privileged application that accesses the symbolic link. If the system notices, it will flag this activity as suspicious.

Performance Characteristics

- Unfortunately, no IDS/IPS system is 100% full-proof (…or even anywhere near 100%!)
- Four performance criteria exist:
  - True Positive Alarm
    - Successfully detected an attack
  - True Negative Alarm
    - Does not report legitimate traffic as an intrusion
  - False Positive Alarm
    - An event that the IDS believes to be an attack but is not
  - False Negative Alarm
    - An attack is not detected by the IDS

Misuse Detection

- Events or sets of events that match a predefined pattern of events that describe a known attack
  - *Such patterns are called Signatures*
- Advantages:
  - Very effective at detecting attacks without generating an *overwhelming* number of false alarms
- Disadvantages:
  - Can only detect attacks they know about
    - New attacks go undetected until a new rule is created
  - Rules tended to be tightly defined
    - Small amendments to old/common attacks are not detected

Misuse Detection

- Misuse-based methods often use *Expert Systems* to analyse the data and apply the rule set.
  - More recent versions use more adaptive methods such as neural networks and Petri nets to improve their detection capabilities.
- Expert systems permit more efficient use of resources
  - certain rule sets can be enabled when particular packets are identified and remain off otherwise

Misuse Detection

- Snort – an open source free NIDS:
  - Developed by Marty Roesch and now owned by SourceFire
  - Traditionally a signature-based NIDS
  - However, if you visit Snort.org

    "*Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of **signature**, **protocol** and **anomaly** based inspection methods. With millions of downloads to date, Snort is the most widely deployed intrusion detection and prevention technology worldwide and has become the de facto standard for the industry".*

Misuse Detection

- Example Snort Alert:

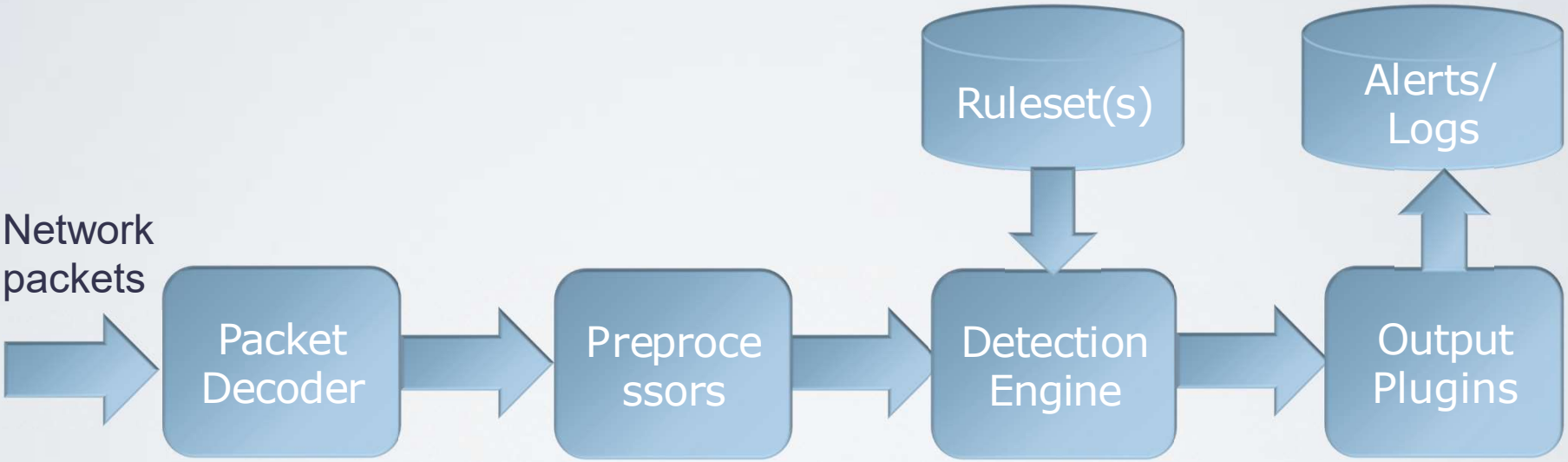
```
[**] Back Orifice [**]
04/24 - 13:33:51.880120 192.168.143.15:60256 ->
  192.168.5.16:31337

UDP TTL:41 TOS: 0x0 ID:49951 Len: 8
```

- Corresponding Rule:

```
Alert udp any any -> 192.168.5.0/24 31337 \
(msg:"Back Orifice";)
```

Packet Flow in Snort



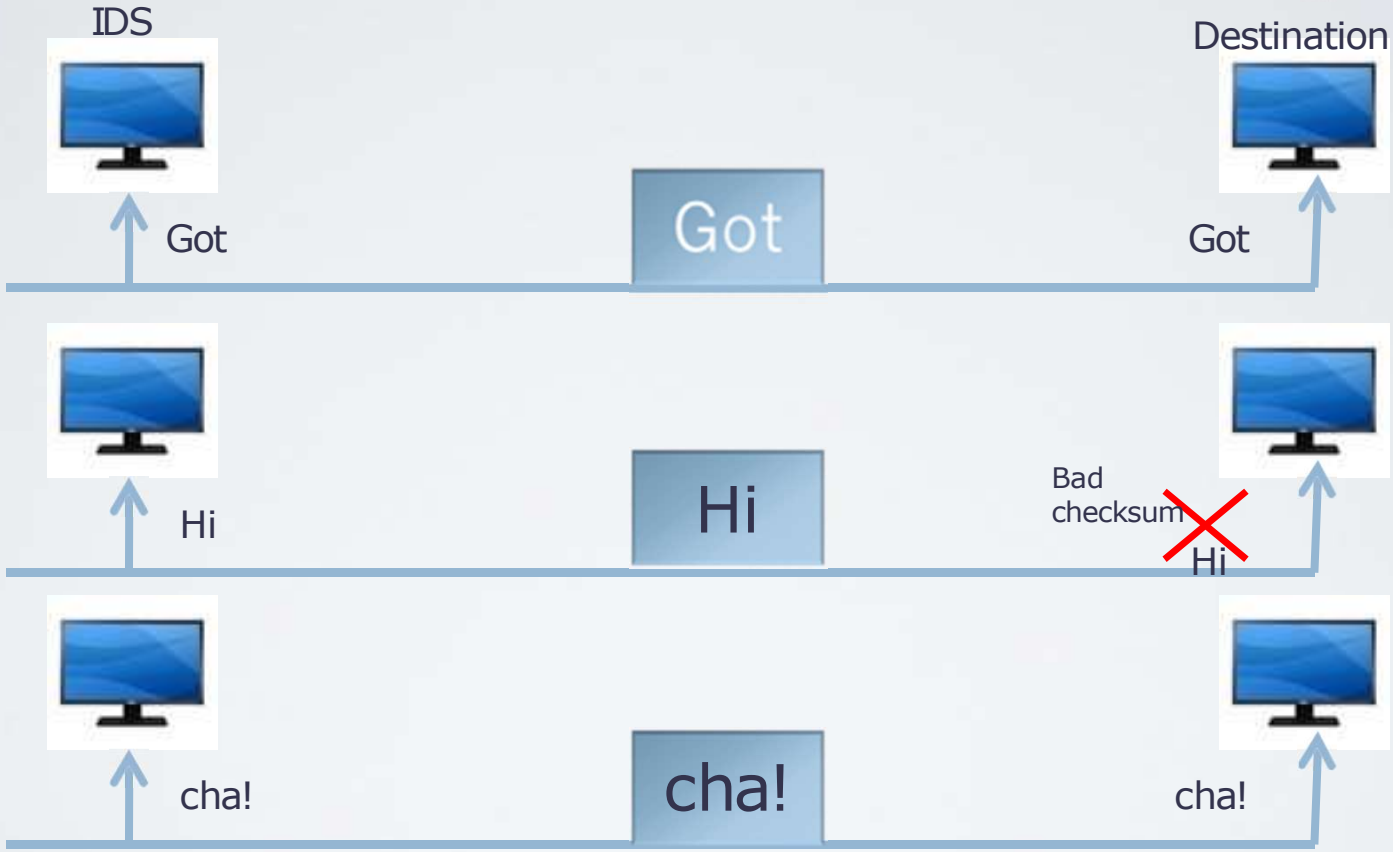
Demo

- alert icmp any any -> any any (msg: “ping detected”; sid: 1000001)

Insertion/Evasion Misuse Detection

- Scenario: Attacker wants to log into Telnet (port 23) with account REWT.
- A signature file exists for preventing this access.
- Insertion:
  - Send a packet with an additional character and invalid TCP checksum
  - NIDS sees ROEWT, Host sees REWT
- Evasion:
  - Add data to the payload of the TCP three-way handshake

Insertion



IDS sees: GotHicha!
Destination sees: Gotcha!

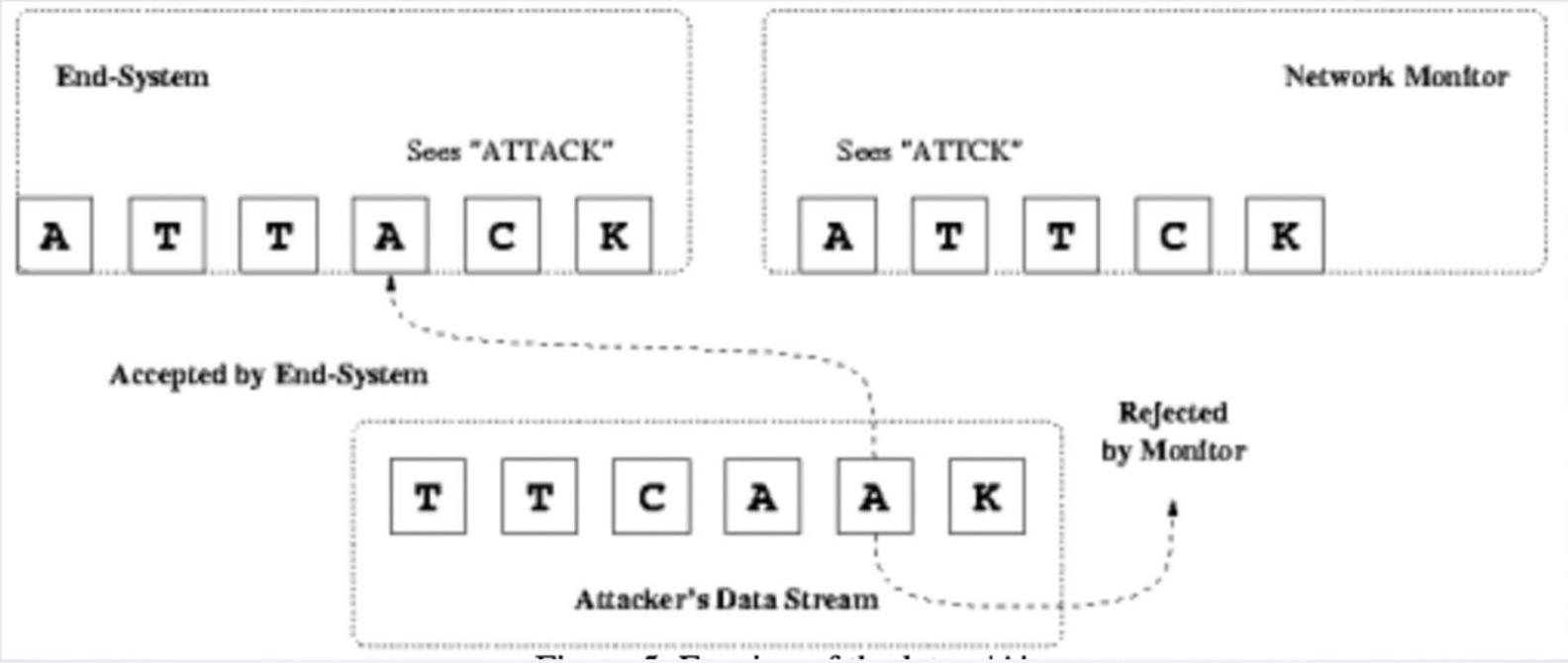
Evasion

IDS sees: cha!
Destination sees: Gotcha!

What type of attack?

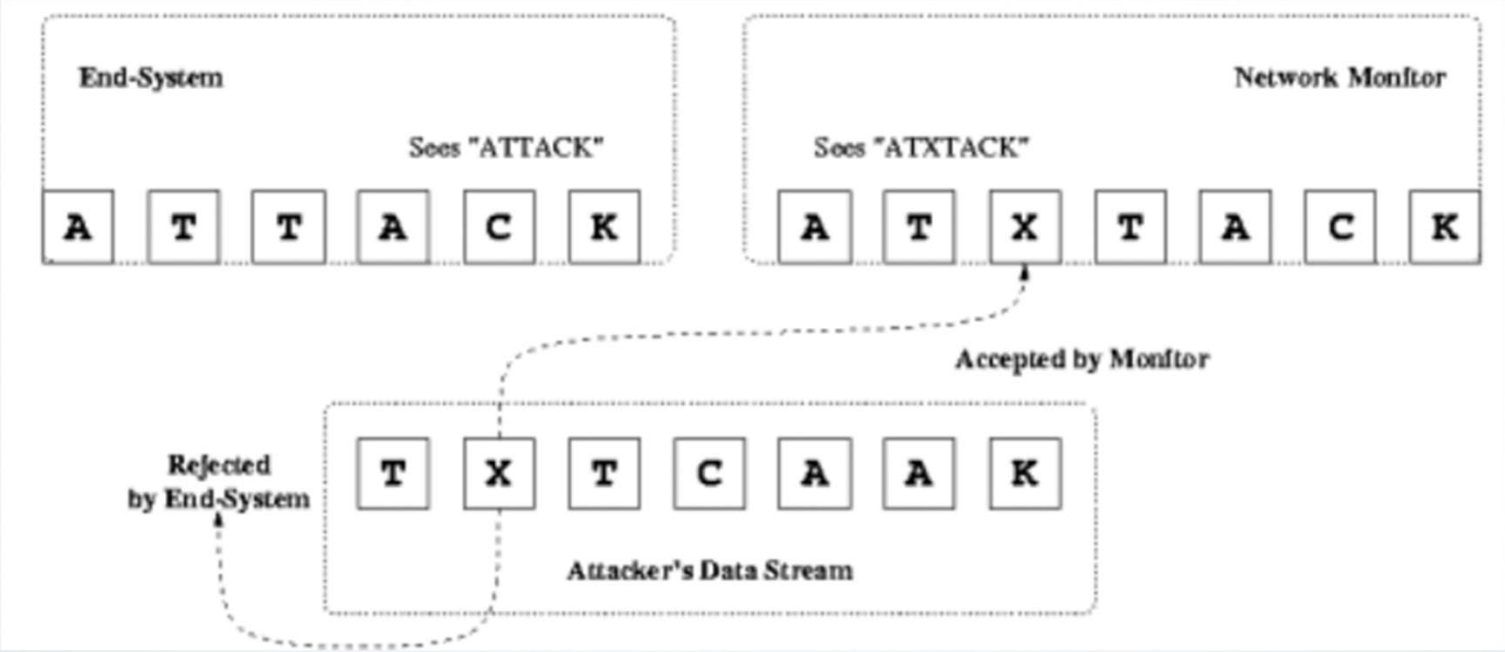
Menti

Example 1



What type of attack

- Menti
- Example 2



What type of attack

- Menti
- Example 3
- “The attacker used several networks to spoof 167 Mpps (millions of packets per second) to 180,000 exposed CLDAP, DNS, and SMTP servers, which would then send large responses to us.”

Anomaly Detection

- Identify abnormal or unusual behaviour
  - *Assumption: Attacks differ from normal behaviour*
- Denning identified three different statistical methods:
  - Threshold Metric
    - A minimum of *m* and maximum of *n* events are expected to occur
  - Statistical Moments
    - Mean and Standard Deviation
  - Markov Model
    - Time/State based. The probability of an event happening given a previous event.

Anomaly Detection

- Other methods have been proposed/exist:
  - Neural Network
    - An offshoot of Artificial Intelligence, NN's have proved highly successful in a number of machine learning applications
  - Genetic Algorithms
    - A search technique used to find approximate solutions to optimisation and search problems.
  - Data Mining
    - Searching large volumes of data for patterns.
  - Computer Immunology
    - Algorithms designed to exploit the immune system's characteristics of learning and memory

Anomaly Detection

- Advantages:
  - Detect unusual behaviour and therefore have the ability to detect symptoms of attacks with specific knowledge
  - Can produce information that can in turn be used to define signatures for misuse detectors
- Disadvantages:
  - Can produce a large number of false positives due to unpredictable behaviour
  - Large “training sets” are required in order to characterise normal behaviour

Comparison

- menti

Conclusions

Conclusions

- Networks has facilitated the widespread use of computing systems
- Also opened up a wide range of security concerns
- Firewalls, Intrusion Detection Systems, Network configurations and Encryption all help in providing *a level* of security
- Defense-in-Depth!

UNIVERSITY OF PLYMOUTH

Dr Hai-Van Dang

hai-van.dang@plymouth.ac.uk

Centre for Security, Communications & Network Research

www.plymouth.ac.uk/cscan