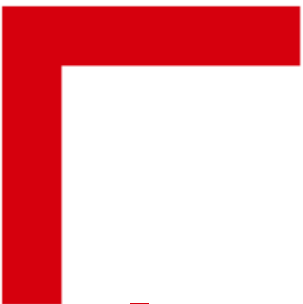





**QUEEN'S
UNIVERSITY
BELFAST**



Introduction to Network Security – Part 2



Dr. Sandra Scott-Hayward

CSC3064 Lecture 03

School of Electronics, Electrical Engineering and Computer Science

Session Overview

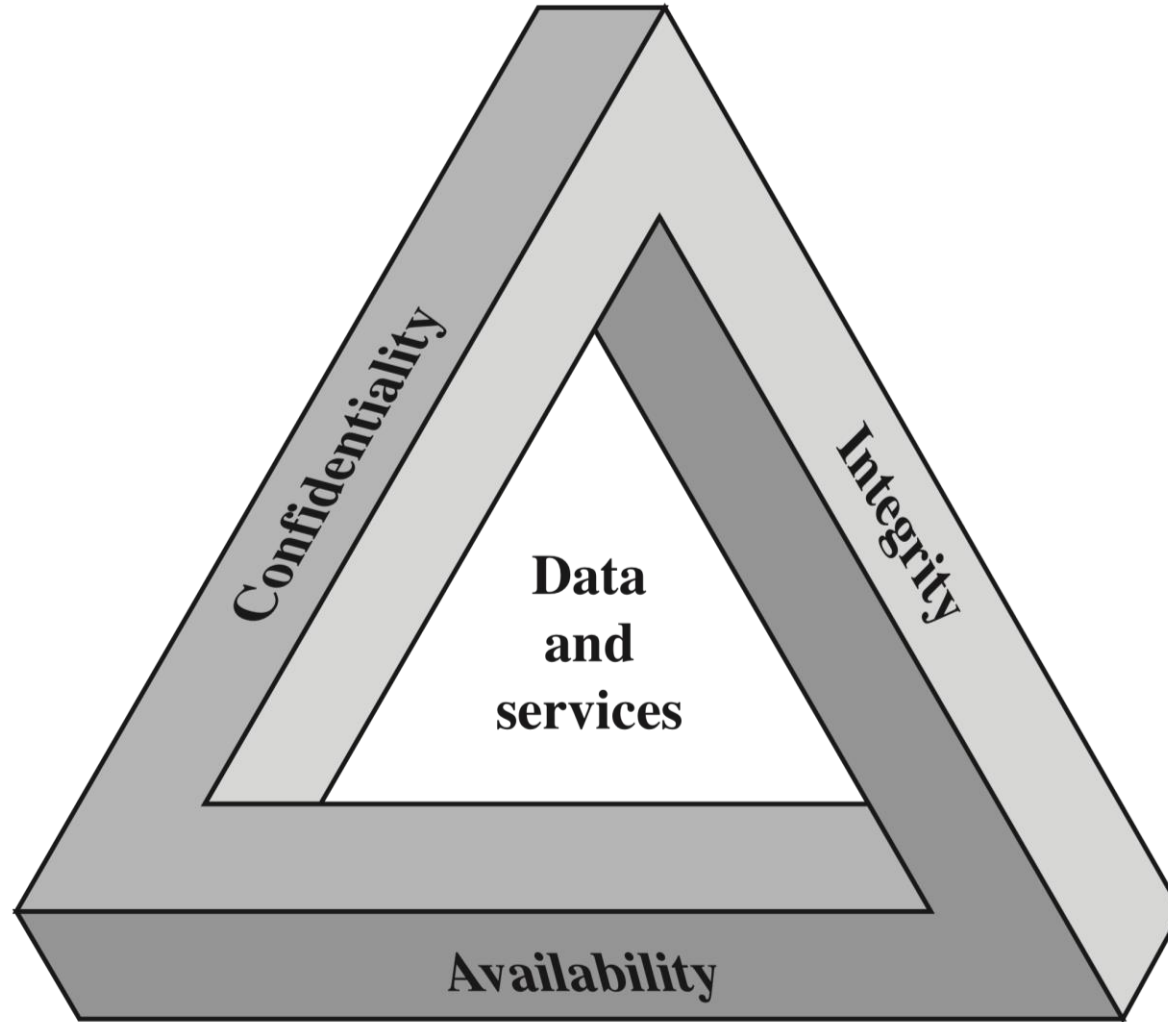
- ❑ Recap of Terminology
- ❑ Threats and Attacks
- ❑ Network Security Taxonomy

References:

Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2014.
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.



CIA Triad



Information Security Objectives

Confidentiality

- Data confidentiality
 - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
 - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
 - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
 - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability

- Assures that systems work promptly and service is not denied to authorized users

Additional Concepts

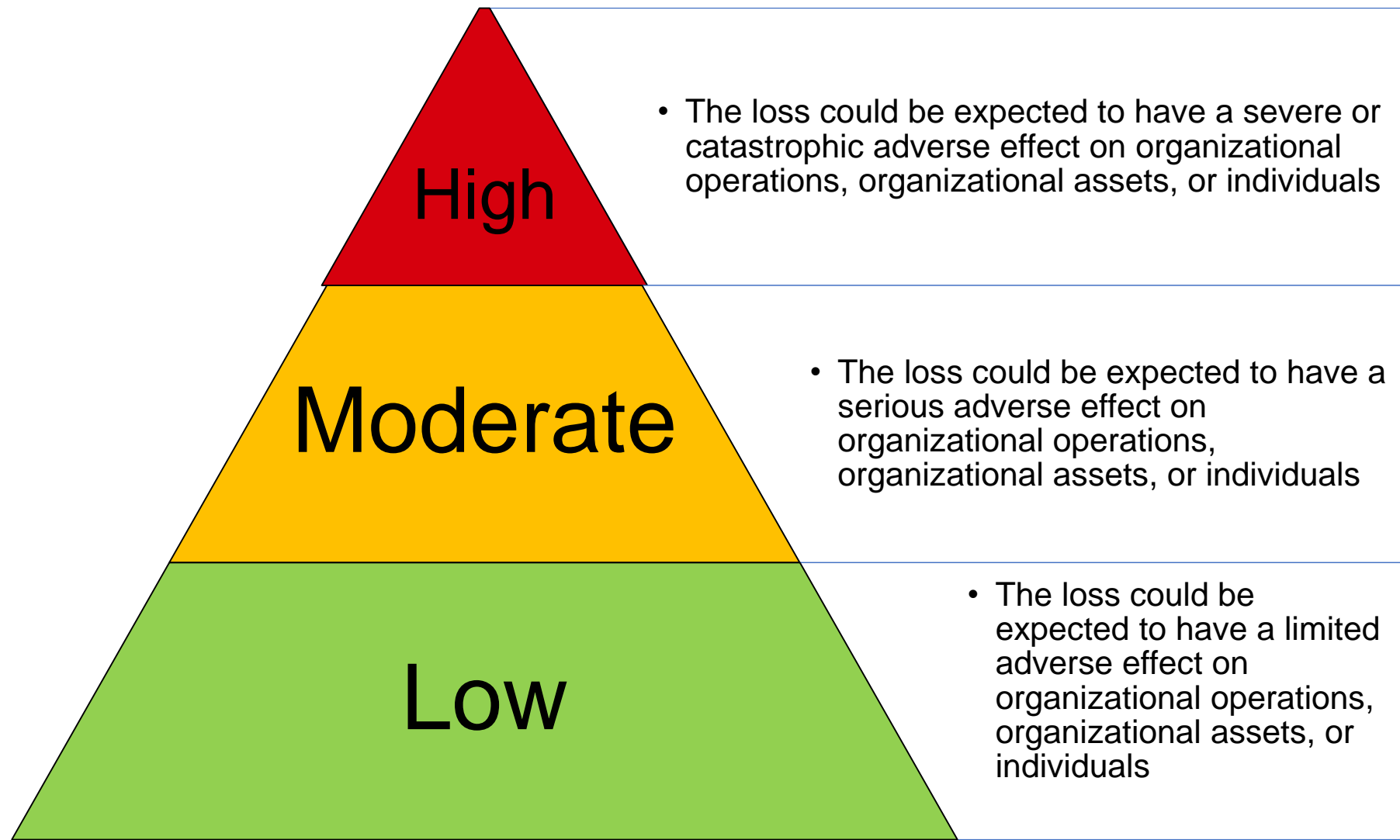
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Breach of Security – Levels of Impact



Examples of Security Requirements

Confidentiality

Student grade information is an asset whose confidentiality is considered to be highly important by students

In the U.S., this is regulated by the Family Educational Rights and Privacy Act (FERPA)

Integrity

Patient information stored in a database – inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability

A Web site that offers a forum to registered users to discuss some specific topic would be assigned a moderate level of integrity

An example of a low-integrity requirement is an anonymous online poll

Availability

The more critical a component or service, the higher the level of availability required

A moderate availability requirement is a public Web site for a university

An online telephone directory lookup application would be classified as a low-availability requirement



**QUEEN'S
UNIVERSITY
BELFAST**

Threats and Attacks (RFC 4949)

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

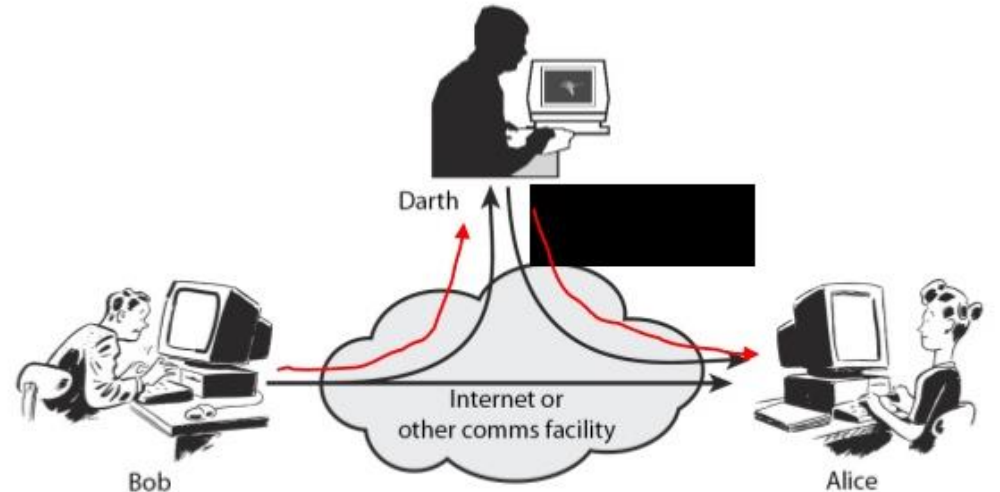
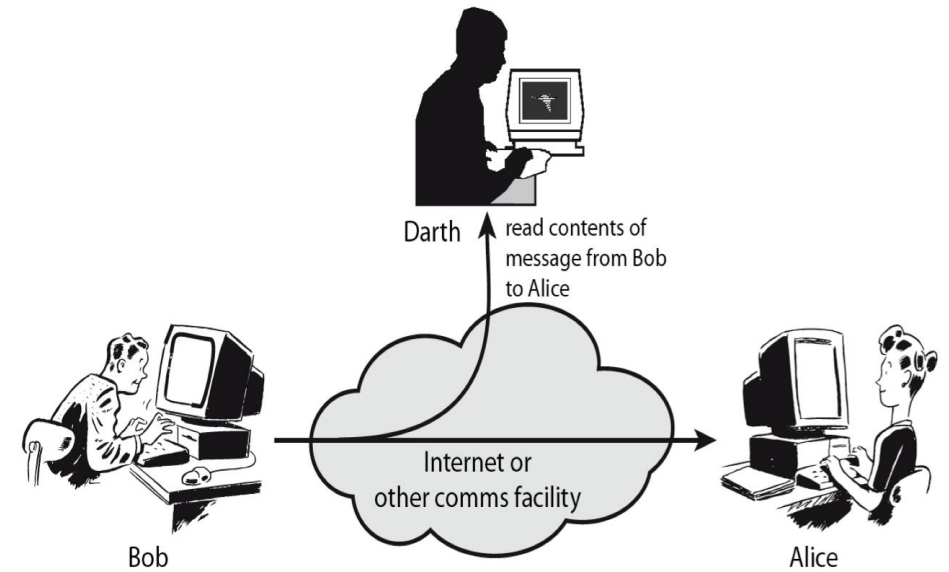
Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Internet Security Glossary - <https://tools.ietf.org/html/rfc4949>

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A ***passive attack*** attempts to learn or make use of information from the system but does not affect system resources
- An ***active attack*** attempts to alter system resources or affect their operation



Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted



Two types of passive attacks are:

- The release of message contents
- Traffic analysis

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

Security services

Defined by ITU X.800 as:

- A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers

<https://www.itu.int/rec/T-REC-X.800-199103-I/en>

Defined by RFC 4949 as:

- A processing or communication service provided by a system to give a specific kind of protection to system resources

X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

AUTHENTICATION	DATA INTEGRITY
<p>The assurance that the communicating entity is the one that it claims to be.</p> <p>Peer Entity Authentication Used in association with a logical connection to provide confidence in the identity of the entities connected.</p> <p>Data-Origin Authentication In a connectionless transfer, provides assurance that the source of received data is as claimed.</p>	<p>The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).</p> <p>Connection Integrity with Recovery Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.</p> <p>Connection Integrity without Recovery As above, but provides only detection without recovery.</p> <p>Selective-Field Connection Integrity Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.</p> <p>Connectionless Integrity Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.</p> <p>Selective-Field Connectionless Integrity Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.</p>
ACCESS CONTROL	NONREPUDIATION
<p>The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).</p>	<p>Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.</p>
DATA CONFIDENTIALITY	
<p>The protection of data from unauthorized disclosure.</p> <p>Connection Confidentiality The protection of all user data on a connection.</p> <p>Connectionless Confidentiality The protection of all user data in a single data block</p> <p>Selective-Field Confidentiality The confidentiality of selected fields within the user data on a connection or in a single data block.</p> <p>Traffic-Flow Confidentiality The protection of the information that might be derived from observation of traffic flows.</p>	<p>Nonrepudiation, Origin Proof that the message was sent by the specified party.</p> <p>Nonrepudiation, Destination Proof that the message was received by the specified party.</p>

Authentication

Concerned with assuring that a communication is authentic

- In the case of a single message, assures the recipient that the message is from the source that it claims to be from
- In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are specified in X.800:

- Peer entity authentication
- Data origin authentication

Access control

- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual

Data confidentiality

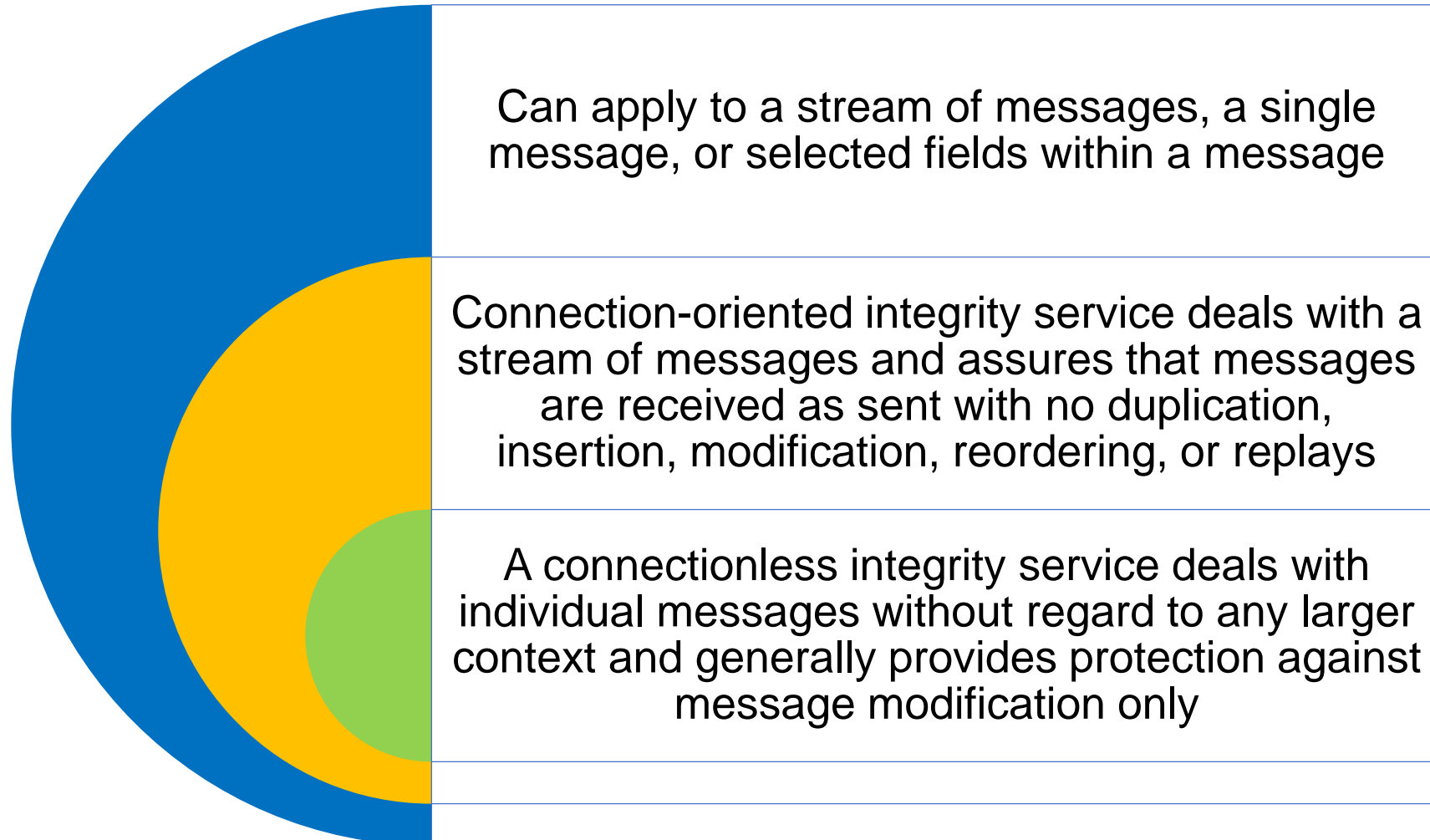
The protection of transmitted data from passive attacks

- Broadest service protects all user data transmitted between two users over a period of time
- Narrower forms of service include the protection of a single message or even specific fields within a message

The protection of traffic flow from analysis

- This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Data integrity



Non-repudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

Availability

Availability

- The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system

Availability service

- One that protects a system to ensure its availability
- Addresses the security concerns raised by denial-of-service attacks
- Depends on proper management and control of system resources

Model for network security

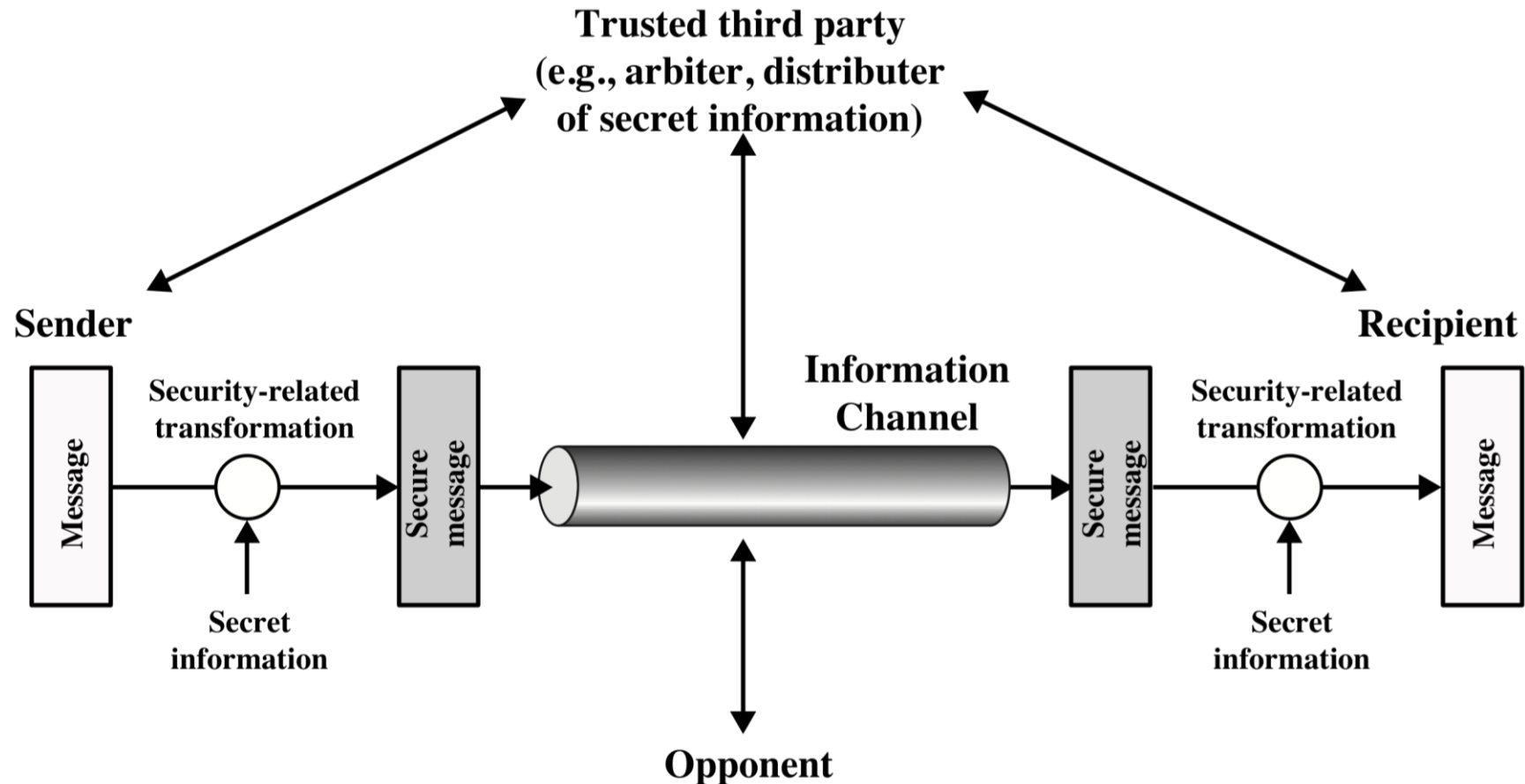


Figure 1.2 Model for Network Security

Network access security model

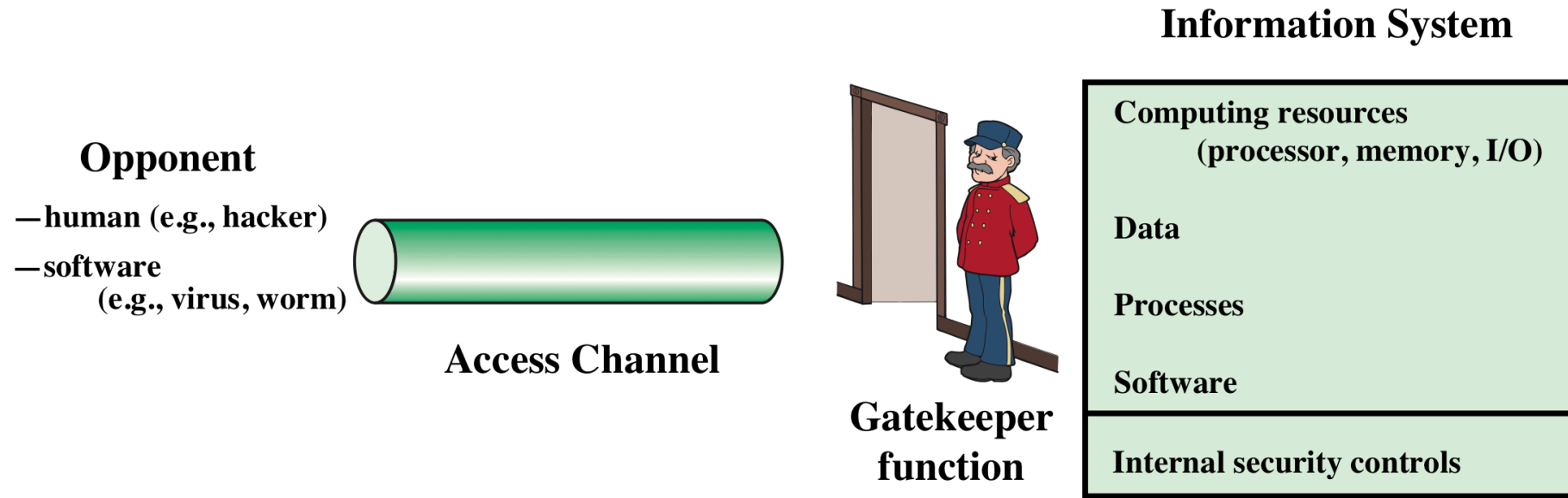


Figure 1.3 Network Access Security Model

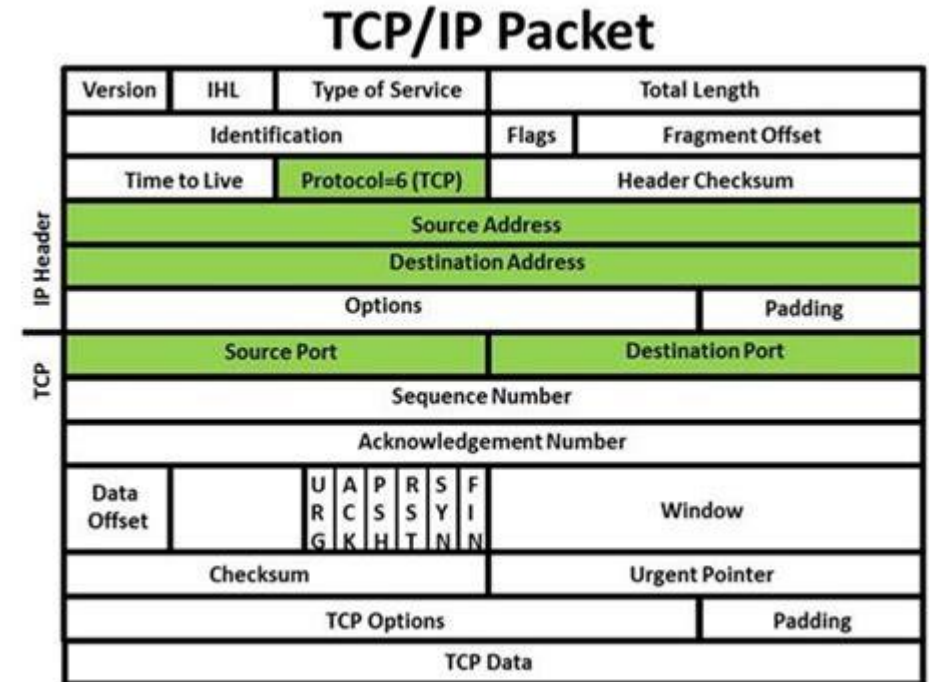
Network security taxonomy

- Header based
- Protocol based
- Authentication based
- Traffic Based



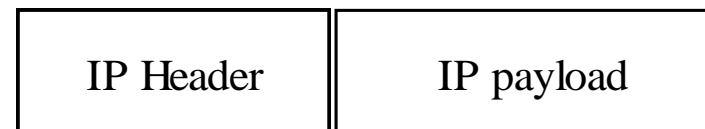
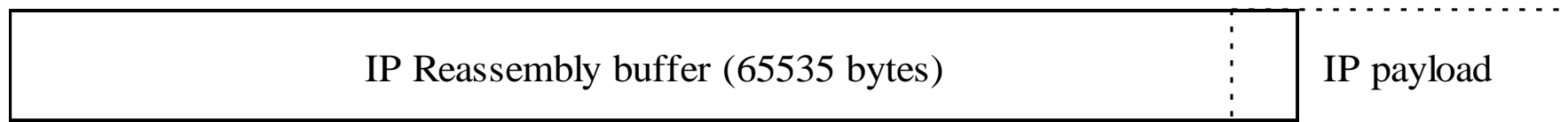
Header based attacks

- Creation of invalid packets, different protocols handle bad packets differently
- Source and destination address manipulation
 - Device can be confused by setting source and destination to the same address
- Setting bits in the header that should not be set
- Putting values in the header that are above or below the level specified in the standard



Header based – Example: Ping of Death

- Correctly formed ping is 64 bytes including IP header
- IPv4 packet may be as large as 65,535 bytes



For a detailed description, see:

<https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/>

offset = 65528 (max value)
length = 100

Network based attacks

Network Protocol Issues:

Timing / procedural

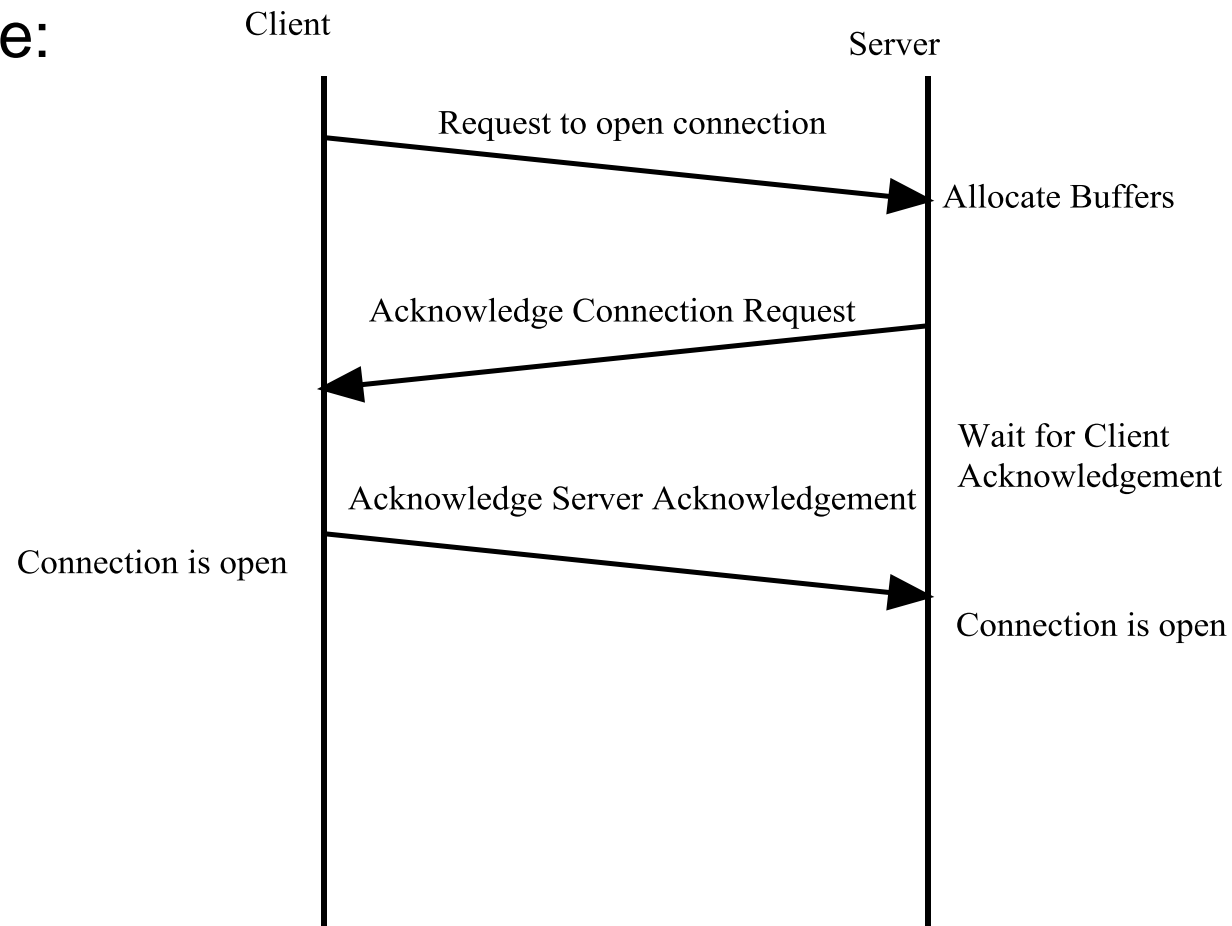
- Who talks first, who says what and when
- Think of a phone call conversation; there is a protocol, the person picking up the phone talks first
- Attacks usually involve valid packets that are out of order, arrive too fast, or are missing packets

Network Protocol Attacks:

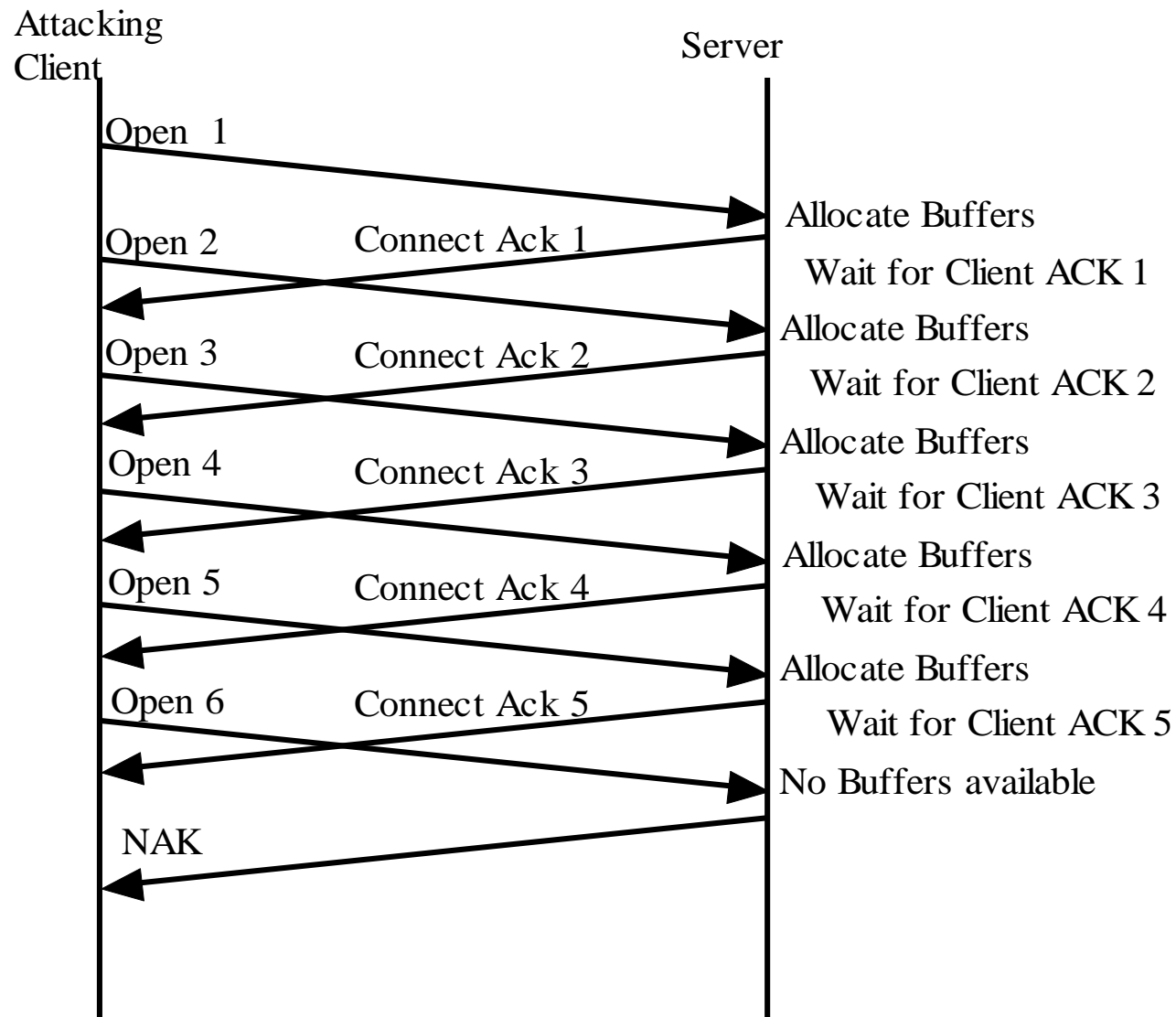
- You can shutdown the protocol itself
- Send packets telling the device to stop talking
- For connectionless protocols you can answer as the server and tell the client the server is down.

Network based – Example: SYN Flood (1)

TCP 3-way handshake:



Network based – Example: SYN Flood (2)



Authentication based attacks

- Authentication is the proof of one's identity to another
- Often thought of as username & password based
- In a network, addresses are often used to authenticate packets
 - Like the 4 addresses used to identify a packet in the Internet

RANK	Password	Change	RANK	Password	Change
1	123456	Unchanged	13	monkey	New
2	password	Unchanged	14	login	Down 3
3	12345678	Up 1	15	abc123	Down 1
4	qwerty	Up 2	16	starwars	New
5	12345	Down 2	17	123123	New
6	123456789	New	18	dragon	Up 1
7	letmein	New	19	password	Down 1
8	1234567	Unchanged	20	master	Up 1
9	football	Down 4	21	hello	New
10	iloveyou	New	22	freedom	New
11	admin	Up 4	23	whatever	New
12	welcome	Unchanged	24	qazwsx	New
			25	trustno1	New

Network authentication

Four different types of authentication:

- User to Host, Host to User, Host to Host, User to User

Example: Brute-Force attack

Allows an attacker to guess a person's user name, password, credit card number, or cryptographic key by using an automated process of trial and error.

```
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: password (3 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 1 complete) Password: 123456789 (2 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 1 complete) Password: password (3 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: success (4 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: asdfghjkl (5 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 1 complete) Password: success (4 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: 11111111 (6 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 1 complete) Password: asdfghjkl (5 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 1 complete) Password: 11111111 (6 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: iloveyou (7 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: letmein (8 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 1 complete) Password: iloveyou (7 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: admin (2 of 3, 1 complete) Password: wonderhow2 (9 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 2 complete) Password: letmein (8 of 9 complete)
ACCOUNT CHECK: [ssh] Host: 1 .103 (1 of 1, 0 complete) User: user (3 of 3, 3 complete) Password: wonderhow2 (9 of 9 complete)
ACCOUNT FOUND: [ssh] Host: 1 .103 User: user Password: wonderhow2 [SUCCESS]
```

Traffic based attacks

Traffic Issues:

- Too much data

To a single:

- Application
- Network device
- Protocol layer

From:

- Multiple machines
- Single attackers
- Traffic Capture (sniffing)

Traffic Attacks:

You can shutdown a service by:

- flooding it with packets
- opening a large number of connections

You can shutdown a network by:

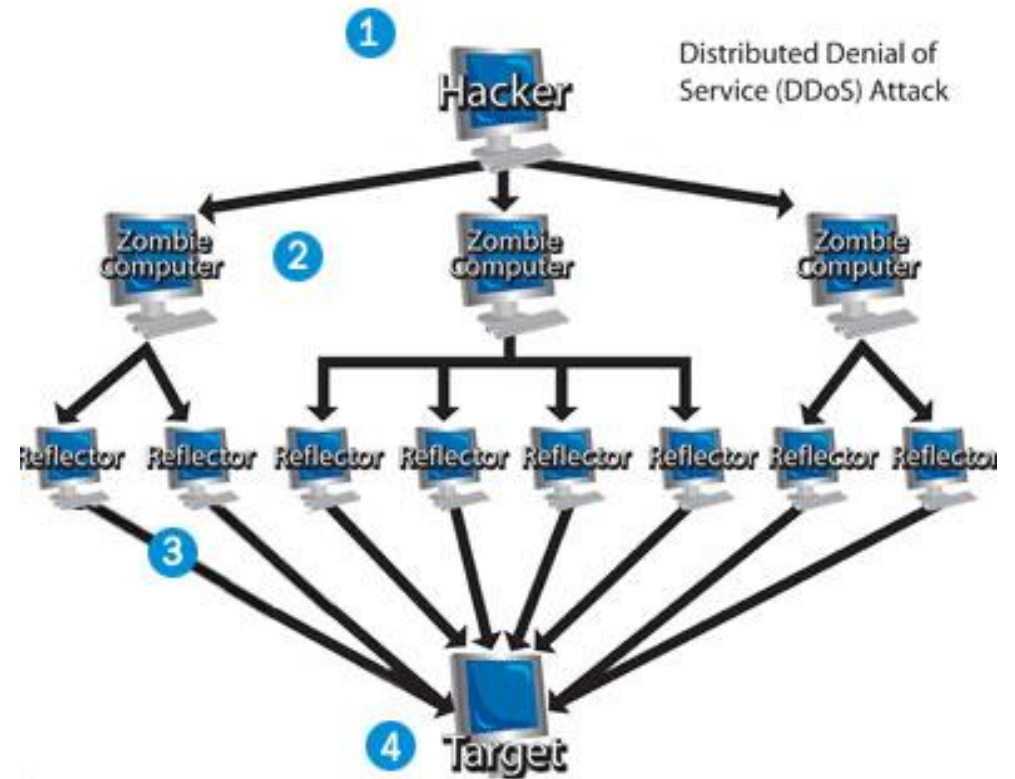
- flooding it with a large number of packets.
- Broadcast packets will do the most damage

You can shutdown a machine by:

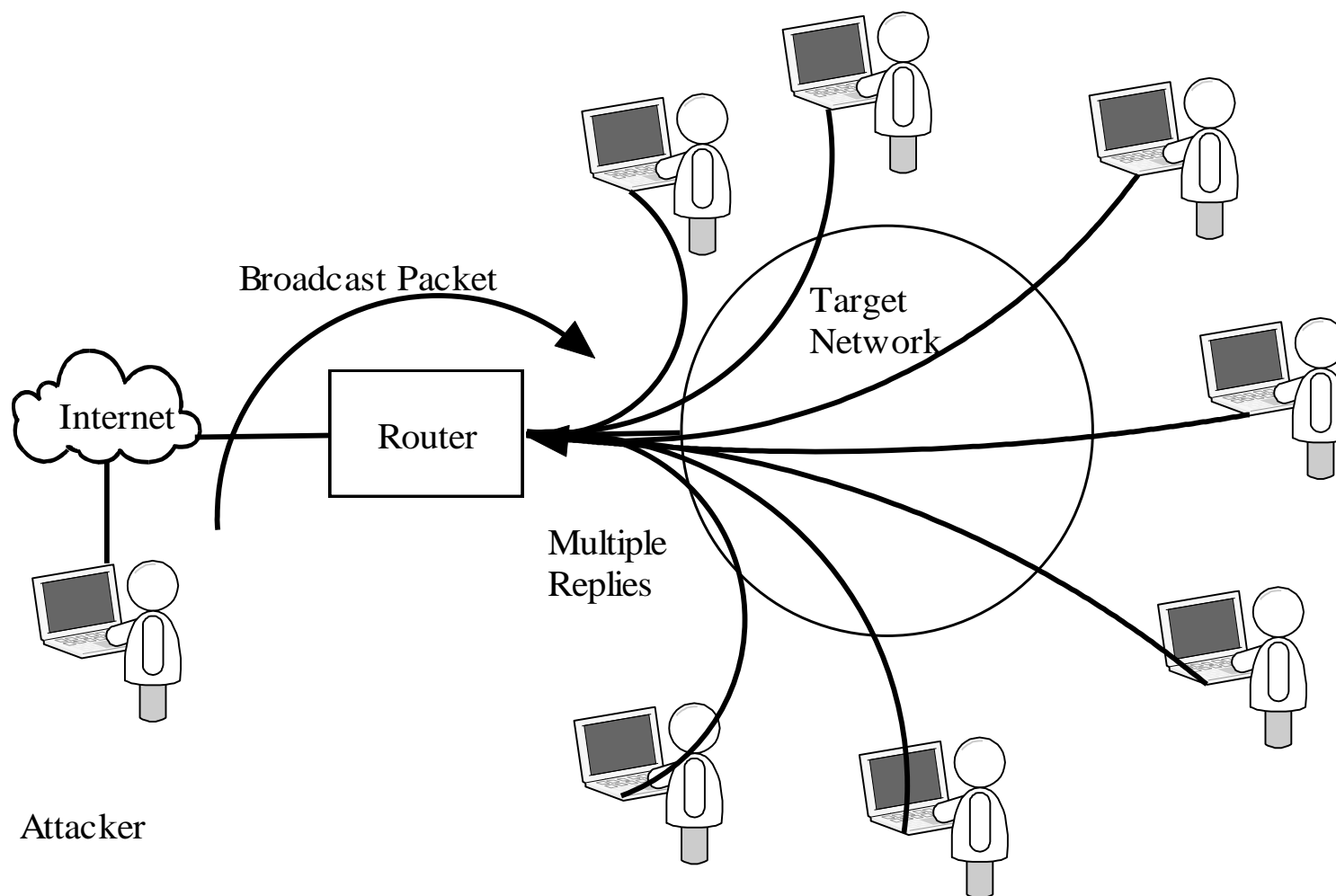
- flooding a machine with packets on multiple services
- Broadcast storms

Traffic based – Example: Denial of Service

- Denial of service is when a third party prevents valid network users access to services, machines, or applications
- Denial of service attacks can be difficult to detect and even harder to defend against



Traffic based – Example: Broadcast Flood



Traffic based – Example: Sniffing

- Packet sniffing can be played out against any layer in the network if the attacker is in a position to “see” the traffic.



Mirai Botnet DDoS Attack -

- Scanner runs on each Bot
- Uses Telnet to randomly attempt login to IP addresses, cycle through factory default usernames/passwords

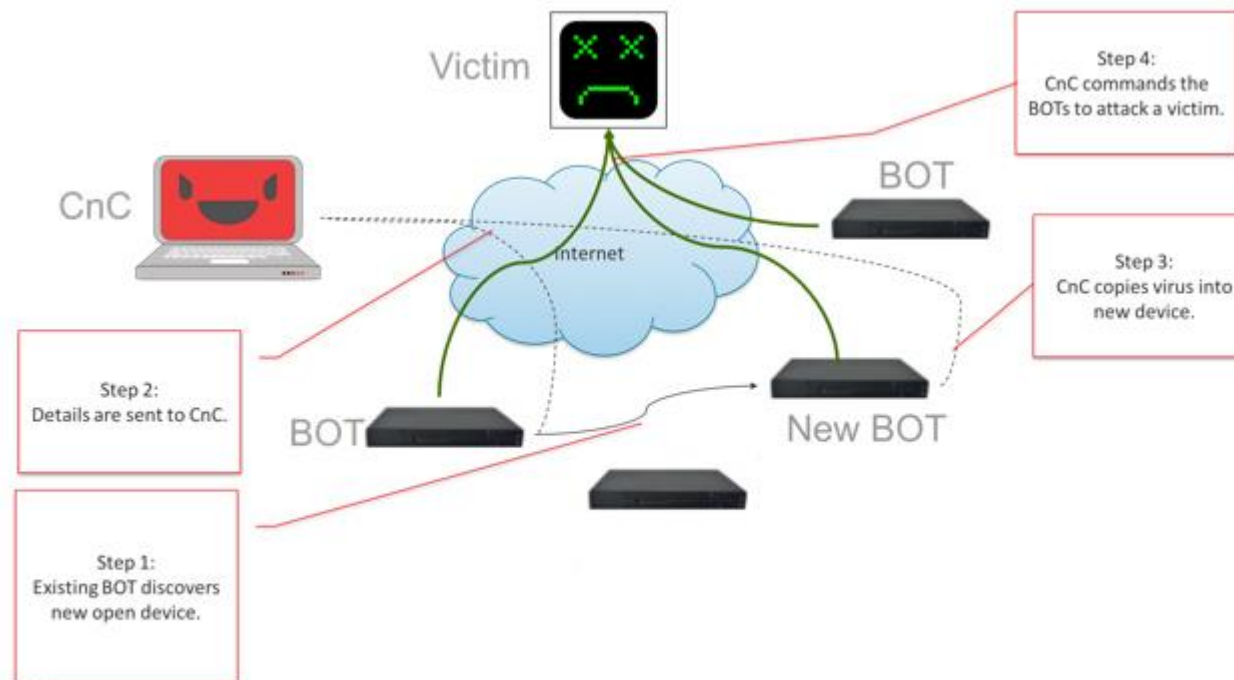


Figure 1 Mirai System

<https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html>

Summary

- ❑ CIA – Security Objectives, Requirements
- ❑ Security Attacks – Passive and Active
- ❑ Security Services – Authentication etc.
- ❑ Network Security Taxonomy – Header-based attacks etc.

Code of Conduct

DO NOT PEN-TEST THE QUB NETWORK OR ANY OTHER PUBLIC NETWORK

- Studying network security means it is necessary to learn about offensive actions and attack techniques. You must use this knowledge responsibly. Such experiments must be confined to the virtual machines provided for the practicals.
- The University has policies relating to information security and acceptable use of computer systems. Breaches of the security policies will be investigated in accordance with the University's disciplinary procedures. You should make yourself aware of these policies:

<http://www.qub.ac.uk/directorates/InformationServices/Services/Security/#Policies>

Questions?

Next Session: Tuesday, 22 January 2019

Network Security Architecture – Part 1