# Computer Network Security

Lesson 1

Introduction to Computer Network Security

Lecturer: Dr Msagha J Mbogholi, PhD

# Content

- Introduction to Network Security
- OSI model and Network Security
- Challenges of Network Security
- Security Services
- Security Models
- Threat Models

# Part 1

## Introduction to Network Security

# Introduction to Network Security

- Let us understand what network security is all about.
- A network is a connection between things or people.
- Security refers to the way(s) in which things or people are kept safe and therefore not in any danger.
- Network security thus refers to the way(s) by which a connection between things is kept safe and therefore not in any danger.
- What “things” are being referred to?
- All the components that make up the network, i.e., hardware, software, information, and ..yes, even the network users.

# Definitions

Some common security vocabulary used in this course includes (Schneider, 1999):

- Vulnerability – a defect or weakness found in the network system, be it in design, operation or maintenance.
- Threat – someone or something capable of exploiting a vulnerability
- Attack – exploitation of a vulnerability (could be for good or bad purpose)
- Attacker – the one who carries out an attack
- Exploit – something that can be used for an attack
- Defender – person or process that mitigates an attack
- Risk – an assessment of the likelihood of an attacker or a threat using an exploit to attack or compromise the network.

# Security Dimensions

- A security dimension is an aspect of security that is used to protect the network.
- There are several dimensions as far as security is concerned, and these are defined in different domains.
- Network security is concerned with three dimensions of security:
    - Confidentiality
    - Integrity
    - Availability
- We can call these the CIA of network security

# Confidentiality

- Confidentiality is the way in which information is only accessed by those who are authorized to do so.
- In a network information can be in one of two states: residing in a device, or in transit to or from a device.
- Confidentiality dimension must ensure that information is not accessed by unauthorized users whether in a network device or in transit.
- There are different mechanisms for implementation of confidentiality, and these will be discussed later.

# Integrity

- Integrity ensures that the information is in the form in which it was entered into the system.
- Essentially this means that integrity ensures that the information has not been tampered with (modified) in any form.
- In a network integrity mechanisms need to be implemented at both source (where the information is stored) and in transit (between points where the information is being sent)

# Availability

- Availability simply means that authorized users can have access to the network as and when they need to use it.
- In the absence of availability the network will not be accessible and users can’t get services that the network is meant to provide.

# CIA

- Consider three friends: Ted, Bob and Tamia.
- When Ted sends a message to Bob he needs to be sure that only Bob can read the contents of his message. If there is a way that only Bob can do so it means the confidentiality of the message is maintained.
- If by a stroke of bad luck Tamia manages to get her hands on the message before it gets to Bob, she can alter it's contents. This means the integrity of the message is compromised.
- Ted is the usual courier of messages between Bob and Tamia (they don't want anybody to know they exchange messages); on the day he falls sick and doesn't come to school it means no messages will be exchanged between the two. This means the system (Ted) is not available, and thus availability is compromised.

# Part 2

## OSI & Network Security

# OSI and Network Security

- It is not possible to discuss network security without examining the role of the OSI model in this context.
- The OSI model was developed by ISO as a model for network engineers to use in 1984.
- It is a theoretical model/framework that seeks to explain what happens in a network, i.e. the functions of the network.
- The model does this by dividing the functions of the network using 7 layers.
- The key question is how security is applied using the model in order to understand in which layers it should be applied and how.

# OSI Model & Security

| Layer | Name | Purpose | Security Issues |
|---|---|---|---|
| 4 | Transport | Disassembly/Reassembly of segments | Attacks on ports and packet sequencing |
| 3 | Network | Packets movement (Packets/IP #) | Router based attacks, e.g. DDoS, router table poisoning, etc |
| 2 | Datalink | Frames movement (Frames/MAC #) | Errors in frame bits |
| 1 | Physical | Physical movement of data (Bits) | Eavesdropping (replays and insertion), DoS attacks, sniffing, etc |

# OSI Model & Security

| Layer | Name | Purpose | Security Issues |
|---|---|---|---|
| 7 | Application | For user applications (Data) | Direct system access at the layer |
| 6 | Presentation | Presentation of data to networks (translation, compression, encryption) | Provides encryption and translation between L7 and L5 |
| 5 | Session | Provides sessions (connection management/duplex, simplex) (Data) | Authentication and authorization issues on sessions |

# Part 3

## Challenges of Network Security

# Challenges of Network Security

The challenges in network security lie mostly with 3 issues:

- Understanding the different ways in which the network can be attacked
- Understanding the types of attacks the network is vulnerable to
- Who the attackers are

# How will the network be attacked?

There are 4 generic steps involved in every network attack:

1. Information Gathering – done by the attacker in order to gather as much information as possible about the network to be attacked. The main purpose of this is to find any weak points such as accessible ports, in the network.
2. Attack – if step 1 is successful the attacker launches an attack and accesses the defenses of the targeted network.
3. Change the padlock – the attacker will now create an entry that can be accessed whenever s/he wants by changing/modifying internal settings accordingly.
4. Camp – since the attacker now has access to the network they can now camp and attack internal network devices as well as external networks and devices from the infiltrated network.

# The 5 Steps Of Network Penetration

- Techrepublic report that according to the Certified Ethical Hacker (CEH) material there are 5 steps to successful network penetration. These 5 steps are very similar to the generic approach. See:
- https://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/

# Types Of Network Attacks

There are two broad classifications of network attacks:

1. Passive attack – this is an attack characterized by the attacker monitoring the goings-on of the targeted network with the purpose of monitoring or getting more information about the communication in that network. The danger of these types of attacks is that the admin may not be aware of the attack due to its passive nature.
2. Active attack – this is a direct attack on the information or on the network itself. This attack targets compromising the CIA of information.

# Categories of Network Attacks

- Access attacks – when the attacker wishes to access information that they are not authorized to see. This compromises the Confidentiality (c) of information. The attack may occur on a device or information in transit.
- Modification attacks – when the attacker seeks to modify information that they are not authorized to modify. This compromises the Integrity (I) of the information. This attack may occur on the device or information in transit.

# Categories Of Network Attacks (cont'd)

- Denial Of Service attack – this occurs when the attacker floods resources on the network such that they are not able to service legitimate users. This attack compromises the Availability (A) of the resources and/or the network as a whole.
- Repudiation attack – to repudiate is to refuse or to deny the validity of something. A repudiation attack occurs when there is an attempt to deny the validity of a transaction or to deliberately give false information. This compromises the accountability of the information or transaction.

# Specific Threats to the Network

- Snooping – this is a basic form of attack where the attacker goes through files with the hope of finding some specific information. This is also known as sniffing. A passive attack.
- Eavesdropping – this is mostly done electronically; the attacker positions himself between the source and the destination hoping to gain access to information. Of course the access is unauthorized. A passive attack.
- Interception – this happens when the attacker positions himself between the source and the destination. The attacker intercepts the information before it reaches its destination; from there the attacker may either let the information go on, modify it, or prevent it from reaching the destination. A man in the middle attack is a form of interception attack. An active attack.

# Specific Threats to the Network (cont'd)

- Change attack – where the attacker changes/modifies information in the network with the intention of misleading users or the public.
- Insertion attack – where the attacker inserts new information to existing information. The purpose is similar to a change attack.
- Deletion attack – the attacker in this case deletes existing information. Like the change and insertion attacks, the purpose is to mislead users or cause damage to an organization.

The above attacks are all classified as active attacks.

# Specific Threats to the Network (cont'd)

- Denial of Service (DoS) attack – in this scenario the attacker floods the resources of a network with the intention of denying legitimate users access to those resources. The attack is normally targeted at a server or router, but may also be targeted at other network resources such as printers. In DoS a single machine targets a single network device (also known as a host)
- Distributed Denial of Service (DDoS) attack – a DDoS is an all out attack on a single machine/device on the network. In this case several machines are used to attack the targeted host. This means that a DDoS is more intense and will ultimately cause more damage in the network.

# Specific Threats to the Network (cont'd)

- Masquerading – the attacker impersonates or pretends to be someone else on the network. They do this with the intention of impersonating a transaction or information on the network. This is the same as spoofing.
- Malicious code attack – this happens when the attacker injects some malicious code into the network with the aim of causing damage to devices and resources on the network. Such malicious code includes viruses, worms and Trojan horses
- Hacking – this is done by hackers who gain unauthorized access to the network. Their intentions may be good or bad.
- Cybervandalism – this occurs when the attacker gains access to the web server with the intention of defacing or just bringing the website down so that it can not be used by others.

# Specific Threats to the Network (cont'd)

- Theft – this happens when the network is physically attacked. The attacker may physically steal network resources with malicious intentions.
- Phishing – this is a form of attack where users are fooled into giving away their personal details thinking it is a legitimate website whereas it is not. Phishing has been improved to include the concept of the "evil twins" around WiFi access points (APs).
- Insider threats – these are the hardest form of attack to control since the attacker is an insider with access to most of the network resources.
- Attack forms are being modified by the day as the average network user becomes more familiar with the attacks. It is for this reason that the modern network security specialist needs to keep abreast of the different forms of attack that the network is vulnerable to; this will help in developing the right preventive defense mechanisms. This leads us to the next question. Who are the attackers?

# Who are the Attackers?

- Hackers – this term loosely refers to anybody who attacks a computer system. Their intentions though, vary. The term white hat hacker usually refers to a hacker who penetrates a system with the intention of exposing the flaws of that system; they do not steal, damage or corrupt any of the information in the network. A black hat hacker is one who attacks the network with the intention of stealing, corrupting or destroying information in the network. Black hats are also known as crackers. There is also a grey hat hacker who is a mix of a black hat and a white hat hacker.

# Who are the Attackers? (cont'd)

- Insiders – these are the most dangerous threat to an organization. They consist of users who are already authorized to use the system, employees, partners (who have access vide the extranet), or even temporary contractors. They will attack the network from inside causing a lot of damage to the information and even resources in the network.
- Cybercriminals – this is a person or group who attack networks with the main purpose of financial gain. They will attack networks with the purpose of stealing information or exposing vulnerabilities, then using these to demand money or steal it electronically. They are the modern day criminal who use cyber crime as a form of white collar crime.

# Who are the Attackers? (cont'd)

- Script Kiddies – as the name implies these are seen as newbies in cyber crime. They will use existing software to penetrate network systems and engage in a form of cyber crime such as cybervandalism or even steal information. In reality they are less experienced crackers.
- Cyberterrrorists – They will attack networks and sites based on their ideologies or religious beliefs. Unlike the hacker who does it for financial gain a cyber terrorist is interested in doing what hackers do but they are driven by different reasons.

# Who are the Attackers? (cont'd)

- Spies – this is the James Bond of the cyber world. They are hired to steal information from the network or a specific computer without leaving a trace that they were ever there; this implies that they are usually very skilled and tech savvy.
- As can be seen the network is exposed to so many different users with different intentions but all ultimately wishing to cause some form of damage or other. So, what are the generic forms of defense that can be used to protect the network?

# Defense Principles

- All networks should be defended from known forms of attack using 5 defense principles.  The application of these principles make up the remaining lessons of this course.
- The principles described in this introduction help the security implementer to understand what the principle is before studying the different implementations of it.

# Defense Principles (cont'd)

- Layering – This is the first defense principle. Layering should be used to protect the network by creating several layers of defense between a potential attacker and the network. Each layer should be difficult to penetrate thus making it literally impossible for the attacker to penetrate all the layers. Layering concept can be explained better by examining an onion which has several layers. As you peel each layer off you are more likely to tear more such that it's actually discouraging to continue the exercise unless you have a very motivating goal! Similarly with networking it should be equally difficult to penetrate all successive layers until the core network is accessed. In other security circles this principle is also referred to as defense- in- depth.

# Defense Principles (cont'd)

- Limiting – this principle is based on the concept of 'need to know'. The access to resources and information is limited to a bare minimum, i.e. only those who need to know. This means that access to files is limited only to those who use those files, while access to certain network resources such as routers is limited only to the personnel who maintain them. Access can be technological and/or physical; for example, using access control on electronic files such as read and write access for authorized personnel. Physical access control can include use of access cards, keys or passwords to access restricted areas.

# Defense Principles (cont'd)

- Diversity – this principle complements the layered approach. The idea is to make it as difficult for the attacker to penetrate the different layers by using diverse defense mechanisms at each layer. Think of the onion, cutting it results in tears as you progress right? This is how it should be with diversity. As with limiting one layer use a form of access control say a key, while a second layer may make use of a biometric scan, while a third layer may involve the use of a password, and so on. This can also be implemented in a software exclusive environment , where an attacker must penetrate several layers of software defense programs before accessing the network.

# Defense Principles (cont'd)

- Obscurity – obscurity is about hiding details; the less an attacker knows about a system they want to penetrate the harder it is to penetrate. This principle is also known as security by obscurity. As an example most hackers are able to penetrate a network by testing the vulnerability of that network. If the hacker does not know the components of the network then it makes it that harder to penetrate the network.
- In certain organizations obscurity is implemented to a tee; there is one that even had the desktops delivered without any logo or technical details availability such that even users had no idea what type or spec of desktop they were using.

# Defense Principles (cont'd)

- Simplicity – admittedly this is hard to achieve. The principle here is to make the defense system easy for the intended user to understand on the inside but make it as complex as possible for the attacker to penetrate on the outside. The balance here is hard to achieve but possible using today's software. As an example it is like a door lock which requires three stages to open from the outside; but from the inside its as simple as just pushing one button to open the same door.

# Part 4

Security Services

# Security Services

- These are the services used to counter the different categories of attacks defined earlier in this lesson.
- The X.800 standard also defines **Security Service** as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or data transfers. There is a small variation in what is defined in X.800 as this is mostly related to the OSI model protocol layers.

# Security Services (cont'd)

- Confidentiality – confidentiality ensures that only authorized users can access information in the network. In order to ensure confidentiality in the network there is a need to identify the vulnerable points in the network where confidentiality should be applied. These are information at source (physical and electronic) and information in transit.
- Confidentiality service should protect against access attacks and different mechanisms exist to implement confidentiality depending on the vulnerability point.

# Security Services (cont'd)

- Confidentiality vulnerability points and possible implementation mechanisms

| Vulnerability Point | Access Attack | Implementation Mechanism |
|---|---|---|
| Source (physical files) | Unauthorized access to the files | Locks, smart card/biometric scan entry |
| Source (electronic files) | Unauthorized access, tampering with data | Access control through the system, user rights, passwords |
| In transit (electronic) | Sniffers, eavesdroppers, interception | Encryption, tunneling protocols, VPNs |

# Security Services (cont'd)

- Integrity – this service ensures that the information has not been modified in any way, i.e. the data is correct and in its original form. Again the integrity of data can only be compromised at same points as in confidentiality, at the source and in transit.
- Integrity service will protect against both modification and repudiation attacks.  Repudiation as the information will change making it possible for the originator to deny the information was from him/her.

# Security Services (cont'd)

- Integrity vulnerability points and possible implementation mechanisms

| Vulnerability Point | Modification & Repudiation Attack | Implementation Mechanism |
|---|---|---|
| Source (physical files) | Unauthorized modification to the files | Signatures on documents, initialing every page, binding to prevent removal of individual pages, can also use seals/watermarks |
| Source (electronic files) | Unauthorized modification, repudiation of data | Digital signatures, access control (read but not write/modify) |
| In transit (electronic) | Interception | Encryption, digital signatures |

# Security Services (cont'd)

- Availability – this is the service that ensures that the network can be accessed and used by authorized users when they need to. It ensures continuity of services and resources. Availability refers to availability of information and the network itself
- The availability service protects against Denial of Service (DoS) attacks.

# Security Services (cont'd)

- Availability vulnerability points and possible implementation mechanisms

| Vulnerability Point | Denial of Service (DoS)Attack | Implementation Mechanism |
|---|---|---|
| Source (physical files) | No access to the files | Backup files |
| Source (electronic files) | No access to the files | Backup files |
| Network | DoS attack | Failover, Disaster Recovery (DR), Redundancy mechanisms |

# Security Services (cont'd)

- Security services as defined by X.800 are Availability, Access Control, Authentication, Confidentiality, Integrity, Non-repudiation and Availability.
- These are described in detail in the document freely available online at:
- https://www.itu.int/rec/T-REC-X.800-199103-I/en

# Part 5

Security Models

# Security Models

- The International Data Cooperation (IDC) present two generic models for network security.  A model is a representation and the Security Models suggest ways in which security services can be implemented in a network to protect it from attacks.
- http://www.idc-online.com/technical_references/pdfs/data_communications/A_Model_for_Network_Security.pdf
- These models are briefly explained.

# Security Models (cont'd)

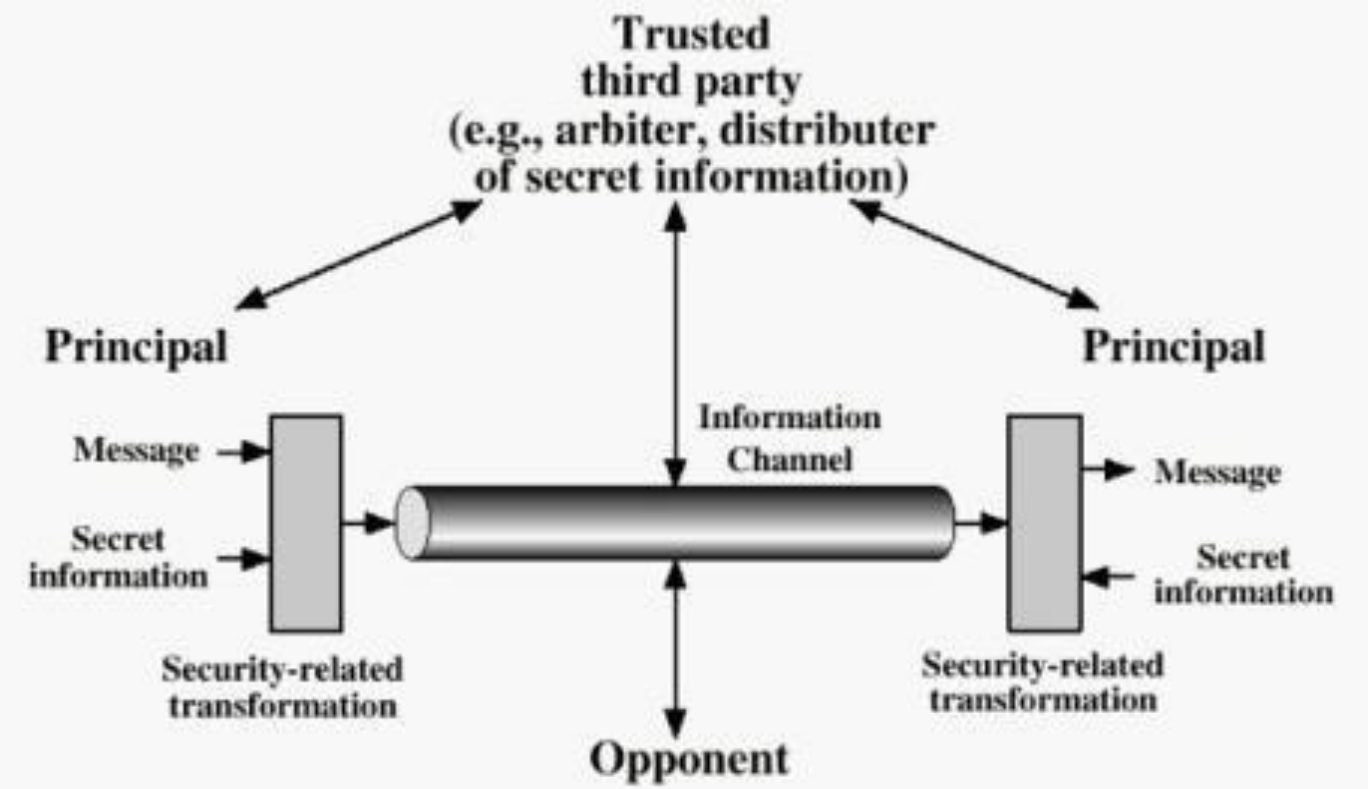


Figure 1.3 Model for Network Security

# Security Models (cont'd)

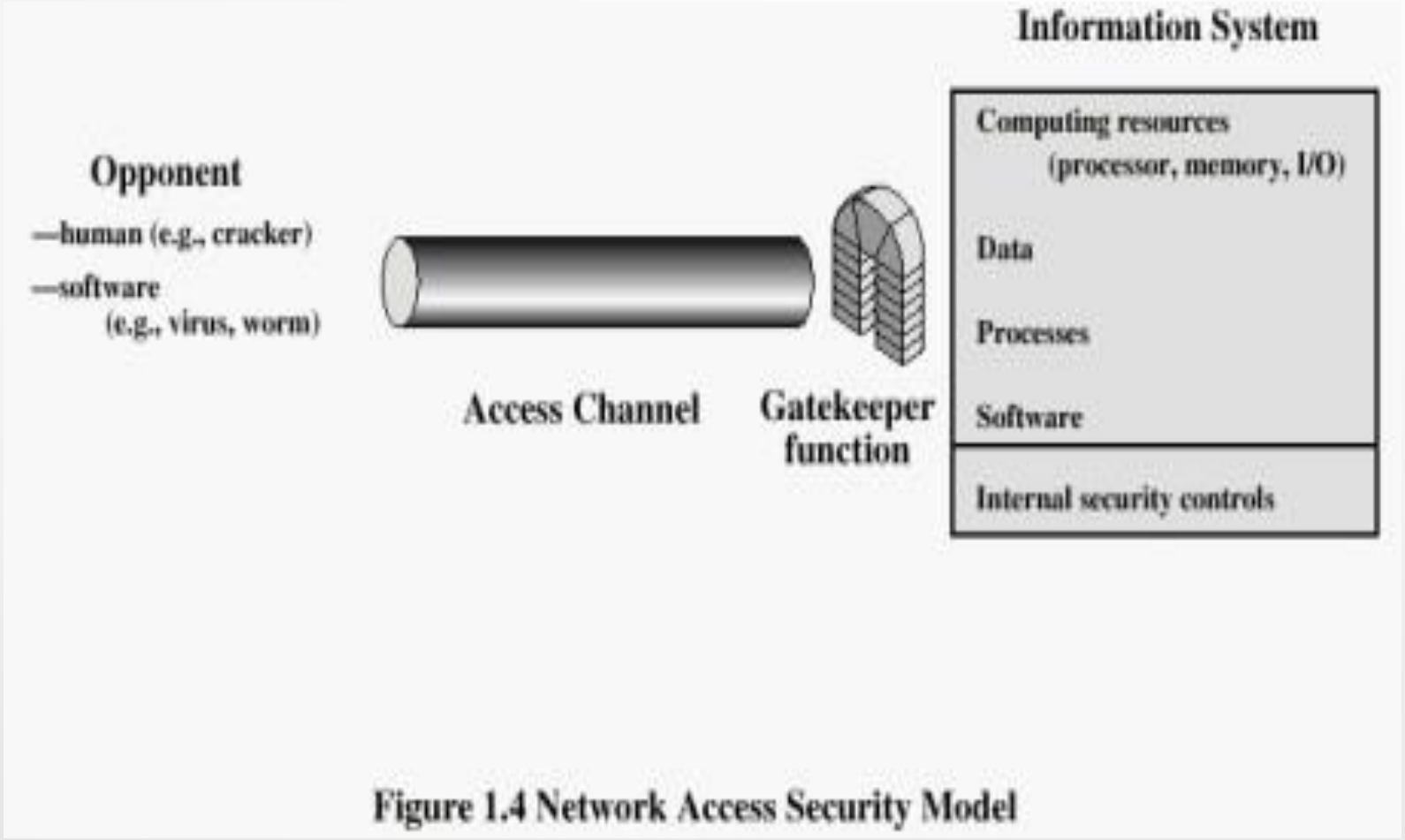


Figure 1.4 Network Access Security Model

# Part 6

Threat Models

# Threat Models

- Threat modeling is the process by which threats to the network can be identified.
- In a standard network there can only be one or both types of attackers: an internal attacker or an external attacker.
- The damage that will occur may be intentional or accidental, but either way the damage has happened.
- A threat model explores the attacks that the network is vulnerable to with a view to devising ways and means of preventing those attacks.
- In networking environments the threat model can be used to test the environment in order to identify threats and possible solutions to the threats; it is a fairly common practice

# Threat Models (cont'd)

- An example of a threat model is presented below:

| Name | Type | Classification | Cause | Measures |
|---|---|---|---|---|
| Access | Internal | High risk | No annual bonus for employees | Review access rights in sensitive areas |
| | | | | |
| | | | | |

# Summary

- Network security is concerned with the CIA dimensions: Confidentiality, Integrity & Availability
- The OSI model explains the different security issues in the 7 layers
- The challenges in network security lie mostly with 3 issues: how will the network be attacked, what type of attack will it be, who is attacking us.
- The 5 defense principles upon which all defense mechanisms are based: layering, limiting, diversity, obscurity, simplicity
- Security services used to counter different categories of attacks: Confidentiality, Integrity, Availability. The X.800 document adds more categories and relates them to the OSI model
- There are 2 models proposed by IDC as generic security service models: Secure Channel Communication and Network Access Security Model
- Threat modeling is the process by which threats to the network can be identified.

# References


- Ciampa, M. (2012). *Security+ Guide to Network Security Fundamentals* (4th ed.). Course Technology.
- Maiwald, E. (2001). *Network Security: A Beginner's Guide* (1st ed.). Osborne_McGraw Hill.
- Krawetz, N. (2007). *Introduction to network security* (1st ed.). Charles River Media.
- Schneider, F. (1999). *Trust in Cyberspace*. National Academy Press, Washington D.C.
- http://www.idc-online.com/technical_references/pdfs/data_communications/A_Model_for_Network_Security.pdf
- https://www.itu.int/rec/T-REC-X.800-199103-I/en
- https://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/