UNIVERSITY OF WESTMINSTER

Cyber Security Concepts and Principles

6COSC019W- Cyber Security

Dr Ayman El Hajjar

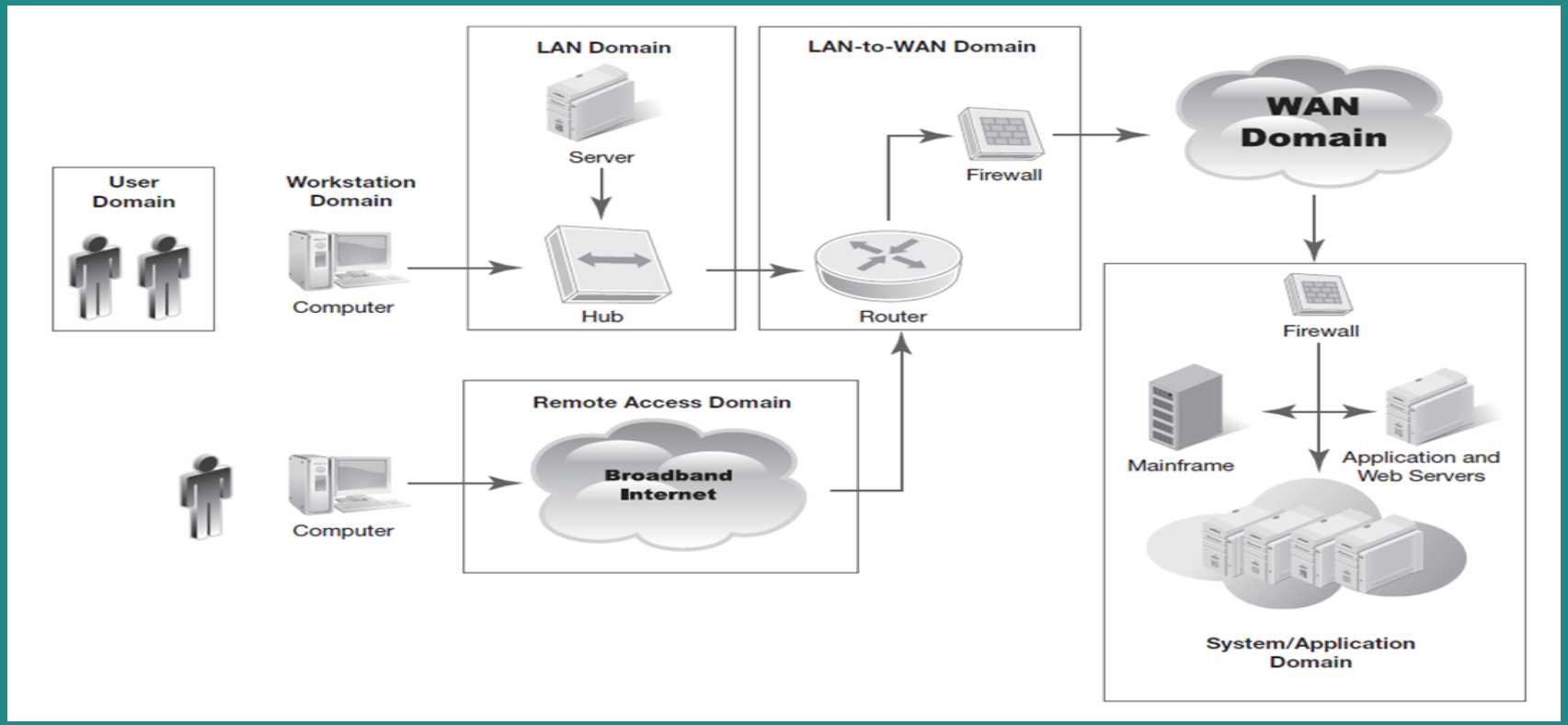
January 23, 2023

School of Computer Science and Engineering
University of Westminster

Outline

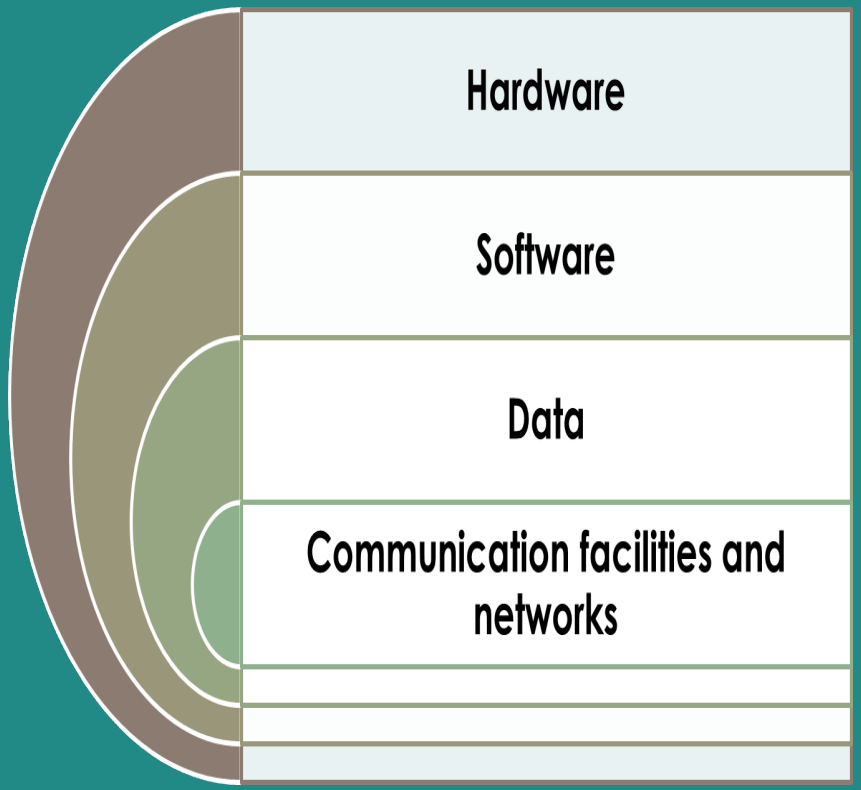
Information Systems

INFORMATION SYSTEM ASSETS



What Are We Trying to Protect?

- Customer data
- IT and network infrastructure
- Intellectual property
- Finances and financial data
- Service availability and productivity
- Reputation



Cyber Security Fundamentals

CYBER SECURITY- A DEFINITION

The NIST Computer Security Handbook definition

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)"

Cyber Security objectives

Confidentiality

- **Data Confidentiality**- Assures that private 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

Cyber Security objectives

Confidentiality

- **Data Confidentiality**- Assures that private 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 any manipulation.

CYBER SECURITY OBJECTIVES

Confidentiality

- **Data Confidentiality**- Assures that private 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 any manipulation.

Availability

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

And some possible additional concepts Objectives

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

Authenticity

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

And some possible additional concepts Objectives

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are as follows:

Authenticity

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

Accountability

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

CIA Triad

- **Confidentiality**, **Integrity**, **Availability** are the three concepts form what is often referred to as the CIA triad.
- The three concepts embody the fundamental security objectives for both data and for information and computing services.

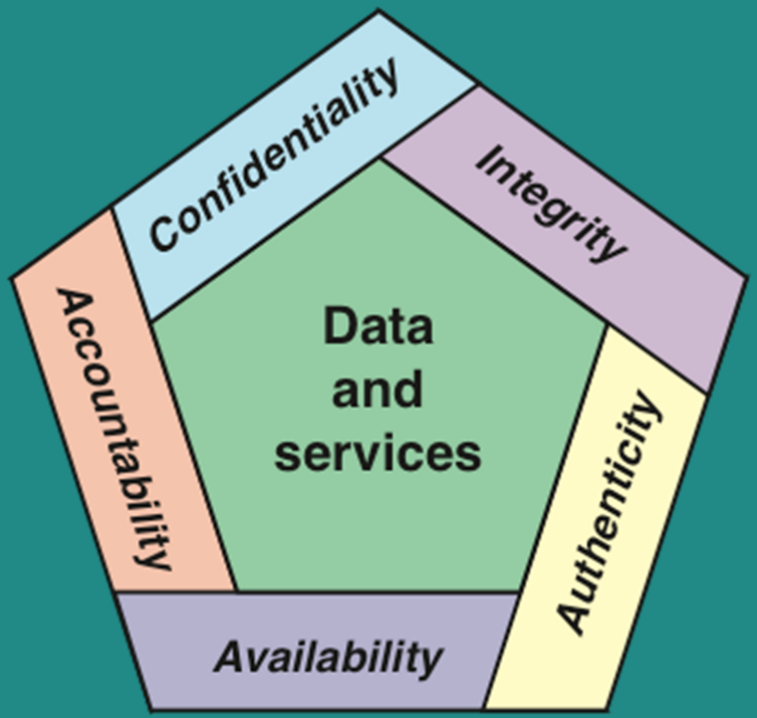


Figure 1: CIA Triad- Confidentiality, Integrity, Availability

What Is a Security Breach?

- Any event that results in a violation of any of the CIA security tenets
- Some security breaches disrupt system services on purpose
- Some are accidental and may result from hardware or software failures

Breach of Security Levels of Impact

High

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Breach of Security Levels of Impact

High

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Moderate

- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

Breach of Security Levels of Impact

High

- The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Moderate

- The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

Low

- The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Examples of Security Requirements

- **Confidentiality**
  - Student grade information is an asset whose confidentiality is considered to be highly important.
  - Regulated by the Data Protection Act in the UK.

Examples of Security Requirements

- **Confidentiality**
  - Student grade information is an asset whose confidentiality is considered to be highly important.
  - Regulated by the Data Protection Act in the UK.
- **Integrity**
  - Inaccurate Patients information could result in serious harm or death to patients 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.
  - A low-integrity requirement example is an anonymous online poll

Examples of Security Requirements

- **Confidentiality**
  - Student grade information is an asset whose confidentiality is considered to be highly important.
  - Regulated by the Data Protection Act in the UK.
- **Integrity**
  - Inaccurate Patients information could result in serious harm or death to patients 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.
  - A low-integrity requirement example is an anonymous online poll
- **Availability**
  - Critical components need a high level of availability.
  - A moderate availability requirement is a public university Web site.
  - An online telephone directory lookup application would be classified as a low-availability requirement

Vulnerabilities, Threats and Attacks

- **Categories of vulnerabilities**
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)

Vulnerabilities, Threats and Attacks

- **Categories of vulnerabilities**
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- **Threats**
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset

Vulnerabilities, Threats and Attacks

- **Categories of vulnerabilities**
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- **Threats**
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- **Attacks (threats carried out)**
  - **Passive** – attempt to learn or make use of information from the system that does not affect system resources
  - **Active** – attempt to alter system resources or affect their operation
  - **Insider** – initiated by an entity inside the security parameter
  - **Outsider** – initiated from outside the perimeter

Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - analysis

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

EXAMPLES OF THREATS

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Cyber Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation

Attack surface

Attack Surface

- Consists of the reachable and exploitable vulnerabilities in a system
- Can be categorized in the following way:

Attack Surface

- Consists of the reachable and exploitable vulnerabilities in a system
- Can be categorized in the following way:
  - Network attack surface
    - This category refers to vulnerabilities over an enterprise network, wide-area network, or Internet

Attack Surface

- Consists of the reachable and exploitable vulnerabilities in a system
- Can be categorized in the following way:
  - Network attack surface
    - This category refers to vulnerabilities over an enterprise network, wide-area network, or Internet
  - Software attack surface
    - Vulnerabilities in application, utility, or operating system code

Attack Surface

- Consists of the reachable and exploitable vulnerabilities in a system
- Can be categorized in the following way:
  - Network attack surface
    - This category refers to vulnerabilities over an enterprise network, wide-area network, or Internet
  - Software attack surface
    - Vulnerabilities in application, utility, or operating system code
  - Human attack surface
    - Refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

In Depth Attack Surface Example

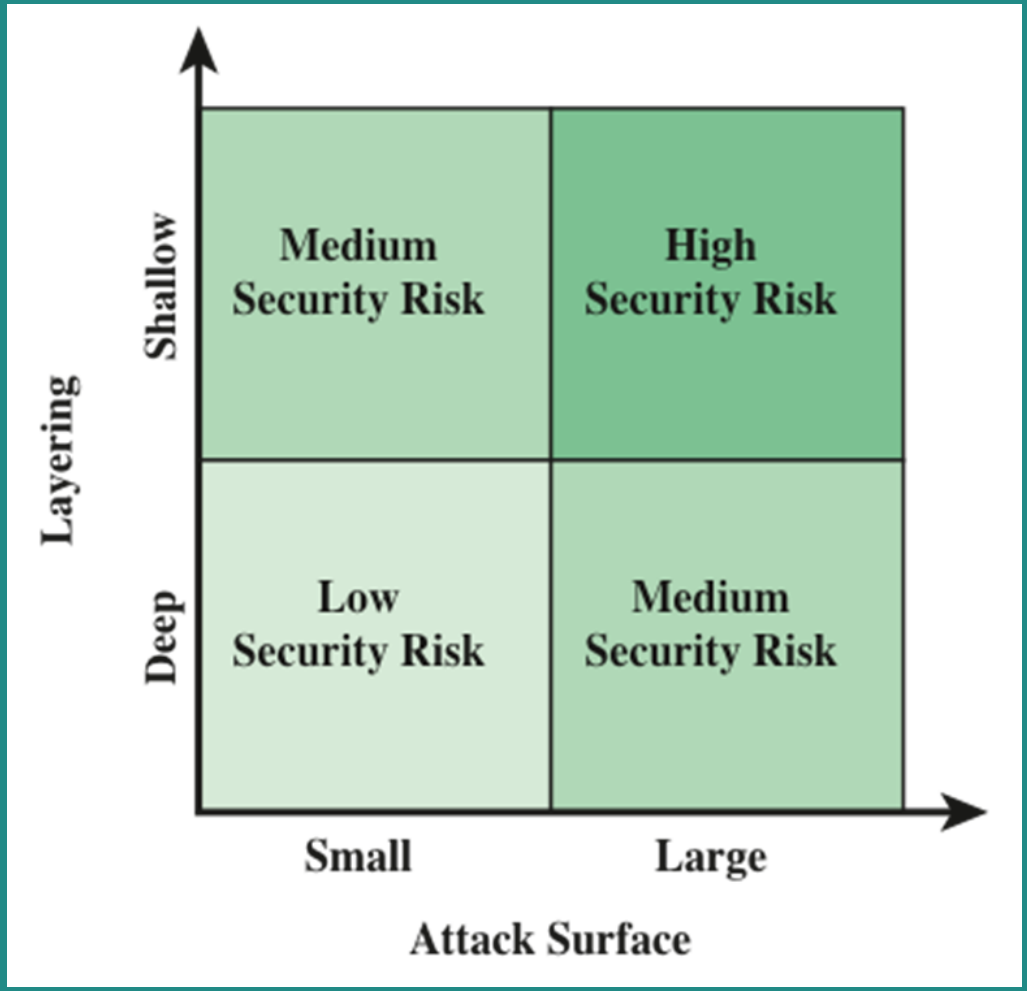


Figure 2: The use of layering, or defense in depth, and attack surface reduction complement each other in mitigating security risk.

ATTACK TREES

A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

The security incident that is the goal of the attack is represented as the root node of the tree

The ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree

Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared

The final nodes on the paths outward from the root, the leaf nodes, represent different ways to initiate an attack

Figure 3: Hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

AN ATTACK TREE FOR INTERNET BANKING AUTHENTICATION

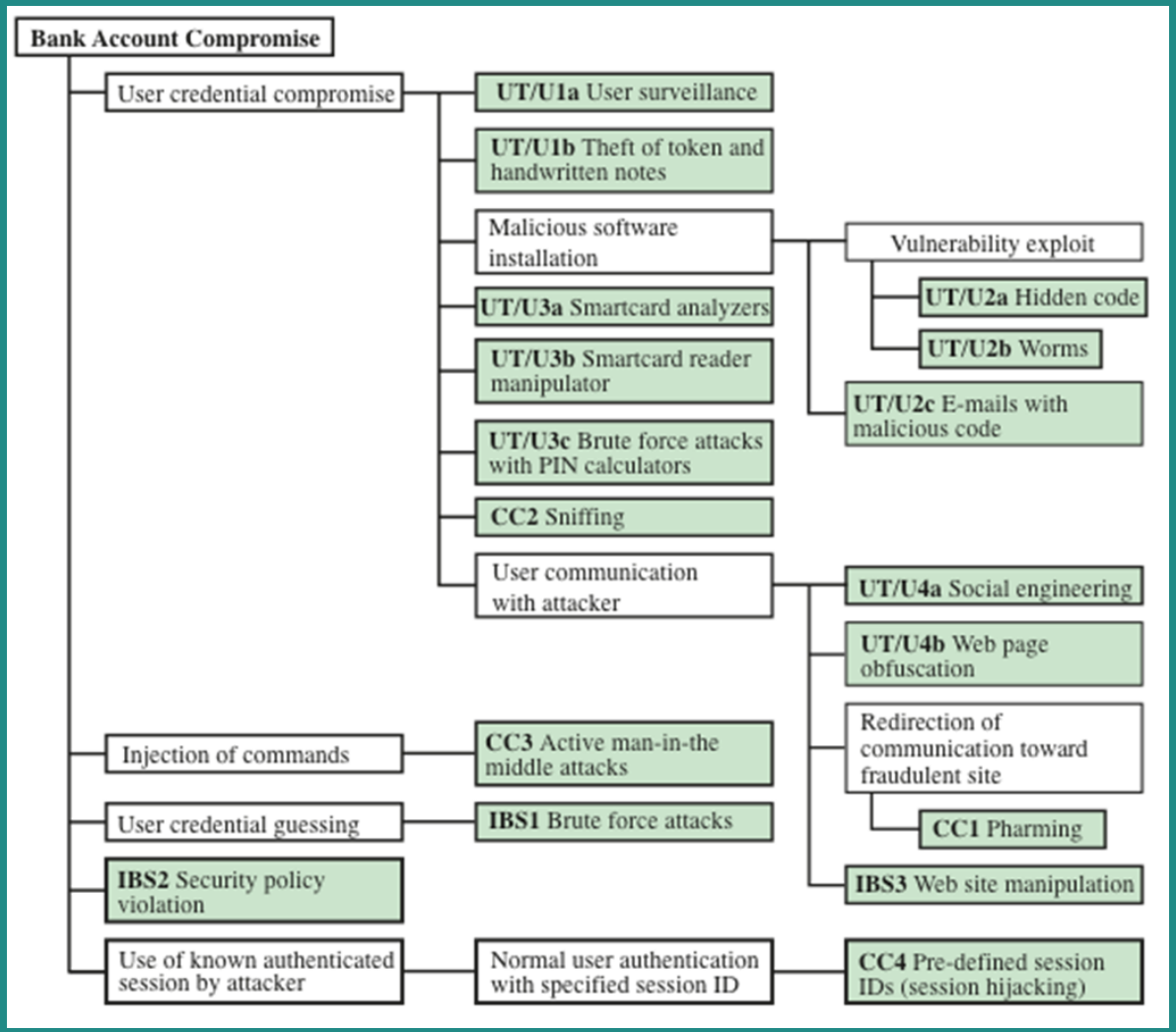


Figure 4: An example of an attack tree analysis for an Internet banking authentication application

Fundamental security design principles

THE TEN SECURITY PRINCIPLES

- The National Centres of Academic Excellence in Information Assurance/Cyber Defence, which is jointly sponsored by the U.S. Department of Homeland Security, list the following as fundamental security design principles:

Economy of mechanism

- The design of security measures embodied in both hardware and software should be as simple and small as possible
  - While applicable to most engineering endeavours, the notion of simplicity is especially important in the security domain, since a simple security framework facilitates its understanding by developers and users and enables the efficient development and verification of enforcement methods for it.

Fail-safe defaults

- Access decisions should be based on permission rather than exclusion—the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted
  - For example, when adding a new user to an operating system, the default group of the user should have minimal access rights to files and services. Unfortunately, operating systems and applications often have default options that favor usability over security.
  - This has been historically the case for a number of popular applications, such as web browsers that allow the execution of code downloaded from the web server.

COMPLETE MEDIATION

- Every access must be checked against the access control mechanism
  - As a consequence, one should be wary of performance improvement techniques that save the results of previous authorization checks, since permissions can change over time.
  - For example, an online banking web site should require users to sign on again after a certain amount of time, say, 15 minutes, has elapsed.

Open design

- The design of a security mechanism should be open rather than secret
  - Security should rely only on keeping cryptographic keys secret.
  - Open design allows for a system to be scrutinized by multiple parties, which leads to the early discovery and correction of security vulnerabilities caused by design errors.
  - The open design principle is the opposite of the approach known as security by obscurity, which tries to achieve security by keeping cryptographic algorithms secret and which has been historically used without success by several organizations.

Separation of privilege

- This principle dictates that multiple conditions should be required to achieve access to restricted resources or have a program perform some action.
- A practice in which multiple privilege attributes are required to achieve access to a restricted resource

LEAST PRIVILEGE

- Every process and every user of the system should operated using the least set of privileges necessary to perform the task
- Each program and user of a computer system should operate with the bare minimum privileges necessary to function properly.
  - If this principle is enforced, abuse of privileges is restricted, and the damage caused by the compromise of a particular application or user account is minimized.
  - The military concept of need-to-know information is an example of this principle.

LEAST COMMON MECHANISM

- In systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimized.
- The design should minimize the functions shared by different users, providing mutual security
  - For example, if a file or application needs to be accessed by more than one user, then these users should have separate channels by which to access these resources, to prevent unforeseen consequences that could cause security problems.

Psychological acceptability

- This principle states that user interfaces should be well designed and intuitive, and all security-related settings should adhere to what an ordinary user might expect.
- Implies that the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access

WORK FACTOR

- According to this principle, the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme.
  - A system developed to protect student grades in a university database, which may be attacked by snoopers or students trying to change their grades, probably needs less sophisticated security measures than a system built to protect military secrets, which may be attacked by government intelligence organizations.

COMPROMISE RECORDING

- This principle states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent it.
  - Internet-connected surveillance cameras are a typical example of an effective compromise record system that can be deployed to protect a building in lieu of reinforcing doors and windows.
  - The servers in an office network may maintain logs for all accesses to files, all emails sent and received, and all web browsing sessions.

Penetration testing

PENETRATION TESTING- AN INTRODUCTION

Penetration testing- An introduction

UK National Cyber Security Center defines Penetration Testing as: ”A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system’s security, using the same tools and techniques as an adversary might”

- **Penetration testing** is to test the security of systems and architectures from the point of view of an attacker (hacker, cracker)
- A penetration test should be thought of as similar to a financial audit. Your finance team tracks expenditure and income day to day. An audit by an external group ensures that your internal team’s processes are sufficient.

Penetration testing is NOT...

- Penetration testing is a core tool for analysing the security of IT systems, but it's not a magic bullet.
- An alternative to other IT security measures – it complements other tests
- Expensive game of Capture the Flag
- A guarantee of security

To Tell or Not To tell

- Telling too many people may invalidate the test
- However, you don't want valuable resources chasing a non-existent "intruder" very long
- And, elevation procedures make not telling risky

Tests basis

Tests can be carried out by testers armed with varying amounts of information about your system:

- **Whitebox testing**
  - Full information about the target is shared with the testers. This type of testing confirms the efficacy of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organisation's systems.
- **Blackbox testing**
  - No information is shared with the testers about the internals of the target.
  - This type of testing is performed from an external perspective and is aimed at identifying ways to access an organisation's internal IT assets.

Why Pentesting

- Mitigate risk
- Legal and compliance
- Validate/Invalidate Security Controls
- Find and Mitigate Vulnerabilities
- Prevent compromise

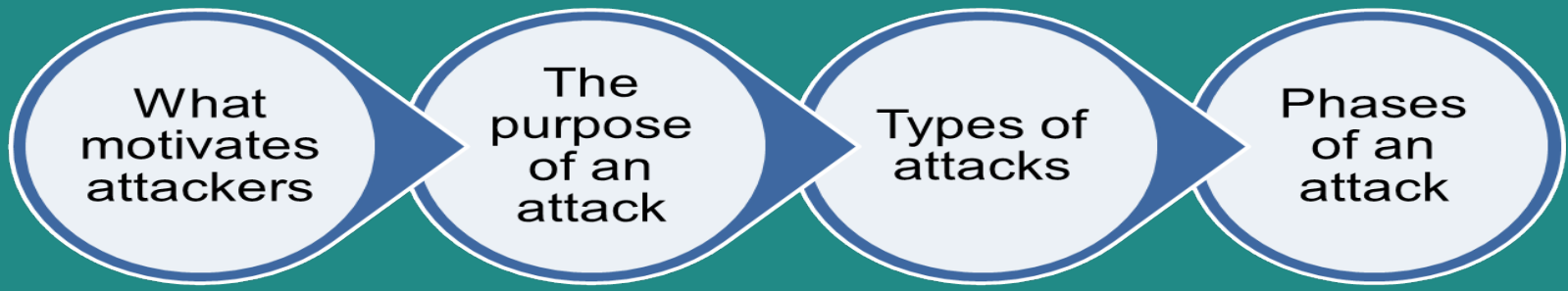
A MODEL PENETRATION TEST ENGAGEMENT

- A typical penetration test will follow this pattern: Initial engagement, scoping, testing, reporting and follow up. There should be a severity rating for any issues found.
- For this model we assume that:
  - You wish to know what the impact of an attacker exploiting a vulnerability would be, and how likely it is to occur
  - You have an internal vulnerability assessment and management process

INITIAL ENGAGEMENT OF THE EXTERNAL TEAM

- A typical penetration test will follow this pattern: Initial engagement, scoping, testing, reporting and follow up. There should be a severity rating for any issues found.
- For this model we assume that:
  - You wish to know what the impact of an attacker exploiting a vulnerability would be, and how likely it is to occur
  - You have an internal vulnerability assessment and management process

Anatomy of an Attack



Preparing for a cyber attack / Ethical Hacking Penetration testing

- To protect your organization from a cyber attack, it's important to understand how an attacker goes about stealing sensitive information.
- Typically, attacks happen in five distinct stages:
  - Reconnaissance and Footprinting
  - Scanning and enumeration
  - Gaining Access
  - Maintaining Access
  - Covering Tracks
- Each stage uses different tools and techniques.
- In this module, we will be looking at those stages and look at tools to proect your orgnization and ultimately prevent the cybercriminal from achieving their goal.

PHASES OF AN ATTACK- RECONNAISSANCE AND FOOTPRINTING

- A large part of the information gathering stage is conducting using passive attacks such as by using public records and Open Source Intelligence (OSINT)
- Attackers then leverage information from a variety of factors to understand their target including identifying network layouts, domains, servers, infrastructure details).
- This will help the pen tester to understand how a network works, including its assets (applications, systems, devices, anything with an IP).
- The reconnaissance stage is crucial to thorough security testing because penetration testers can identify additional information that may have been overlooked, unknown, or not provided

Phases of an attack- Scanning and enumeration

- Once the target is identified, the next step is to identify a weak point that allows the attackers to gain access.
- This is usually accomplished by scanning an organization's network to find entry points.
- This step of the process usually goes slowly, sometimes lasting months, as the attackers search for vulnerabilities.
- **Enumeration** Enumeration is basically counting. A hacker establishes an active connection to the target host. The vulnerabilities are then counted and assessed. It is done mainly to search for attacks and threats to the target system.
- Enumeration is used to collect usernames, hostnames, IP addresses, passwords, configurations, etc.
- Enumeration is very important to programmers, as it poses significant challenges to the security of any system

PHASES OF AN ATTACK- GAINING ACCESS

- Attackers break into the network, delivering targeted malware to vulnerable systems and people, often without the user being aware they are a target.
- They then map the organization's defences from the inside and create a battle plan for information they intend to target.
- Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.
- After interpreting the results from the vulnerability assessment, penetration testers use manual techniques, human intuition, and their backgrounds to validate, attack, and exploit those vulnerabilities.

Phases of an attack- Maintaining Access

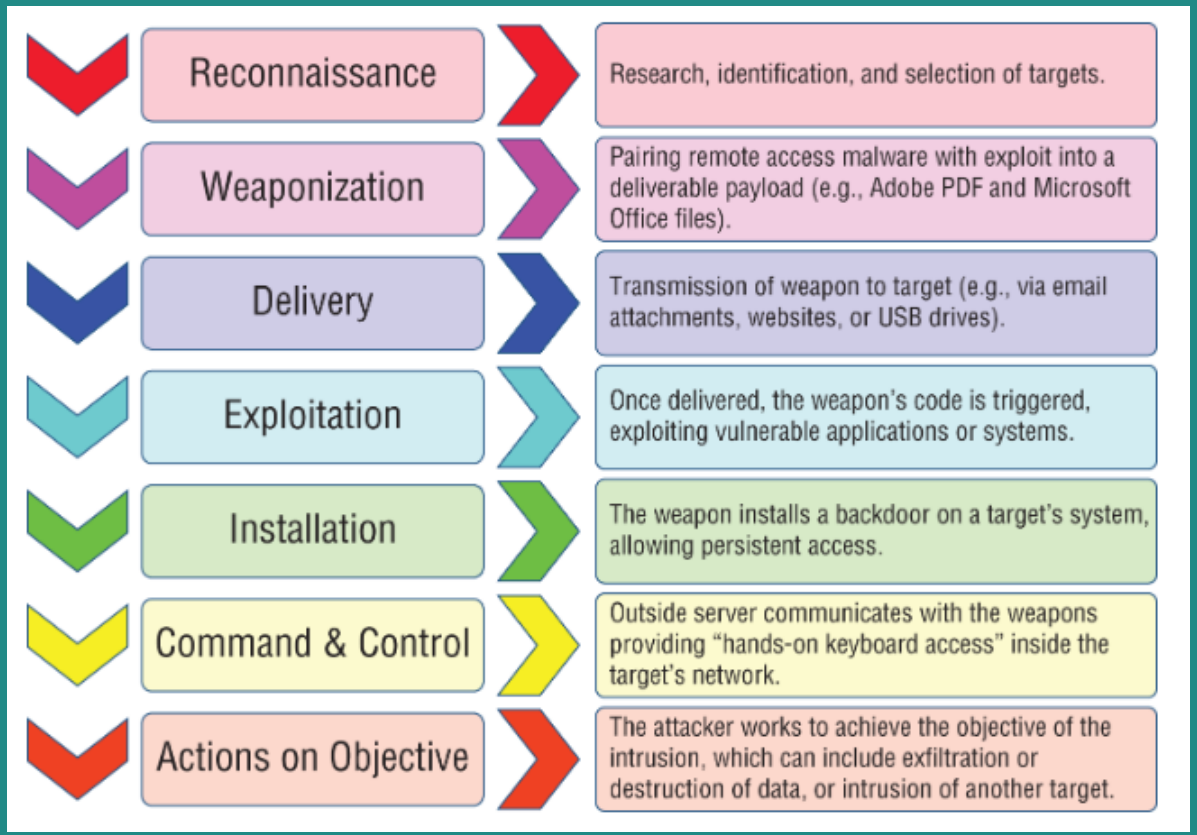
- Now that weaknesses in the target network are identified, the next step in the cyber attack is to gain access and then escalate.
- In almost all such cases, privileged access is needed because it allows the attackers to move freely within the environment.
- Once the attackers gain elevated privileges, the network is effectively taken over and is now ”owned” by the intruders.
- This is another stage where malware can be beneficial. You may need to install a rootkit
- **Data Exfiltration** is then conducted and the tester uses tools and techniques to extract data from the network, simulating the actions of hackers.

Phases of an attack- Covering Tracks

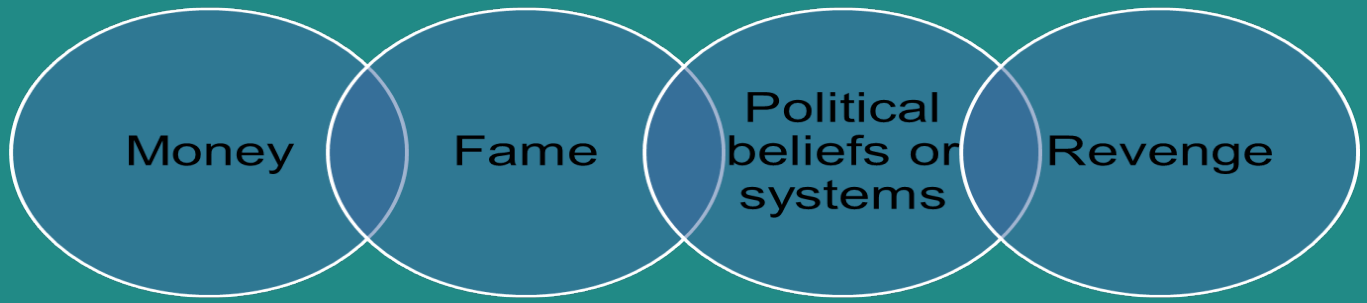
- Covering your tracks is where you hide or delete any evidence to which you managed to get access.
- Additionally, you should cover up your continued access.
- This can be accomplished with malware that ensures that your actions aren't logged or perhaps misreports system information, like network connections.

CYBER KILL CHAIN

- Lockheed martin adapted the military concept of a kill chain to the information security space.
- The idea of a kill chain is that you can identify where the attacker is in their process so you can adapt your own response tactics.



Intruders/Hackers Motivations



- **Amateurs**
  - Not very sophisticated
- **Crackers**
  - Access resources without permission
- **Career criminal**
  - Well-planned attacks, usually for financial gain
- **Military**
  - Done to disable opposing forces & gain strategic advantage

MOTIVATION EXAMPLES

- **Casual snooping** - Inquisitive crackers who look around seeing what they can find, without any of the following motives
- **Disruption** - preventing or inhibiting legitimate users from use of the system
- **Espionage** - attempting to extract information from a system (perhaps commercial information).
- **Use of resources** - once compromised, a system or network can be used to launch attacks on other networks.
- **Making a statement** - social, political, anarchistic etc.

Social Engineering

With that knowledge in mind, here are questions that come up with regard to information gathering:

- How can you gather information?
- What sources exist for social engineers to gather information?
- What can you glean from this information to profile your targets?
- How can you locate, store, and catalog all this information for the easiest level of use?

Social Engineering Examples

Elicitation

- Elicitation is ”the subtle extraction of information during an apparently normal and innocent conversation.”

Pretexting-A good liar...

- Some people say Pretexting is just a story or lie during a **social engineering** engagement.

Influence: The Power of Persuasion

- Persuasion and influence involve emotions and beliefs . **You have to know how and what people are thinking.**

Social Engineering example: Blocking you out of your account
click here for Youtube video

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **Recommended Readings note:** Focus on what was covered in the class. Other parts will come later in other lectures.
  - Chapter1, Computer Security: Principles and Practice, , William Stallings and Lawrie Brown
  - Chapter 1, CyBOK, The Cyber Security Body of Knowledge