Computer Security
Basic Concepts

Lecture-1

Department of CSE, IUT

Outline

- Context: Cyber attack in Bangladesh
- Context: Global Cyberattack
- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Learning objectives

- Describe the key security requirements of confidentiality, integrity and availability
- Discuss the types security threats and attacks that must be dealt with
- Summarize the functional requirements for computer security
- Explain the fundamental security design principles
- Discuss the use of attack surfaces and attack trees
- Understand the principle aspects of a comprehensive security strategy

Do you have experienced with Cyber Attack

Bangladesh has become one of the most vulnerable countries in cyber space

- BGD e-GOV CIRT

Context: Cyber Attack in Bangladesh

- Recently, Bangladesh suffered a major and coordinated cyber attack (Feb, 2021)
  - A total of 147 banks and non-bank financial institutions
    - Bangladesh Bank (BB), Lanka Bangla Finance, Trust Bank, Bank Asia, Dhaka Bank
    - Hacker group called Hafnium known as threat actor
  - Tactic: a malware is inserted through Microsoft Exchange Server(MES)
    - Microsoft detected multiple zero day exploitations
    - What are the consequences?
    - How to mitigate?
      - Microsoft's Test-ProxyLogon.ps1 script
      - Scanner "MSERT

https://thefinancialexpress.com.bd/national/latest-cyber-attack-hit-at-least-147-bangladeshi-entities-1617416432

Context: Cyber Attack in Bangladesh

- In Nov 2017, SWIFT warned banks around the world
  - What : A hacker stole $81 million from Bangladesh Bank in February 2016.
  - How: Customized malware attack that compromised SWIFT software so that threat actor can infiltrate the system and transfer funds
- DBBL cyber attack
  - What : losing $3 million between May 1 and 3 from cash machines in Cyprus, Russia and Ukraine.
  - How: A malware in the bank's card management system around three months ago and duplicate switch, which the bank could not detect.
  - It is undetected: Visa asked it to settle payments for transactions made by the bank's "clients" in Cyprus
  - Why DBBL?
    - It has the highest number of ATM booths across the country

Context: Cyber Attack in Bangladesh

- Bangladesh Bank Warned to all banks of a fresh cyber attack from North Korea based hacker group during the Pandemic
- Banks limits online activities which is already boosted during the pandemic
- The monthly transactions increased to Tk7,421 crore by June this year.

Let’s talk about the global cyber attack

Global Cyberattack: Game PublisherElectronic Arts (EA)

- A very recent attack on 10/06/2021
- One of the largest game companies in the works
  - Battlefield, Star Wars: Jedi Fallen Order, The Sims
- Hackers have stolen valuable information
  - Consequence: 780GB of data was stolen which is source code of the game
  - Consequence: intrusion into the network
  - But, no player data had been stolen in the breach
- Does not impact on the games or our business

Global Cyberattack: JBS

- World's largest meat supplier targeted by a sophisticated cyber-attack on May 31, 2021
  - Consequence: Temporarily shutting down some operations in Australia, Canada and the US, with thousands of workers affected.
  - Consequence: Forced the shutdown of all its U.S. beef plants
  - Consequence: Delay certain transactions with customers and suppliers.
  - Threat actor: Criminal group from Russia
  - Threat: Ransomware attack
    - Hackers get into a computer network and threaten to cause disruption or delete files unless a ransom is paid.
    - Suspended all affected IT systems as soon as the attack was detected

What Security goal is affected?

https://whttps://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-cyber-victim-as-hackers-hit-top-supplier-jbs

Global Cyberattack : British Airways

- BA website diverted to a fraudulent site disclose 380,0 data in 2018.

  Login detailed, bank detailed

- Stolen data did not include travel or passport details.
- Magecart a financially-motivated threat group used malicious piece of code
  - Monitored for certain mouse-up and touch-up interactions, extracted data entered in the checkout page payment form, and sent it to a remote server

This is the biggest shake-up to data privacy in 20 years.

Background-Cyber Security

- Today, cyber security requires a new line of defence
  - Traditional security defence such as signature based detection is not sufficient
  - Every year there are new threats, breaches and unknown vulnerabilities
- Severity of cyber security risk is very high
  - Attacks are well funded and well organized
  - The stakes at cyber security risk become larger every year
  - half of business organizations suffer at least one security incident per year

norm rather than an exception

- We need
  - Proactive defence
  - Shorten the window between compromise and detection
  - Predicate future risk
    - Effectiveness of existing controls

Cyber Threats Numbers

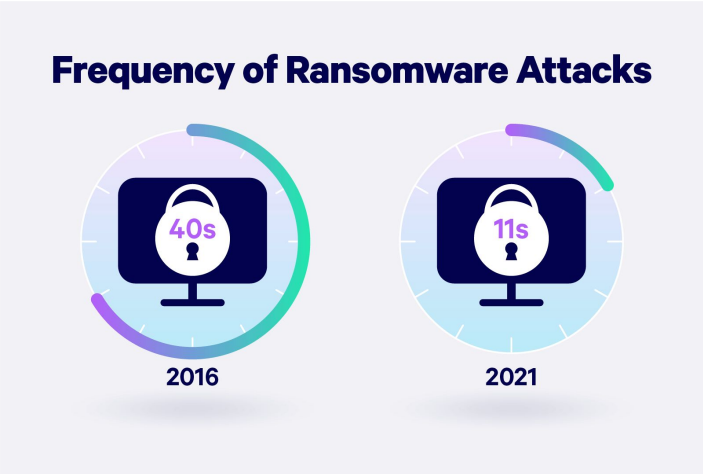
- How many cyber attack / day?
  - 30,000 website hacked per day
  - 4.3 million phishing attempts / hour
  - Every 39 seconds, there is a new attack somewhere on the web.
- There were 20M breached records in March 2021.
- It only takes 82 seconds to become the first victim of malware spam
- Companies 500 employees or more the average cost of the most severe breach is now between £1.46 million and £3.14 million
- 88% of organizations worldwide experienced spear phishing attempts in 2019.
- An estimated 300 billion passwords are used by humans and machines worldwide.

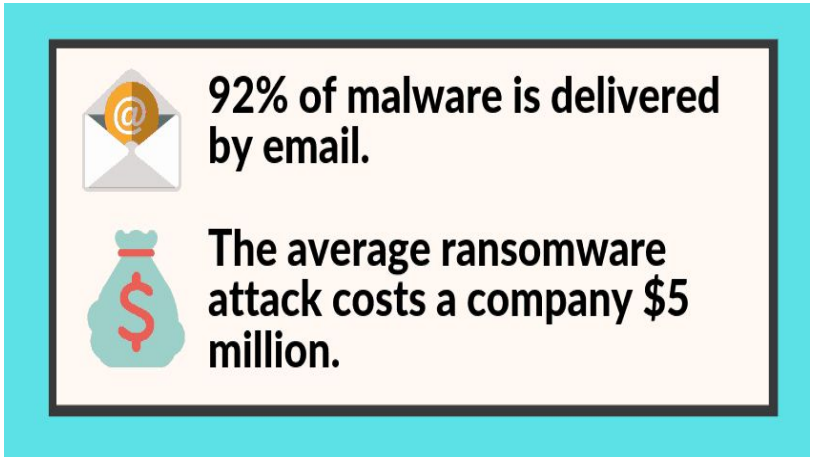
It difficult for computer users to stay safe online

Source: EU, McAfee, UK Gov,Deloitte

Attack Trends

- There are side effects of the global pandemic
- .zip and .jar are the most popular malicious e-mail attachments
- 48% of malicious email attachments are office files.
- About 20% of malicious domains are very new and used around one week after they are registered.



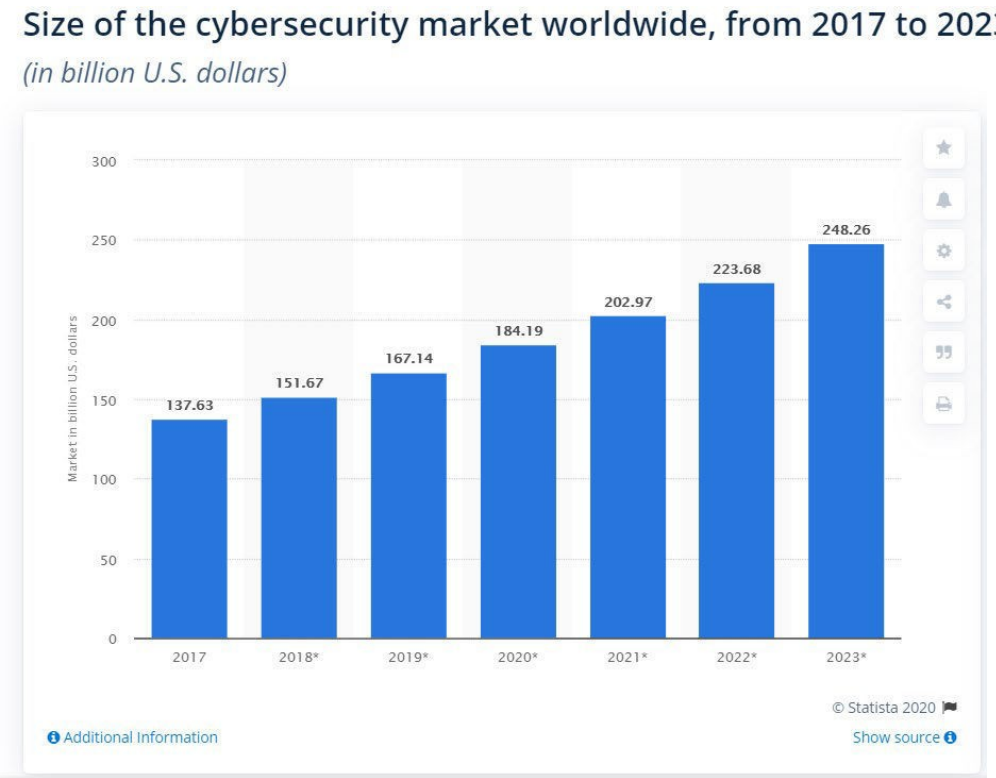


Cyber Security Market

- IT investment
  - Cybersecurity has the most significant budget

Worldwide information security market is forecast to reach $170.4 billion in 2022

-Gartner



Phishing: Tactics

- **Email:** appears in inbox. usually with a request to follow a link, send a payment, reply with private info, or open an attachment.
- **Domain spoofing:** mimic valid email addresses. These scams take a real company's domain (ex: @iit.du.ac.bd) and modify it.
- **Social media phishing:** Threat actor uses posts or direct messages to persuade victim into a trap.
- **Clone phishing:** duplicates a real message that was sent previously, with legitimate attachments and links replaced with malicious ones.
- Examples of common phishing scams
  - The tax refund/rebate
  - Contest winner/Inheritance email.
  - Office 365 deletion alerts

Potential Threat: Malware

- A Malware is a set of instructions that run on your computer and make your system do something that an attacker wants it to do.
- The purpose is often to steal, damage or manipulate sensitive information relating to an individual

Malware = Malicious Software

- Set of instructions that cause a site's security policy to be violated
- Often leveraging an inadvertent flaw or vulnerability (design or implementation)

–To propagate/install on target

–To cause harm on target

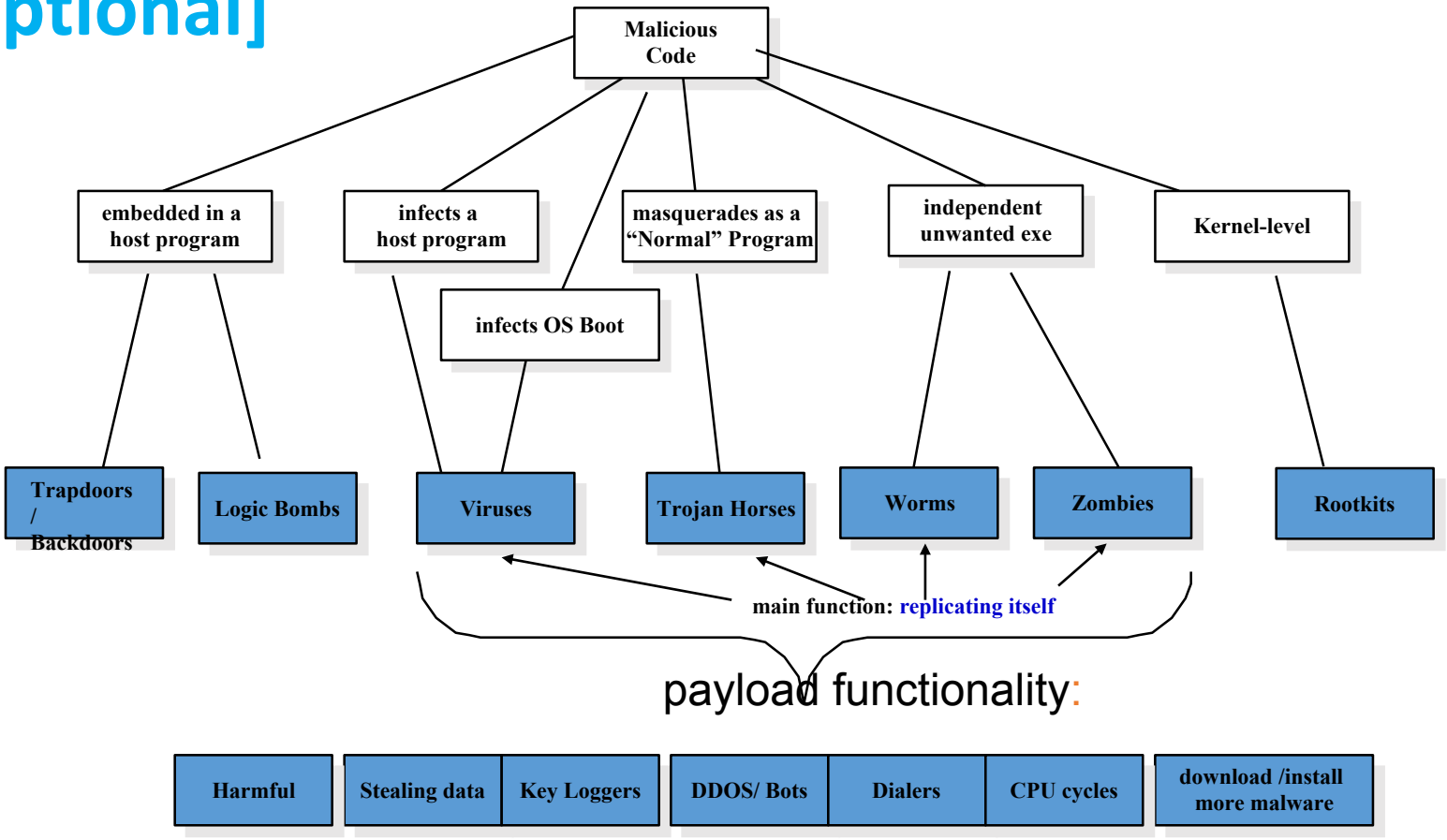
 Today, most malware possesses intent to destroy systems including:

  - Files
  - Web pages
    - Estimated that about 1 in 10 web pages contain malicious code.

Malware

- Zero day exploit
  - An exploit takes advantage of a vulnerability to attack a system and enact malicious behaviour
    - A Zero-Day exploit is based on a recently discovered vulnerability, that has no patch available yet
    - Time between exploit discovery and wide activation shrinking
    - Malware developer has trade-off
  - Big splash but faster discovery
  - Reduced attack rate but longer undiscovered

Malware Taxonomy: Pay load functionality: [Optional]



Payload

- The action that a threat performs, apart from its main behaviour.
- Malware that the threat actor intends to deliver
- Payloads can range from stealing personal information to deleting the contents of a hard drive.
- Example of Payload
  - Ransomware is a kind of cyber attack that involves hackers taking control of a computer system and blocking access to it until a ransom is paid.
  - Restricting the ability to carry out general activities on the system
    - Encrypting files
    - Disabling Apps

According to Symantec one in every 359 emails in existence contains a malicious payload

Final Note

- It is not realistic to believe that organisation can defend against every potential attack
  - Cyber attack will succeed to the infrastructure
    - May be not today but tomorrow or coming days
  - Organisations must have ability to identify and tackle the attack for the overall business continuity
- Cyber Security is a context specific
  - Need to consider defensive strategy based on the context
- What next then

Time to Think Beyond Cyber Security

A context is

given let's

move on to

Theory

What is Computer Security

- Most developers and operators are concerned with **correctness: achieving desired behavior. (What should DO?)**
  - A working banking web site, word processor, blog,…

- Security is concerned with **preventing undesired behavior. (What should Not Do?)**
  - Consider an employee/opponent/hacker/adversary who is actively and maliciously trying to circumvent any protective measures you put in place

Kinds of undesired behavior

confidentiality

Kinds of undesired behavior

- Stealing information: ~~**confidentiality**~~
  - Corporate secrets (products plan, source code,..)
  - Personal information (credit card numbers, SSNs)

Kinds of undesired behavior

- Stealing information: ~~**confidentiality**~~
  - Corporate secrets (products plan, source code,..)
  - Personal information (credit card numbers, SSNs)

integrity

Kinds of undesired behavior

- Stealing information: ~~**confidentiality**~~
  - Corporate secrets (products plan, source code,..)
  - Personal information (credit card numbers, SSNs)

- Modifying information or functionality: ~~**integrity**~~
  - Installing unwanted software (spyware, botnet client,…)
  - Destroying records (accounts, logs, plans,..)

Kinds of undesired behavior

- Stealing information: ~~**confidentiality**~~
  - Corporate secrets (products plan, source code,..)
  - Personal information (credit card numbers, SSNs)

- Modifying information or functionality: ~~**integrity**~~
  - Installing unwanted software (spyware, botnet client,…)
  - Destroying records (accounts, logs, plans,..)

availability

Kinds of undesired behavior

- Stealing information: ~~**confidentiality**~~
  - Corporate secrets (products plan, source code,..)
  - Personal information (credit card numbers, SSNs)

- Modifying information or functionality: ~~**integrity**~~
  - Installing unwanted software (spyware, botnet client,…)
  - Destroying records (accounts, logs, plans,..)

- Denying access: **availability**
  - Unable to purchase products
  - Unable to access banking information

A definition of computer security

- **Computer security:**

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

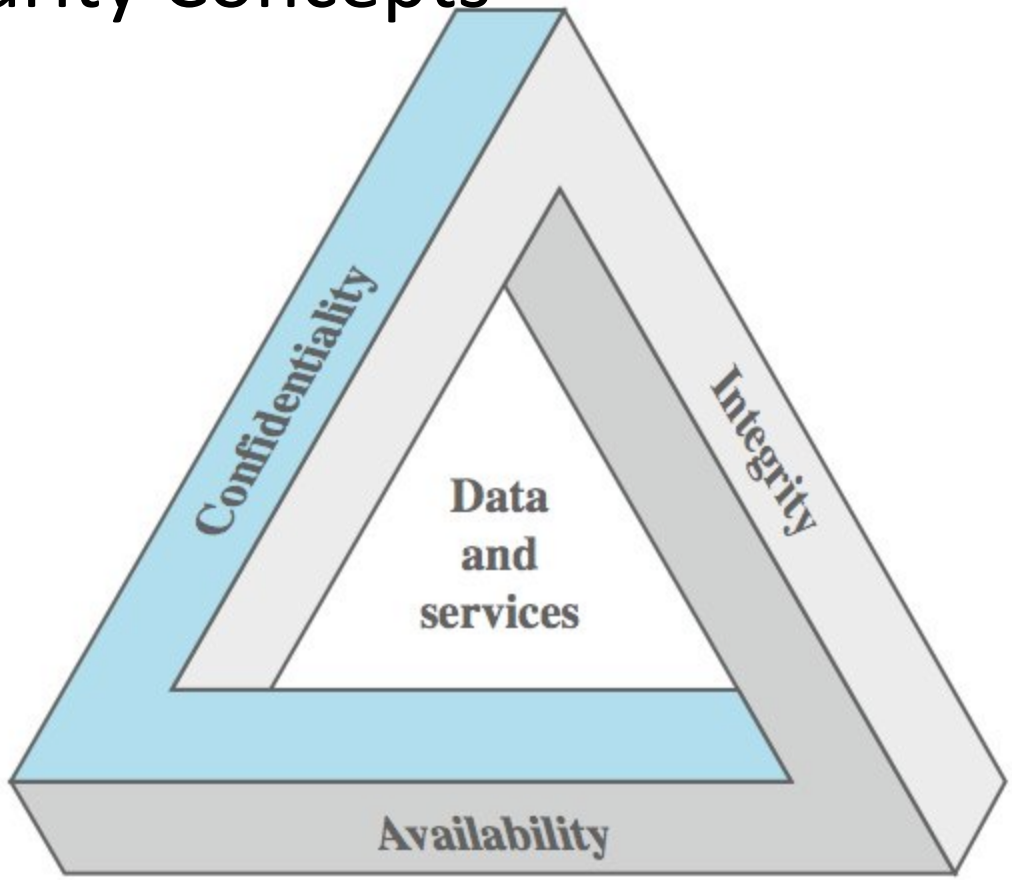
(includes **hardware, software, firmware, information/data, and telecommunications**)

NIST 1995

Three key objectives (the CIA triad)

- **Confidentiality**
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individual control or influence what information may be collected and stored
- **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 operations in unimpaired manner
- **Availability**: assure that systems works promptly and service is not denied to authorized users

Key Security Concepts



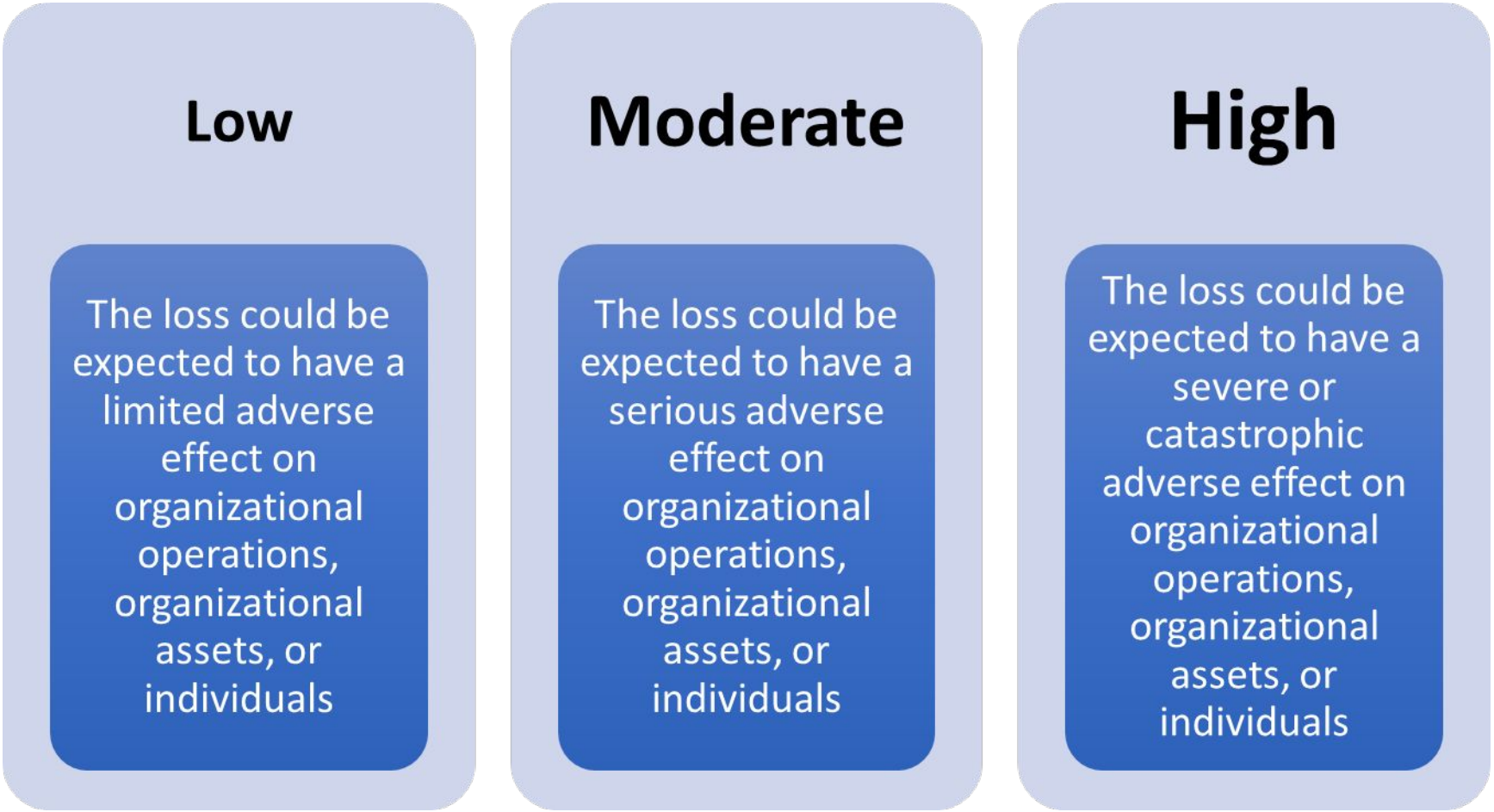
Other concepts to a complete security picture

- **Authenticity**: the property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator

Other concepts to a complete security picture

- **Accountability**: generates the requirement for actions of an entity to be traced uniquely to that individual to support nonrepudiation, deference, fault isolation, etc

Levels of Impact



Examples of security requirements: **Confidentiality**

- Student grade information is an asset whose **confidentiality** is considered to be **very high**
  - The US FERPA Act: grades should only be available to students, their parents, and their employers (when required for the job)
- Student enrollment information: may have moderate **confidentiality** rating; **less** damage if enclosed
- Directory information: **low confidentiality** rating; often available publicly

Examples of security requirements: **Integrity**

- A hospital patient's allergy information (high integrity data): a doctor should be able to trust that the info is correct and current
  - If a nurse deliberately falsifies the data, the database should be restored to a trusted basis and the falsified information traced back to the person who did it
- An online newsgroup registration data: moderate level of integrity
- An example of low integrity requirement: anonymous online poll (inaccuracy is well understood)

Examples of security requirements: Availability

- A system that provides authentication: high availability requirement
  - If customers cannot access resources, the loss of services could result in financial loss
- A public website for a university: a moderate availably requirement; not critical but causes embarrassment
- An online telephone directory lookup: a low availability requirement because unavailability is mostly annoyance (there are alternative sources)

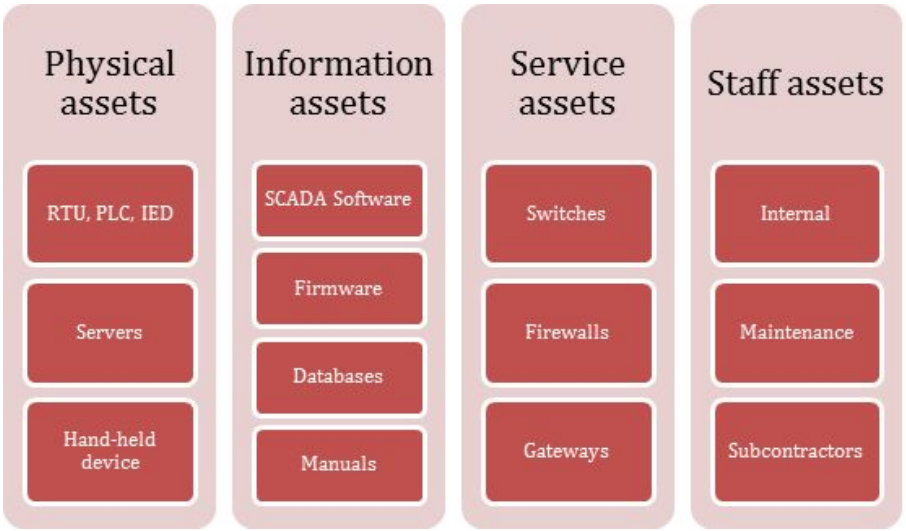
Challenges of computer security

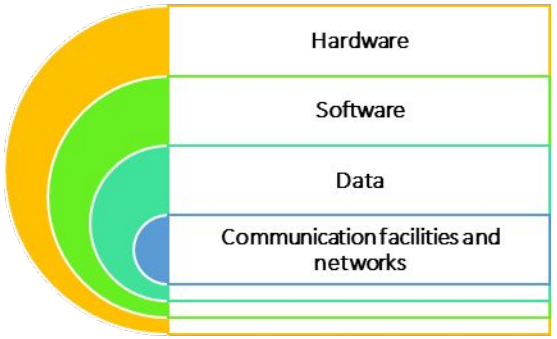
- Computer security is not simple
- One must consider potential (unexpected) attacks
- attackers only need to find a single weakness, the developer needs to find all weaknesses
- Procedures used are often counter-intuitive
- Must decide where to deploy mechanisms
- multiple algorithms or protocols may be involved
- A battle of wits between attacker / admin
- It is not perceived on benefit until fails
- Requires constant monitoring
- is often an afterthought to be incorporated into a system after the design is complete

Computer Security: **Terminology**

- **Asset** –(System Resource) – anything that has value to an individual, an organization or a government

Examples:



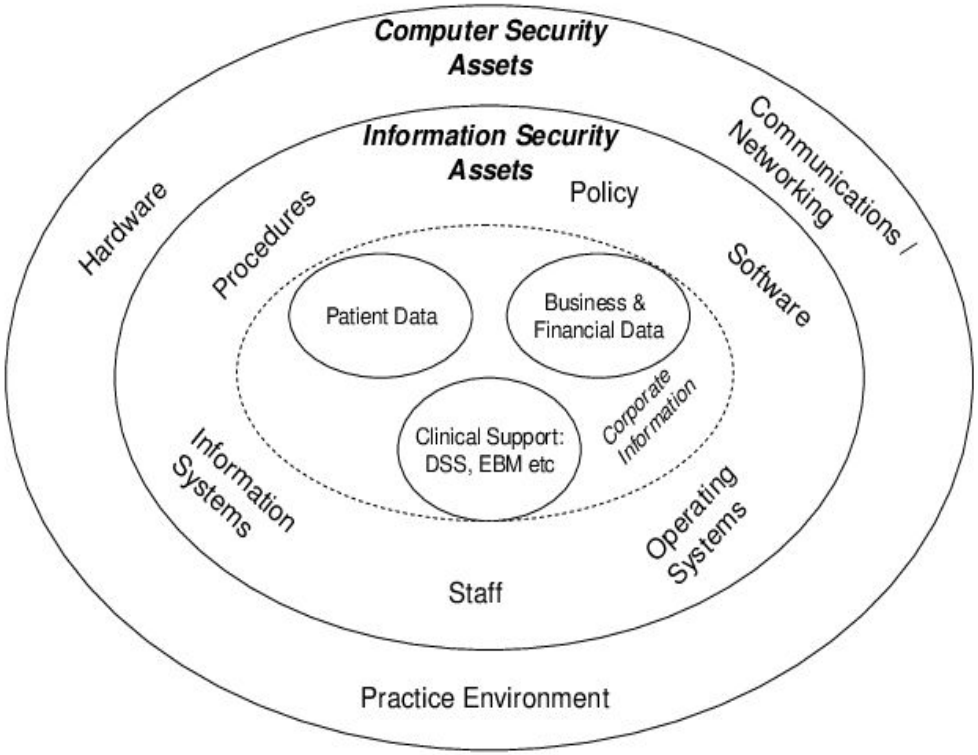


Computer Security: **Terminology**

- **Asset** –(System Resource) – anything that has value to an individual, an organization or a government

Examples:

- digital document
- database
- password
- encryption key
- …….
- ….



Computer Security: **Terminology**

- **Asset** –(System Resource) – anything that has value to an individual, an organization or a government

Examples:

People	Staff Interns Guests
Equipment	Servers Laptops Printers
Environment	Building locations Asset locations
Software	Websites Applications
Data	Online data Stored data
Organisation	Reputation Responsibilities
Third parties	External administrators IT vendors

Computer Security: **Terminology**

- **Access -** a subject or object's ability to use, manipulate, modify, or affect another subject or object.

- **Threat Agent** (**Adversary**) - An entity that attacks, or is a threat to, a system.

  Examples:

  •malicious hackers,
  •insiders (including system administrators and developers),
  •terrorists,
  •nation states.

- **Malicious contents-** applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

Computer Security: Terminology

- **Vulnerability** – weakness of an asset or control that can be exploited by a threat
- Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

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

Computer Security: Terminology

- **Threat** – : potential cause of an unwanted incident, which may result in harm to a system, individual or organization

- **If you tell someone "I am going to kill you," this is an example of a threat.**

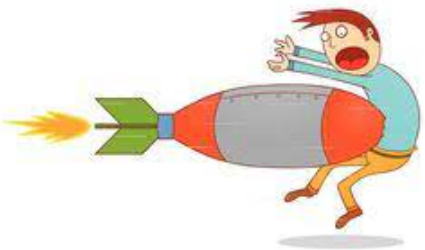
- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset

Computer Security: **Terminology**

- **Exposure** - a single instance of being open to damage.
- **Exploit -** to take advantage of weaknesses or vulnerability in a system.

Computer Security: **Terminology**

- **Exposure** - a single instance of being open to damage.
- **Exploit -** to take advantage of weaknesses or vulnerability in a system.
- **Attack** - an act that is an intentional or unintentional attempt to cause damage or compromise to the information and/or the systems that support it.



gg75772701 GoGraph.com

- Categories of Attacks
  - 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 perimeter
  - Outsider – initiated from outside the perimeter

Computer Security: Terminology

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
  - Traffic 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

Computer Security: **Terminology**

- **Risk** - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Computer Security: **Terminology**

- **Countermeasure** - An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

- **Security Policy** - A set of rules and practices that specify how a system or org provides security services to protect sensitive and critical system resources.

Computer Security: **Terminology**

- **Cyber Space-** interconnected digital environment of networks, services, systems, and processes
- **Cyber incident-** cyber event that involves a loss of information security or impacts business operations
- **Cyber insurance:** insurance that covers or reduces financial loss to the insured caused by a cyber incident
- **Cyber-Physical Systems (CPS):** are systems composed of physical systems (hardware), software systems and potentially other types of systems (e.g., human systems). These are closely integrated and networked to deliver some global behaviour.

Computer Security: **Terminology**

- **Cyber-Physical Systems (CPS):** are systems composed of physical systems (hardware), software systems and potentially other types of systems (e.g., human systems). These are closely integrated and networked to deliver some global behaviour.

Computer Security: Terminology

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

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.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

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.

Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Assets of a Computer System

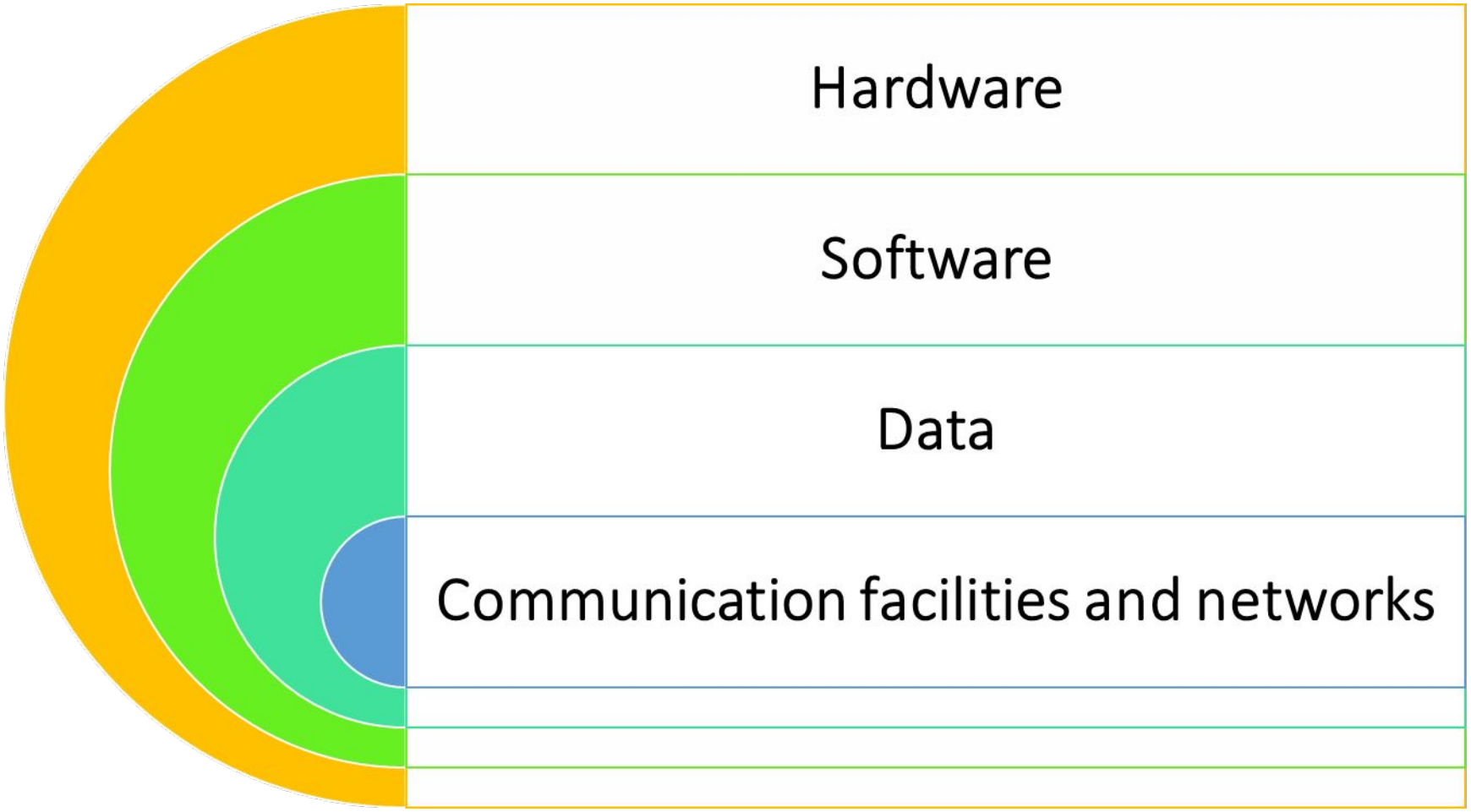


Table 1.3

Computer and Network Assets, with 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.

Security Concepts and Relationships

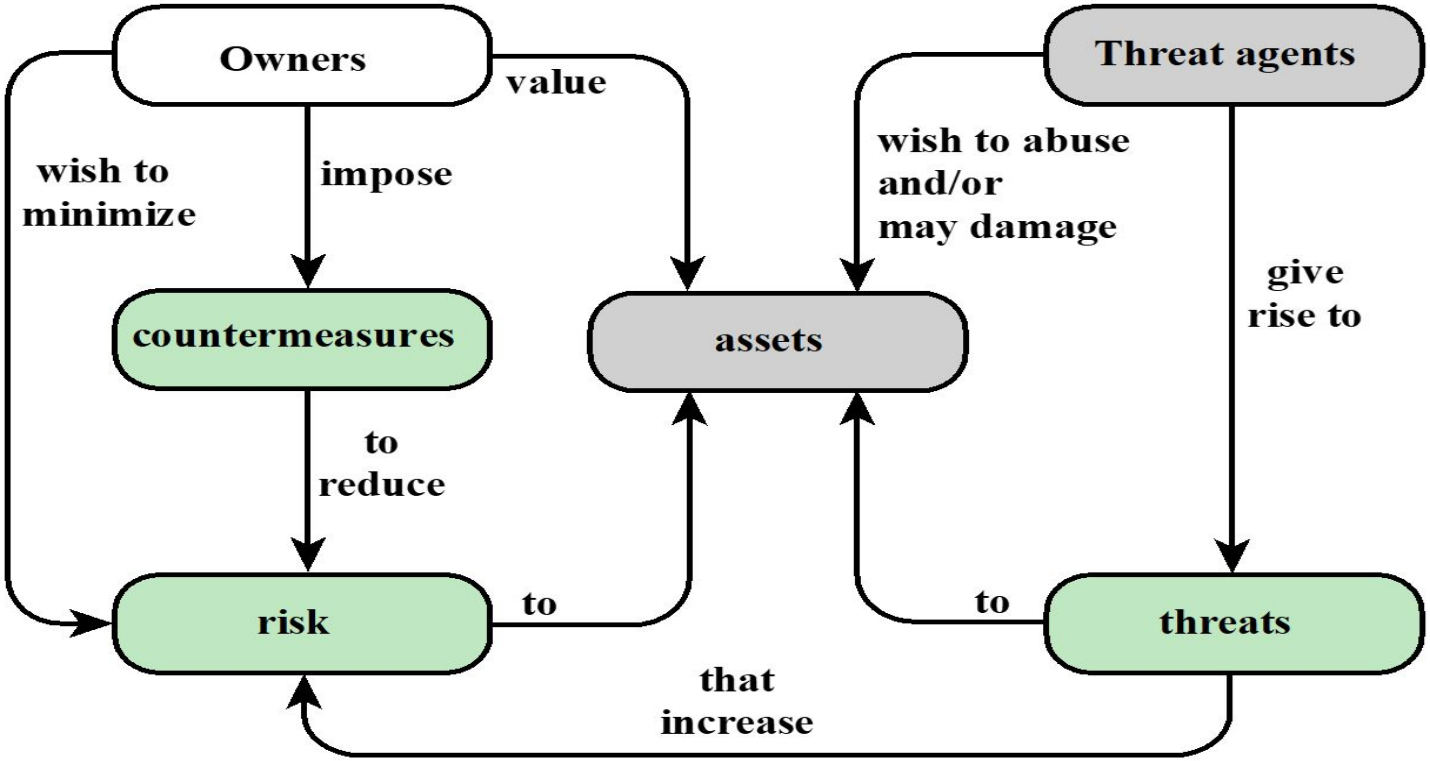
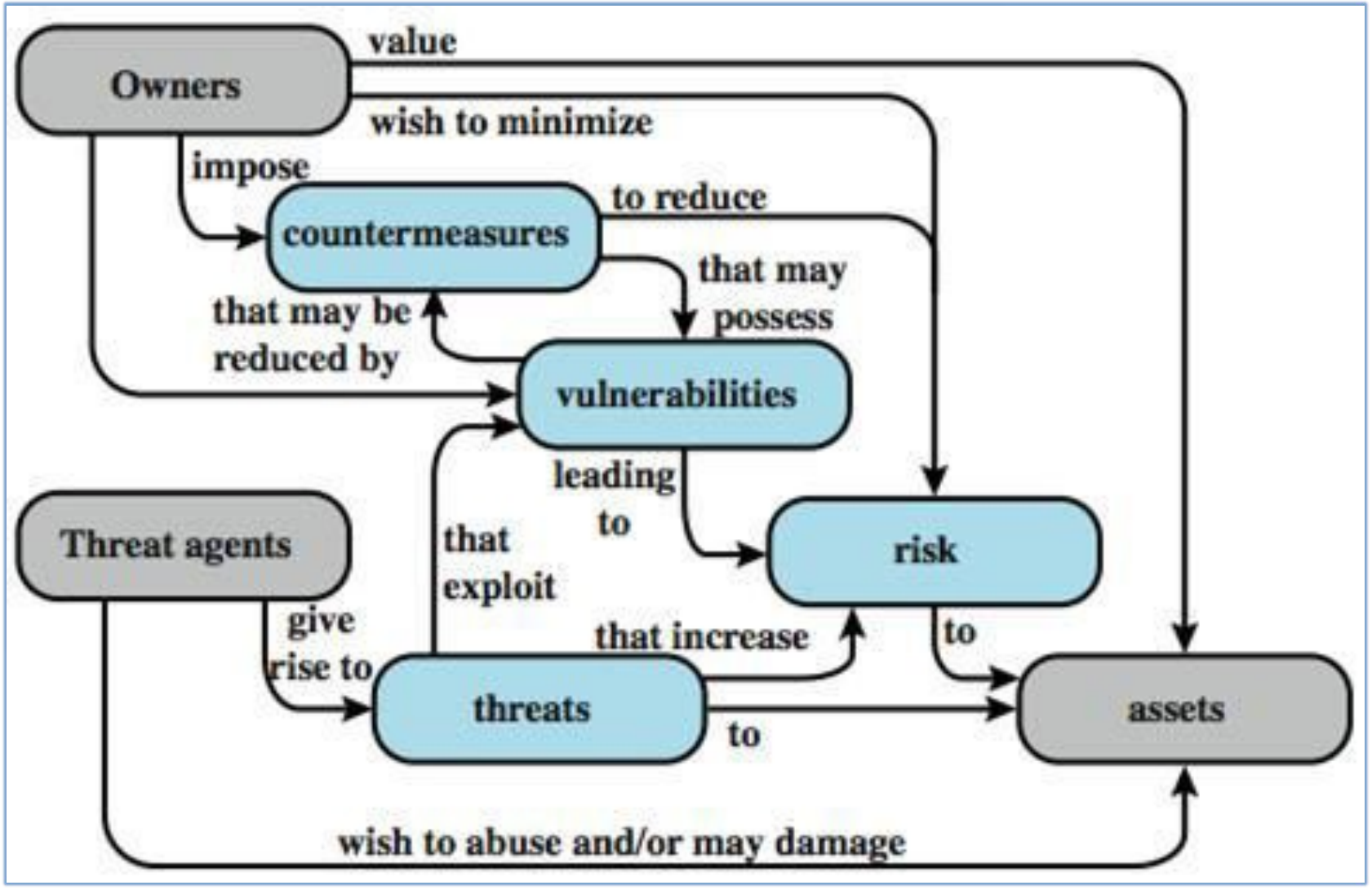


Figure 1.1 Security Concepts and Relationships

Security Concepts and Relationships



Threat Consequences & Types of Threat Actions

That cause each Consequence

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Threat Consequences & Threat Action (attack)

Unauthorized Disclosure is a threat to **confidentiality**

- **Exposure**: This can be deliberate or be the result of a human, hardware, or software error
- **Interception**: unauthorized access to data
- **Inference**: e.g., traffic analysis, use of limited access to get detailed information
- **Intrusion**: unauthorized access to sensitive data

Threat Consequences & Threat Action (attack)

Deception is a threat to either system or Data Integrity

- **Masquerade**: e.g., an attempt by an unauthorized user to gain access to a system by posing as an authorized user; Trojan horse.
- **Falsification**: altering or replacing of valid data or the introduction of false data
- **Repudiation**: denial of sending, receiving or possessing the data.

Threat Consequences & Threat Action (attack)

Disruption is a threat to availability or System Integrity

- **Incapacitation**: a result of physical destruction of or damage to system hardware
- **Corruption**: system resources or services function in an unintended manner; unauthorized modification
- **Obstruction**: e.g. overload the system or interfere with communications

Threat Consequences & Threat Action (attack)

Usurpation is a threat to System Integrity.

- **Misappropriation**: e.g., theft of service, distributed denial of service attack

- **Misuse**: security functions can be disabled or thwarted

References

- Chapter -1 : Computer Security: Principles and Practice- by Lawrie Brown and William Stallings