Computer Security deals with computer related assets that are subject to a variety of threats and various measures are taken to protect those assets.

We dealing with Computer security we look at:.
-categories of computer-related assets that users and managers wish to protect.
-various threats and attacks that can be made on those assets.
-the various measures that can be taken to deal with those threats.

Key to consider:
-What assets do we need to protect?
-How are those assets threatened.
-What measures can we take to counter those threats .

NIST⇒ National Institute of Standards and Technology.
FIPS ⇒ Federal Information Processing Standard Publication.
FIPS 199 ⇒ a standard by NIST.

Data vs Information.
Data are simply fact and figures; bits of information but not actually information.
When data is processed, organized and structured, and is presented in a meaningful. way it becomes information.
Information provides context for data.

What is Computer Security?
Is it the measures and controls that ensure the Confidentiality, Integrity, Availability, (Authenticity, and Accountability), of Information system assets such as hardware, software, firmware, and information that processed, stored and communicated.

NIST standard FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems, February 2004) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems.

But some in the security field also list Authenticity and Accountability.

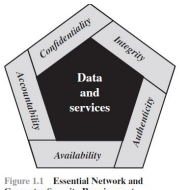

Figure 1.1 Essential Network and Computer Security Requirements

FIPS 199 also defines these level of impact:
Low .
Moderate.
High.

These 5 terms are objectives that are at the heart of computer security. They ensure that there is a standard that needs to be met for the protection of computer related assets.

Key objectives sated only by FIPS 199:

1. Confideality covers concepts such as :
Data confidentiality ⇒ This concept assures private or confidential data is accessible to unauthorized individuals.
Privacy ⇒ Assures individuals determine or influence what information about them is collected, by whom is it collected and stored and to whom it is disclosed too.

2. Integrity
Data integrity⇒ Assures that data and program is not changed due to unauthorized access.
System Integrity ⇒ Assured system works un-impaired, it is not manipulated by unauthorized access.

3. Availability ⇒ Assures there is redundancy. Meaning that the system or service is working promptly and that authorized users are not denied access.

Nonrepudiation is the assurance that someone cannot deny something.

Definitions of the 5 key objectives:

a)What does this objective mean? & b) how can it be lost?

1. **Confidentiality?:**
    a. **Preserving authorized restriction on information access, including means to protect private and proprietary information.**
    b. **A loss of confidentiality is unauthorized access or disclosure of information.**
2. **Integrity?**
    a. **Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity**
    b. **A loss of integrity is unauthorized modification or destruction of information.**
3. **Availability?**
    a. **Assures system works promptly and authorized users are not denied access**
    b. **A loss of availability is the disruption of access to or use of information or information system.**
4. **Authenticity?**

a. **Property of being genuine; being able to be verfied and trusted. Confidence in the validity of a transmission, message or message originator.**
b. **It means users say who they are and input arriving to the system is coming from a trusted source.**
c. **A loss of authenticity is when trust is lost from a message originator, or if a message causes damage to system since the source was not verified and trusted .**

5. **Accountability?**
    a. **Generates the requirement that the actions of an entity should be traced back to the entity.**
    b. **A loss of accountability is when there is no logging to trace events that occur in a system.**

Impact levels:
Low:

1) **Cause limited degradation to system mission capabilities but primary functions still work.**
2) **Results in minor damage to organizational assets.**
3) **Results in minor hard to individuals.**

Moderate:

1) **Cause significant degradation to system mission capabilities but primary functions still work.**
2) **Results in significant damage to organizational assets.**
3) **Results in significant damage to individuals.**

High:

1) **Cause severe degradation or loss of system mission capability, which means no primary functions work.**
2) **Results in major damage to organizational Assets.**
3) **Results in serious or life-threatening damage to individual.**

Examples of the 5 key objectives.
What is an asset and what it's security value.

Example of confidentiality:
Low level.⇒ contact information from general directory.
Moderate level. ⇒ student enrollment information.
High Level. ⇒ student grade information.

Examples of integrity:
Low level? ⇒ an anonymous online poll. Intentioally have few safeguards and the unaccuray and un-scienditicness is well understood.
Moderate level?⇒ Website forum about specific content. Attacker chooses to falsify entries and deface websites
High level? ⇒ patient's allergy information stored on database. Information about the patient needs to authentic and correct, free from any unauthorized modifications

Examples of Availability?: The more critical a component is, the more high level of availability is required
Low level? ⇒ online telephone directory.
Moderate level? ⇒ Typical public university website that provides basic information. Will cause embarrassment but it is not critical.

High level?⇒ for authentication service that provides access to critical system, application and programs. Authorized users not having access would result in loss of operation time which would result in large financial loss in terms of employee productivity and potential customers

Encryption?
In transit?:
HTTP/HTTPS & SSL/TCP

At rest:
AWS S3
AWS KMS - Key management service
AWS SSE C
Customer side encryption

The Challenges of Computer security?

1. **Computer security may seem simple but the mechanisms to meet the 5 key objects are complex. THey involve subtle reasoning.**
2. **Always consider all the potential risks your security mechanism, system or algorithm. Often times a flaw is found is by looking at problem in a different way.**
3. **Thus, bc of point 2 Services used in security mechanisms are counter-intuitive, i.e. not simple. They are complex. Often make sense when considering various aspects of a threat.**
4. **Once you design various security mechanism, you have to decide where to use them. You have to consider this in terms of physical placements (at what points in a network are certain security needed) and logical sense, (at what layers of TCP/IP model are security needed.)**
5. **Security mechanisms involve use of algorithm, protocol and some form of secret (like a encryption key. Eg: AWS KMS). Communication protocols could complicate tasks if connection is unpredictable and there is dependence of transit time limit. Whereby if there are unpredictable delays it could you cause meaningless issues.**
6. **Computer security is a battle of wits. Attacker has advantage since he/she has to find one vulnerability to exploit system (attack could active ==>cause disruption to operation or passive⇒ learn and make use of system). But designer has to account all possible weaknesses.**

7. **It is natural tendency of users and system managers to find little benefit from security investment until security failure occurs.**
8. **Security requires constant monitoring, which is hard nowadays since we work in such overloaded environment.**
9. **Security is still an afterthought and not considered as part of the design process.**
10. **Strong Security is viewed as an impediment to efficient and user-friendly operation of an information system or use of information.**

A Model for Computer Security.

Information system asset? ⇒ Hardware, software, firmware, data, Communication facilities and networks.

Hardware?: Including computer assets and other data processing, data storage and data communication devices.
Software?: including operating system , system utilities and applications
Firmware?: permanent software programmed into a read-only memory. For eg BIOS in IBM programming computers
Data?: file and databases and security data such as passwords
Communication facilities and networks?: local and wide area networks links, bridges, routers, and so on.

In context to security our concern is with regards to VULNERABILITIES of system resources.
National Research Council? ⇒ NRC

According to NRC 02, a report about security of computing, these are the general categories of vulnerabilities of a computer system or network asset.:

1. **System may be corrupted:**
    a. **It does the wrong thing or gives the wrong answers.**
    b. **This is with regards to integrity. (READ ABOUT THIS)**
2. **System can become leaky:**
    a. **Unauthorized access is gained from network.**
    b. **This is with regards to confidentiality. (READ ABOUT THIS)**
3. **System may become unavailable or very slow:**
    a. **Using the system becomes impossible or impractical.**
    b. **This is with regards to availability. (READ ABOUT THIS)**

Vulnerabilities to a system are threats.

An attack is a threat carried out. If successful it leads to serious security violations and consequences.

The agent carrying out the threat/attack is called the threat agent.

The attacker or threat agent represents RISK to an asset.

We can distinguish attack into 2 types?:

1. **Active : An attempt to alter system resources and affect their operation.**
2. **Passive : Attempt to learn and make use of information, which affect system resources.**

We can also classify attack based on origin of attack:

1. **Inside ⇒ Initiated from inside the security perimeter by insider.**
2. **Outside ⇒ Initiated by unauthorized or illegal users from outside the security perimeter**

Countermeasures are taken to deal with security attacks.

Ideally countermeasures are devised to prevent the success of a security attack

If prevention is not possible, then the goal is to detect the attack and recover from the effects of the attack.

Computer security Terminology?:

1)Adversary: an individual or group of individuals who cause harm or intend to cause harm to information system assets.

2)Attack: A malicious attempt to collect, deny, degrade or destroy information system resources or information itself.

Countermeasure.:
A device or technique that has it's objective as the impairment of the operational effectiveness of adversary activities (such as theft, espionage, unauthorized access to or use of sensitive information).

Risk.: is a measure of the extent to which an entity could cause potential harm to a given information system, its resources and information itself. Typically causes by ⇒ 1) Adverse impacts by activities of adersaries & 2) The likelihood of occurrence

Security Policy.:
A set of criteria for provisioning security resources. It defines and constraints the activities of data processing facilities in order to maintain security.

**********IMPORTANT ===> System Resource (Asset): What is considered to be an Asset???**

1) **A major application.**
2) **A general support system.**
3) **A high impact program.**

4) **A physical plant.**
5) **A mission critical system .**
6) **Personeel.**
7) **Equipment.**
8) **A group of logically related systems.**

Threat:
Any event or circumstance that has potential to cause harm to organizational operations, assets, individuals or a nation's through unauthorized access, denial of service, and modification/destruction of information.

Vulnerability:
A weakness in a information system, security procedure, internal control or implementation that could be exploited or triggered by threat source.

Adversary (threat agent)
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack
Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure
A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Security Policy
A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset)
A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

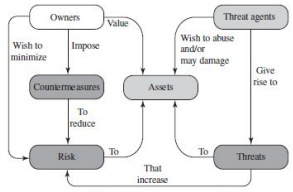

Figure 1.2 **Security Concepts and Relationships**

Chapter 1.2 ----------Threats, Attacks and Assets----------

Threat Consequence bc of action	Threat Actions
Undisclosed Disposure: - **Unauthorized entity gains access to sensitive information.** - **Is a breach of confidentiality.**	**-Exposure: sensitive data is directly accessed by unauthorized entity** **-Interception: sensitive data is directly accessed when travelling between two sources** **-Interference: sensitive data is indirectly assessed as a byproduct of communication** **-intrusion: An unauthorized entity gains accesses by circumventing security protections**

Threat Consequence	Threat Actions
Deception: - **Circumstance or event where authorized entity receives data and believes it to be true** - **Is a breach of integrity**	**-Masquerade: unauthorized entity gains access and acts like authorized entity, in order to deceive.** **-Falsification: false data used to deceive authorized entity.** **-Repudiation: one entity deceives another by denying responsibility for actions .**

Threat Consequence	Threat Actions
Disruption: - **A circumstance or event that prevents the correct system operation or function.** - **Is a breach of availability.**	**-Incapacitation: stop system operation by disabling a component.** **-Corruption: alter system operation by modifying system function or data** **-Obstruction: a threat action that interrupts the delivery of system services by hindering system operation.**

Threat Consequence	Threat Actions
Usurpation: - **A circumstance or event which causes an unauthorized entity to gain access to system services or functions.**	**Misappropriation: entity gains unauthorized physical or logical control of a system resource.** **Misuse: cause a system component to perform actions that are detriment to system security.**

READ BOOK FOR EXAMPLES OF THESE.

System resources (Assets) & CIA triad.

Hardware: This includes computer resources and other data processing, data storage, and data communication devices.
-A major threat to hardware is threat to availability.
-Hardware is most susceptible to attack and least susceptible to automate controls.
-Threats include accidental or deliberate damage to equipment as well as theft.
-theft of use == loss of confidentiality.

Software: this includes the operating system, system utilities and application program.
-a key threat to software is attack on availability .
-software can be easily deleted. Thus make backups for high availability.
-software modification is hardest to deal with ⇒ threat to integrity/authenticity.
-computer viruses such as trojan horse software that gain unauthorized access and modify information ⇒ threat to integrity/authenticity.
-Pirating software by copying it has not been solved but some countermeasures are available.

Data: includes files and databases and security related files such as passwords.
-Security concerns regarding data include: availability, secrecy and integrity
-How? :
-with availability, ⇒ accidental or malicious destruction of files.
-with secrecy, ⇒ unauthorized access and reading of files or databases. Eg ⇒ use aggregation of data sets and using statistical databases.
-with integrity, ⇒ modification of datafiles which can be minor or even disastoratious.

Communication facilities and networks: includes local and wide area network linkages, bridges, routers etc.
-Network attacks can be classified as passive and active.

-PASSIVE Attacks is when ⇒ entity tries to learn or make use of the information but does not affect the system resource.
-DO NOT involve alteration of data, thus are hard to detect.
-Therefore emphasis is on prevention rather than detection to counter passive attacks. Use encryption!!!

Two types of passive attacks are:

1. **Release of message content ⇒ adversary tries to learn content of message.**
2. **Traffic analysis ⇒ more subtle and used to determine the nature of conversation taking place, even if messages are encrypted.**

-Active Attacks ⇒ entity tries to directly interfere with the operation of system resource.

-They involve the alteration of data thus are easier to find than passive attacks.
-Involves modification or even a creation of false data stream.

Passive attacks hard to find but easy to deal with. Focus is on prevention.
Active attacks hard to find but hard to deal with. Goal is to detect and recover.

Subdivided into four categories:

1. **Replay, ⇒ capture of data unit & its subsequent transmission to produce replay-able copy for unauthorized us.**
2. **Masquerade,: when one entity acts as another. Includes replay, thus, masquerade is a part of Active attacks.**
    a. **Uses replay to capture access, credentials and use that to accesses an authorized users system without permission. Often modifying operation etc.**
3. **Modification of messages, ⇒ original message is altered, delayed, or re-ordered to produce and unusual effect.**
4. **Denial of service, ⇒ prevents normal use or management of communication facilities. Attack may have specific target (example: suppress messages being sent to a specific location), or can cause denial of service by disrupting, or disabling network by overloading it with messages to degrade performance.**

Chapter 1.3

Key word lol, => computer security technical measures.

Countermeasures into two categories:
-those that require computer security technical measures (covered in Parts One and Two), either hardware or software, or both.

and

-those that are fundamentally management issues (covered in Part Three).

-Security involves more than technology, it involves management component.

- “If you think technology can solve all your security problems, then you don't understand security and you don't understand technology.”

Security requirements based on Federal Information Processing Standard Publication FIPS 200.
<INSERT BIG TABLE WITH ALL THOSE REQUIREMENTS>

**********Chapter 1.4: Fundamental security design principles.**********

It is not yet possible to have a security design or implementation that excludes all flaws and prevents all unauthorized access.
-Thus, are a set of security design techniques that are considered to guide the development of the security mechanism.
- By National Center of Academic Excellence in Information (NCAE13), the design principles are:
-Economy of mechanism,
-Failsafe defaults,
-Complete mediation,
-Open design,
-Separation of privilege,
-Least privilege,
-Least common mechanism,
-Psychological acceptability,
-Isolation,
-Encapsulation,
-Modularity,
-Layering, and
-Least astonishment.
**********Chapter 1.5: Attack surfaces and attack trees*******

-used to evaluate and classify threats!
**********Chapter 1.6 Computer Security Strategy**********
-We look at overall strategy for providing computer security.

Computer scientist Butler Lampson suggests that a comprehensive security strategy involves three aspects:

- **Specification/policy: What is security scheme supposed to do?**
- **Implementation/mechanisms: How does it work?**
- **Correctness/assurance: Does it really work?**