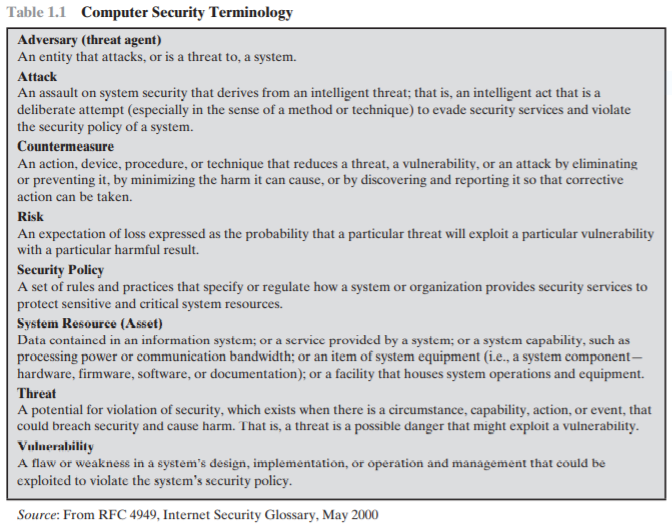
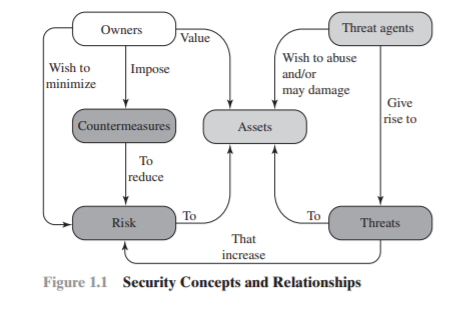
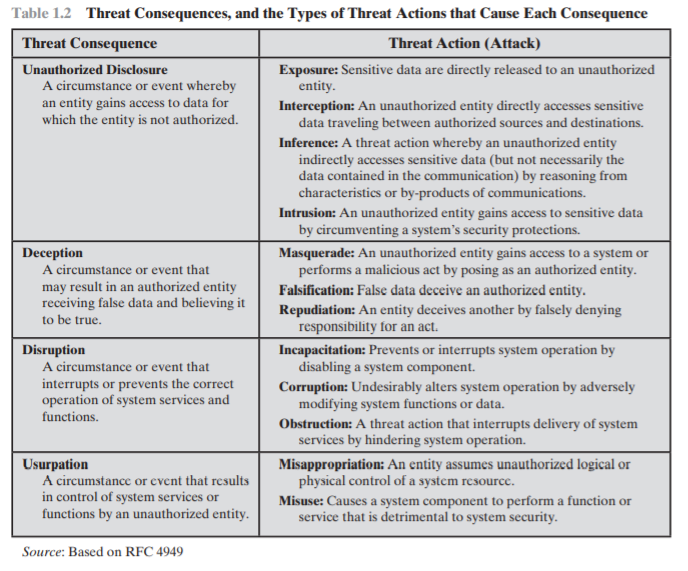
**Chapter 1:**

* 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).
* Confidentiality: This term covers two related concepts:
  + Data confidentiality:1 Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  + Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
* Integrity: This term covers two related concepts:
  + Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  + System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
* Availability: Assures that systems work promptly and service is not denied to authorized users.
* The three highlighted points are known as the **CIA triad**
* FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:
  + Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
  + Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
  + Availability: Ensuring timely and reliable access to and use of information. A loss of availability
* While the CIA triad paints a good picture, not everyone believes it paints the full picture. Two extra points are often mentioned:
  + Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
  + Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes
* Three levels of danger are presented from Low to Moderate to High





* Users wish to protect many things including:
  + Hardware
  + Software
  + Data
  + Communication facilities and networks
* Examples of vulnerabilities:
  + Corrupted: stored data / retrieved data is manipulated
  + Leaky: someone who shouldn’t be able to access the information can do so
  + Unavailable: super slow to reach or completely inaccessible
* Person Carrying out attack on system is known as the **threat agent**
* Two main types of attacks:
  + **Active**: attempt to alter system resources or affect operation
  + **Passive attack:** an attempt to learn or make use of info taken
* Further classify attacks as:
  + Inside: “insider” attack, someone who obtains access the right way but uses the info in the wrong way
  + Outside: “outsider” attack, range from pranksters, to terrorists, to hostile governments
* **Unauthorized Disclosure** = threat to confidentiality. Some of the following can be the attacks that cause the consequence:
  + Exposure: This can be deliberate, as when an insider intentionally releases sensitive information, such as credit card numbers, to an outsider. It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorized knowledge of sensitive data. There have been numerous instances of this, such as universities accidentally posting student confidential information on the Web
  + Interception: Interception is a common attack in the context of communications. On a shared local area network (LAN), such as a wireless LAN or a broadcast Ethernet, any device attached to the LAN can receive a copy of packets intended for another device. On the Internet, a determined hacker can gain access to e-mail traffic and other data transfers. All of these situations create the potential for unauthorized access to data.
  + Inference: An example of inference is known as traffic analysis, in which an adversary is able to gain information from observing the pattern of traffic on a network, such as the amount of traffic between particular pairs of hosts on the network. Another example is the inference of detailed information from a database by a user who has only limited access; this is accomplished by repeated queries whose combined results enable inference.
  + Intrusion: An example of intrusion is an adversary gaining unauthorized access to sensitive data by overcoming the system’s access control protections.
  + Deception is a threat to either system integrity or data integrity. The following types of attacks can result in this threat consequence:
    - Masquerade: One example of masquerade is an attempt by an unauthorized user to gain access to a system by posing as an authorized user; this could happen if the unauthorized user has learned another user’s logon ID and password. Another example is malicious logic, such as a Trojan horse, that appears to perform a useful or desirable function but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic
    - Falsification: This refers to the altering or replacing of valid data or the introduction of false data into a file or database. For example, a student may alter his or her grades on a school database
    - Repudiation: In this case, a user either denies sending data or a user denies receiving or possessing the data.
  + Disruption is a threat to availability or system integrity. The following types of attacks can result in this threat consequence:
    - * Incapacitation: This is an attack on system availability. This could occur as a result of physical destruction of or damage to system hardware. More typically, malicious software, such as Trojan horses, viruses, or worms, could operate in such a way as to disable a system or some of its services.
      * Corruption: This is an attack on system integrity. Malicious software in this context could operate in such a way that system resources or services function in an unintended manner. Or a user could gain unauthorized access to a system and modify some of its functions. An example of the latter is a user placing backdoor logic in the system to provide subsequent access to a system and its resources by other than the usual procedure.
      * Obstruction: One way to obstruct system operation is to interfere with communications by disabling communication links or altering communication control information. Another way is to overload the system by placing excess burden on communication traffic or processing resources. Usurpation is a threat to system integrity. The following types of attacks can result in this threat consequence:
      * Misappropriation: This can include theft of service. An example is a distributed denial of service attack, when malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host. In this case, the malicious software makes unauthorized use of processor and operating system resources.
      * Misuse: Misuse can occur by means of either malicious logic or a hacker that has gained unauthorized access



**Vulnerabilities**

* Hardware is a major threat from stealing to damage to unauthorized access
* Software (OS, utilities, apps) is easy to delete, damage/alter, and manipulate.
  + Includes viruses and such
* Data (including data security)
  + Data affects statistics and manipulation of nay point will throw statistics in unprecedented direction
* Communication lines and networks

CHAPTER 2:

