BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction – Part-1

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Security - Introduction

innovate achieve lead

Agenda

- Computer Security Concepts
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy
- Standards

Threats & Assets

Threats & Assets

Categories

- The assets of a computer system can be categorized as:
  - Hardware
  - Software
  - Data
  - Communication lines and networks

Threats & Assets

innovate achieve lead

Hardware

- Includes personal computers, workstations, networks, and peripherals such as USB Drives, External Hard drives, etc.
  - Availability
    - A major threat to computer system hardware is the threat of availability
    - Hardware is the most vulnerable to attack and automated controls have least effect on them
    - Threats include accidental and deliberate damage to equipment as well as theft
    - The proliferation of personal computers and workstations and the widespread use of LANs increase the potential for losses in this area
  - Confidentiality
    - Theft of USB Drives can lead to loss of confidentiality
    - Physical and administrative security measures are needed to deal with these threats

Threats & Assets

Software

- Includes the operating system, utilities, and application programs
  - Availability
    - Application software, is often easy to delete
    - Software can also be altered or damaged to render it useless
    - Software configuration management, which includes making backups of the most recent version of software, can improve availability
  - Integrity
    - A modified software can still function but that behaves differently than before
    - Computer viruses and related attacks fall into this category
  - Confidentiality
    - Protection against software piracy is a major challenge
    - Although certain countermeasures are available, by and large the problem of unauthorized copying of software has not been solved.

Threats & Assets

innovate achieve lead

Data

- Involves files and other forms of data controlled by individuals, groups, and business organizations
  - Availability
    - Involves destruction of data files
  - Integrity
    - Data modifications can have consequences ranging from minor to disastrous
  - Confidentiality
    - Unauthorized reading of data files or databases has been the most researched topic in the area of computer security

Threats & Assets

innovate achieve lead

Communication Lines and Networks

- Attacks on communication lines and networks can be classified as passive attacks and active attacks
- Passive attack
  - Attempts to learn or make use of information from the system but does not cause any harm to the system resources
- Active attack
  - Attempts to alter system resources or affect their operation

Threats & Assets

innovate achieve lead

Communication Lines and Networks

- Passive attack
  - They are in the nature of eavesdropping on (monitoring of) transmissions
  - The goal of the attacker is to obtain information that is being transmitted
  - Two types of passive attacks:
    - Release of message contents
    - Traffic analysis

Threats & Assets

Communication Lines and Networks

- Passive attack
  - Release of message contents
    - E.g., a telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information
    - We would like to prevent an opponent from learning the contents of these transmissions.
  - Traffic analysis
    - Suppose that we can encrypt the contents of messages so that opponents, even if they captured the message, could not extract the information from the message
    - An opponent might still be able to observe the pattern of these messages
    - The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged
    - This information might be useful in guessing the nature of the communication that was taking place

Threats & Assets

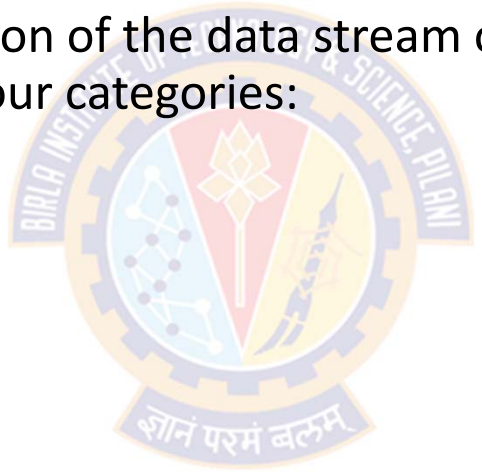
Communication Lines and Networks

- Passive attack
  - Passive attacks are very difficult to detect because they do not involve any alteration of the data
  - Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern
  - However, it is feasible to prevent the success of these attacks, usually by means of encryption
  - Thus, the emphasis in dealing with passive attacks is on prevention rather than detection

Threats & Assets

Communication Lines and Networks

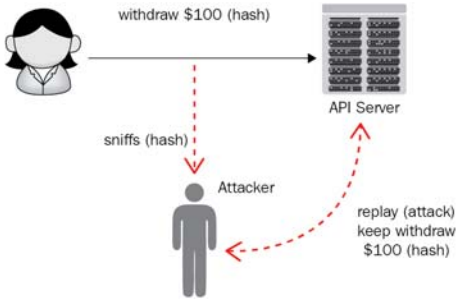
- Active attacks
  - They involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:
    - Replay
    - Masquerade
    - Modification of messages, and
    - Denial of service.



Threats & Assets

Communication Lines and Networks

- Active attacks
  - Replay
    - Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
  - Masquerade
    - A masquerade takes place when one entity pretends to be a different entity
    - A masquerade attack usually includes one of the other forms of active attack (E.g., Replay attack)
    - For example:
      - Authentication sequences are captured
      - After a valid authentication sequence has taken place, it is replayed, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges



Threats & Assets

Communication Lines and Networks

- Active attacks
  - Modification of messages
    - It means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect
    - For example, a message stating, "Allow John Smith to read confidential file accounts" is modified to say, "Allow Fred Brown to read confidential file accounts."
  - The denial of service
    - Prevents or inhibits the normal use or management of communication facilities
    - This attack may have a specific target
      - For example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service)
    - Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance

Threats & Assets

Communication Lines and Networks

- Active attacks
  - Whereas passive attacks are difficult to detect, measures are available to prevent their success
  - On the other hand, it is quite difficult to prevent active attacks 100%
    - Because to do so would require physical protection of all communication facilities and paths at all times
  - Instead, the goal is to detect them and to recover from any disruption or delays caused by them
  - Because the detection has a deterrent effect, it may also contribute to prevention

Threats & Assets

Threats and Assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service	An unencrypted USB drive 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


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!