BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction

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

Agenda

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

Security Design Principles

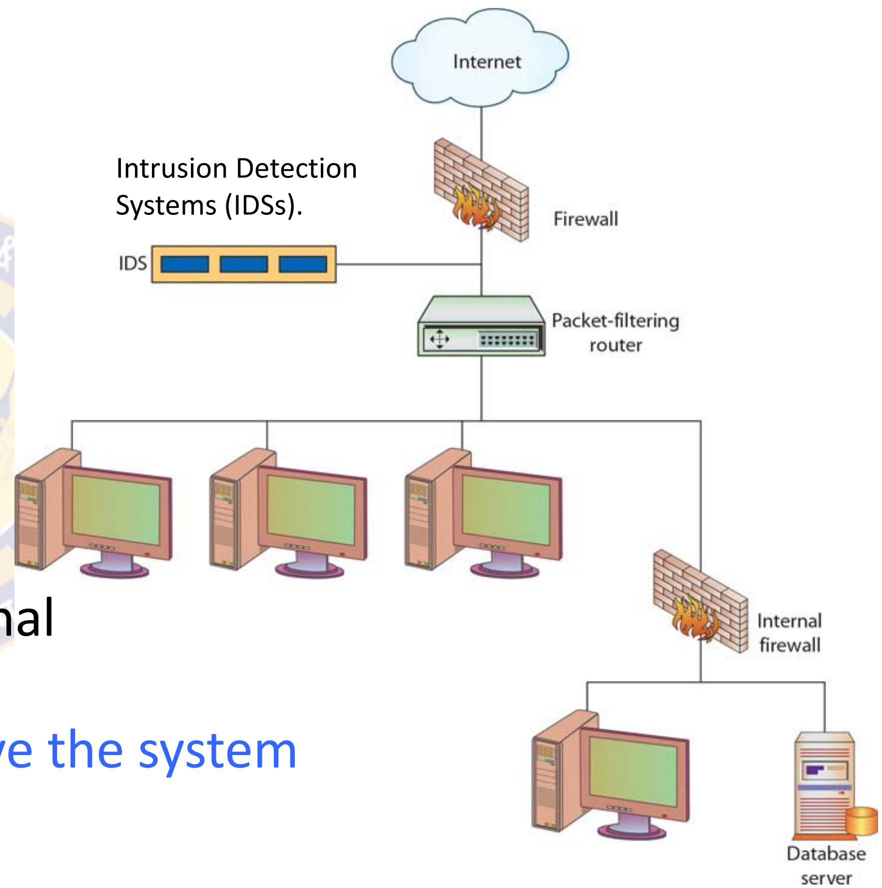
Modularity

- Modularity principle says that the security mechanism must be developed:
  - as separate and protected modules, and
  - using the modular architecture
- The design goal here is to provide security functions and services (E.g., cryptographic functions), as common modules
- Numerous protocols and applications make use of cryptographic functions
- Rather than implementing such functions in each protocol or application, provide a common cryptographic module that can be invoked by other applications
- The module structure helps us in
  - a) focusing on the secure design and implementation of a single cryptographic module
  - b) focusing on the mechanisms to protect the module from tampering
  - c) migrating to new technology or upgrading the features of security mechanism without modifying the entire system

Security Design Principles

Layering

- Similar to defense in depth
- Involves the use of multiple, overlapping protection approaches in a series
- Provides multiple barriers to the adversary from accessing the protected system
- Allows for different types of controls to guard against threats
- Addresses people, technology, and operational aspects of information systems
- Security breach of any one layer will not leave the system unprotected



Security Design Principles

Least Astonishment

- Security mechanisms should use a model that the users can easily understand
- The security mechanisms should be designed such that using the mechanism is simple
  - Hide complexity introduced by security mechanisms
  - Ease of installation, configuration, and use
- The security mechanism should be such that the user has a good intuitive understanding of how the security goals map to the provided security mechanism
- The program should always respond in the way that is least likely to astonish the user
  - E.g., at the time of login, the system should not ask your SSN or date of birth
- Configuring and executing a program should be as easy and as intuitive as possible, and any output should be clear, direct, and useful

Attack Surfaces and Attack Trees

Attack Surfaces and Attack Trees

Attack Surfaces

- An attack surface
  - is the set of entry points that attackers can use to compromise a system.
  - consists of reachable and exploitable vulnerabilities in a system
- Keeping the attack surface as small as possible is a basic security measure
- Examples:
  - Open ports on outward facing Web and other servers, and code listening on those ports
  - Services that are available on the inside of a firewall
  - Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
  - Interfaces, SQL, and Web forms
  - An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surfaces and Attack Trees

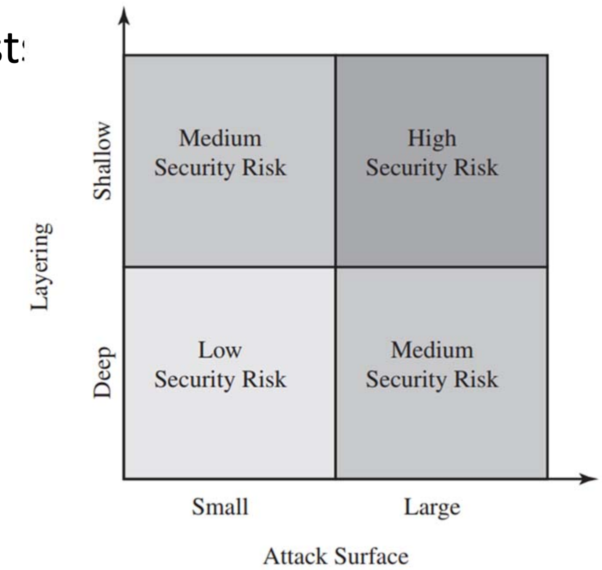
Attack Surfaces

- Categories of Attack surfaces:
  - Network attack surface
    - Refers to vulnerabilities over LANs, WANs, or the Internet
    - Includes network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.
  - Software attack surface
    - Refers to vulnerabilities in application, utility, or operating system code
    - A particular focus in this category is Web server software
  - Human attack surface
    - Refers to vulnerabilities created by employees or outsiders
    - Includes, social engineering, human error, and trusted insiders

Attack Surfaces and Attack Trees

Attack Surface Analysis

- Is a useful technique for assessing the scale and severity of threats to a system
- A systematic analysis of vulnerable points makes security analysts aware of where security mechanisms are required
- Once an attack surface is defined, designers may be able to find ways to make the surface smaller, thus making the task of the adversary more difficult
- It provides guidance on:
  - setting priorities for testing,
  - strengthening security measures, or
  - modifying the service or application

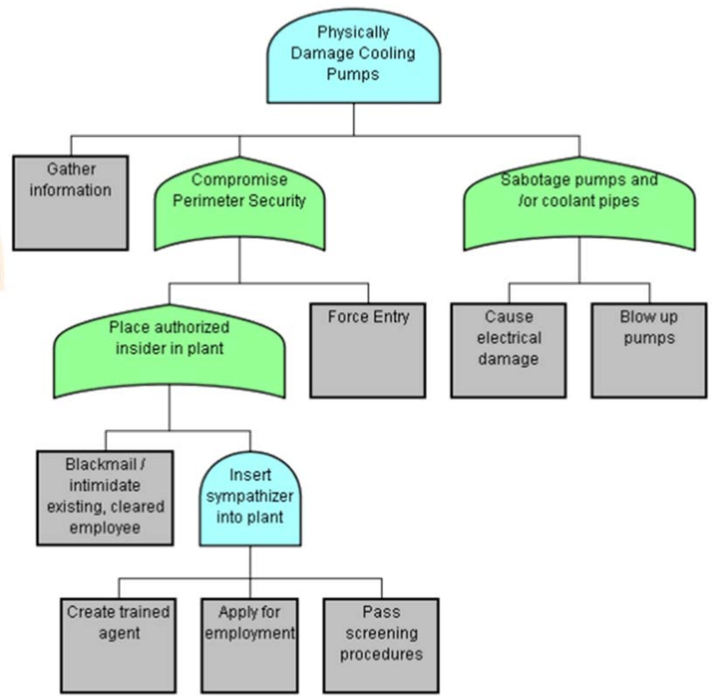


- The use of layering (or defense in depth), and attack surface reduction complement each other in mitigating security risk

Attack Surfaces and Attack Trees

Attack Trees

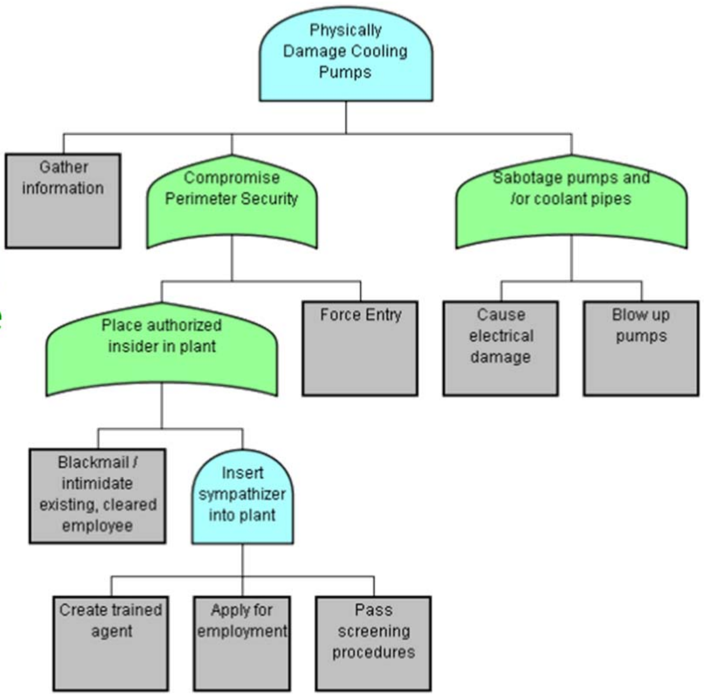
- An attack tree shows a set of potential techniques for exploiting security vulnerabilities
- The goal of the attack (the security incident) is represented as the root node
- Branches and subnodes represent the ways in which the goal can be reached
- Each subnode defines a subgoal
  – Each subgoal may have its own set of further subgoals, etc.



Attack Surfaces and Attack Trees

Attack Trees

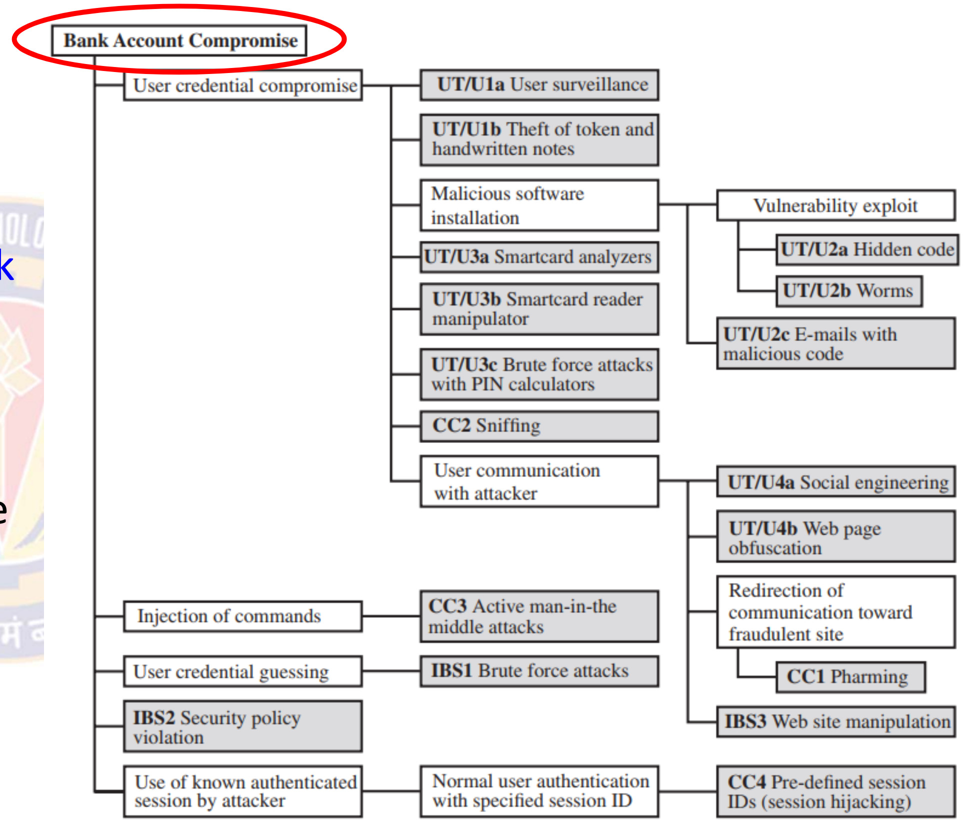
- The leaf nodes represent different ways to initiate an attack
- Each node other than a leaf is either an AND-node or an OR-node
- To achieve the goal represented by an AND-node,
  - all the subgoals represented by that node's subnodes must be achieved
- To achieve the goal represented by an OR-node,
  - at least one of the subgoals must be achieved
- Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared



Attack Surfaces and Attack Trees

Attack Trees – Example

- The goal of the attacker is to compromise a user's bank account
- The shaded boxes (leaf nodes) represent the attack events
- The white boxes are categories which consist of one or more specific attack events (leaf nodes)
- In this tree, all the nodes other than leaf nodes are OR-nodes
- Three components involved in authentication:
  - User terminal and user (UT/U)
  - Communications channel (CC)
  - Internet banking server (IBS)

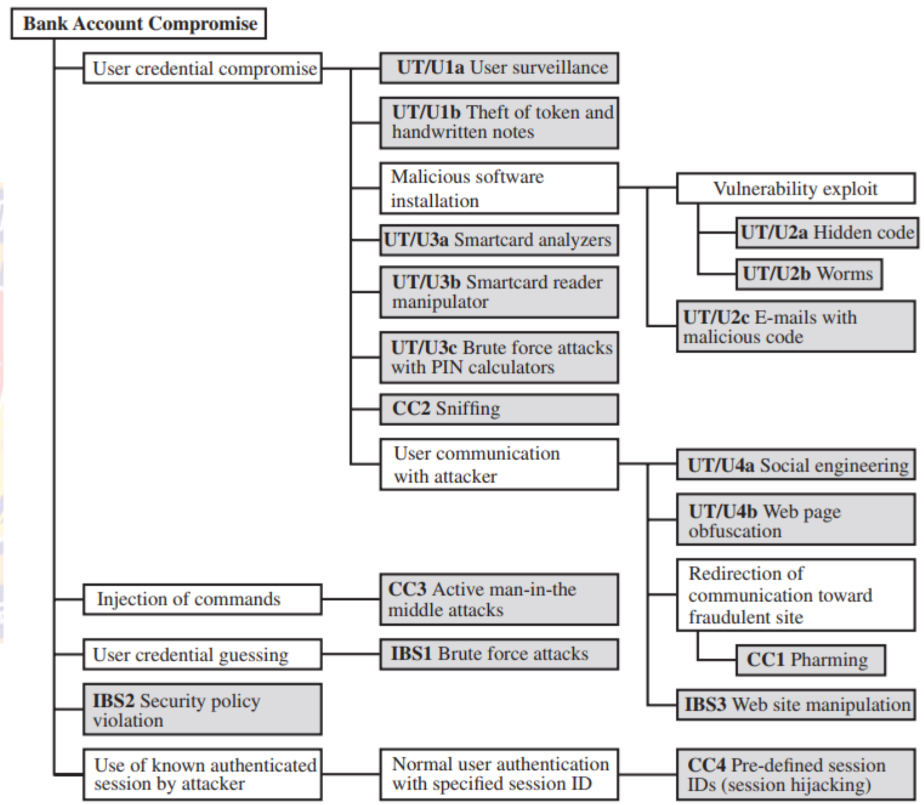


An Attack Tree for Internet Banking Authentication

Attack Surfaces and Attack Trees

Attack Trees – Example

- User terminal and user (UT/U):
  - These attacks target the user equipment, including the tokens such as smartcards or other password generators, as well as the actions of the user
- Communications channel (CC):
  - This type of attack focuses on communication links
- Internet banking server (IBS):
  - These types of attacks target the servers that host the Internet banking application

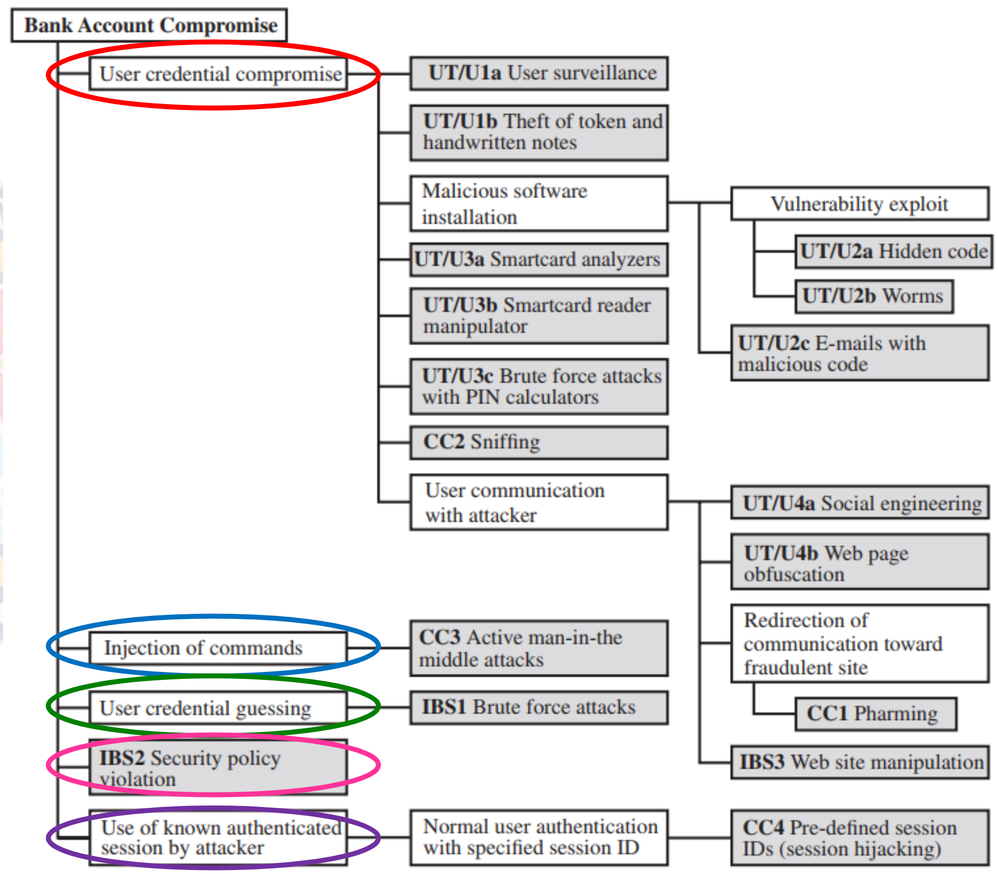


An Attack Tree for Internet Banking Authentication

Attack Surfaces and Attack Trees

Attack Trees – Example

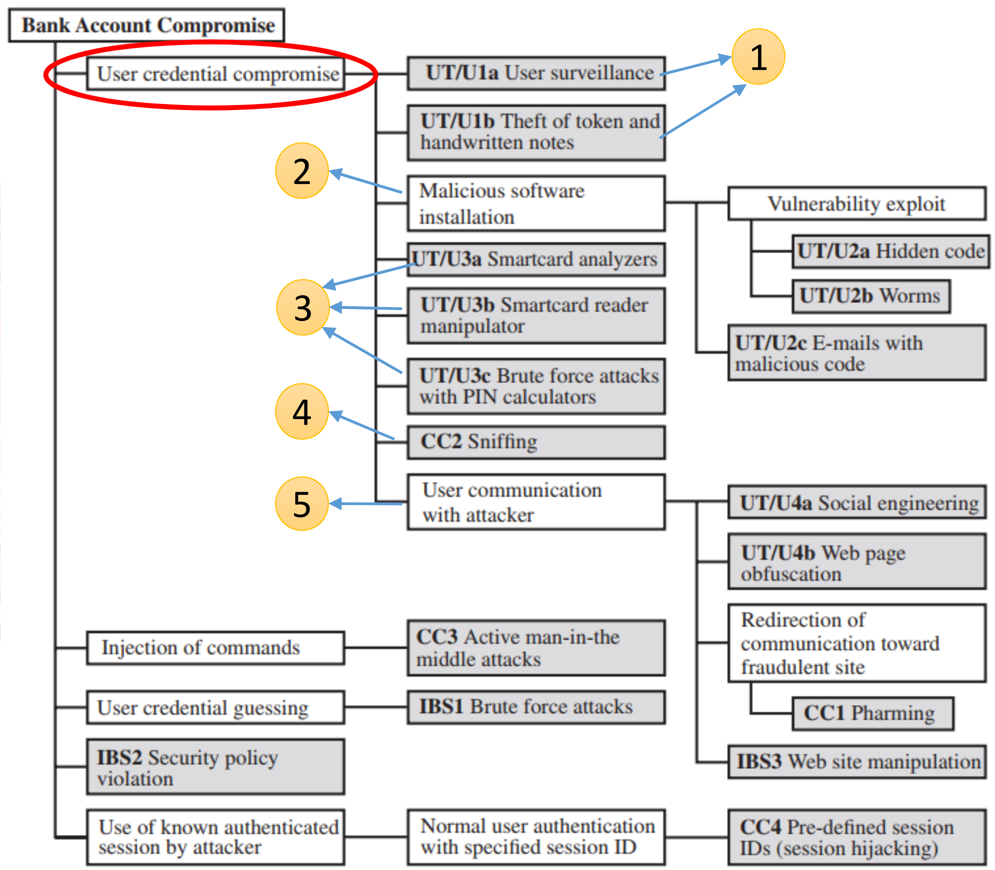
- Attack Strategies
  - Five attack strategies can be identified
    - User credential compromise
    - Injection of commands
    - User credential guessing
    - IBS Security policy violation
    - Use of known authenticated session
  - Each of the above exploits one or more of the three components



Attack Surfaces and Attack Trees

Attack Trees – Example

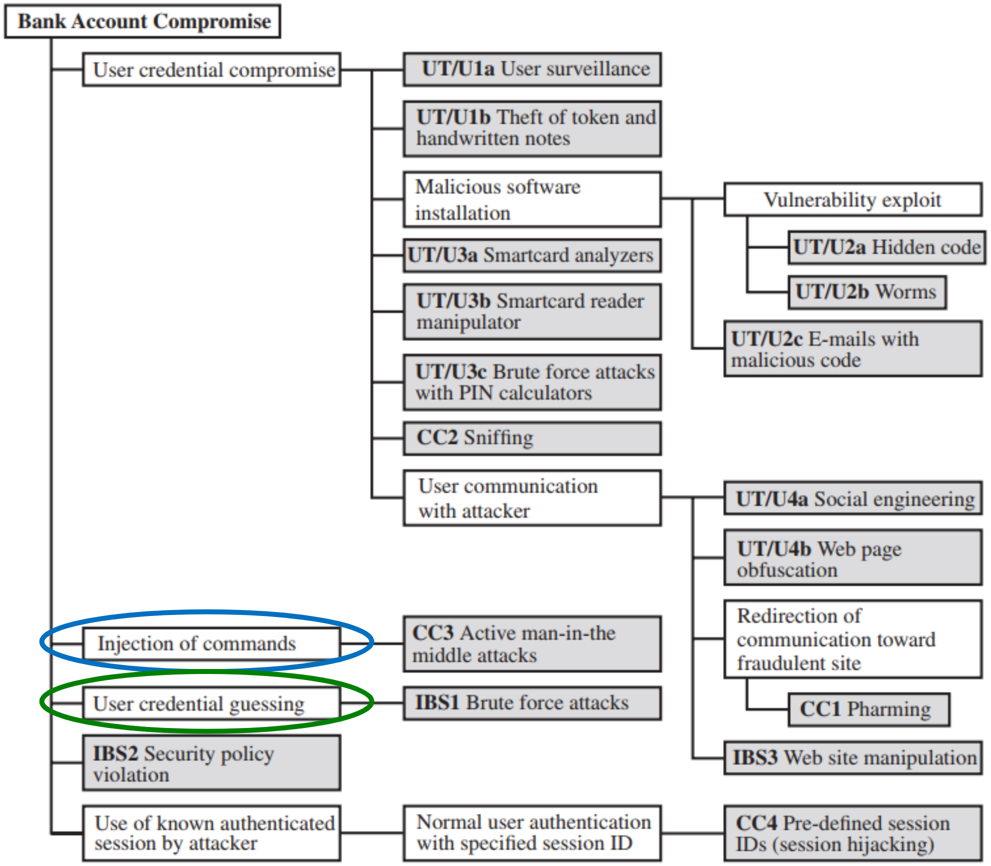
- User credential compromise
  - This strategy can be used against many elements of the attack surface
  - 1) by using procedural attacks
    - Monitoring a user's action to observe a PIN or other credential
    - Theft of the user's token or handwritten notes
  - 2) embedding malicious software to compromise the user's login and password
  - 3) by using token attack tools
    - Hacking the smartcard
    - Using a brute force approach to guess the PIN
  - 4) obtaining credential information via the communication channel (sniffing)
  - 5) engaging in communication with the target user



Attack Surfaces and Attack Trees

Attack Trees – Example

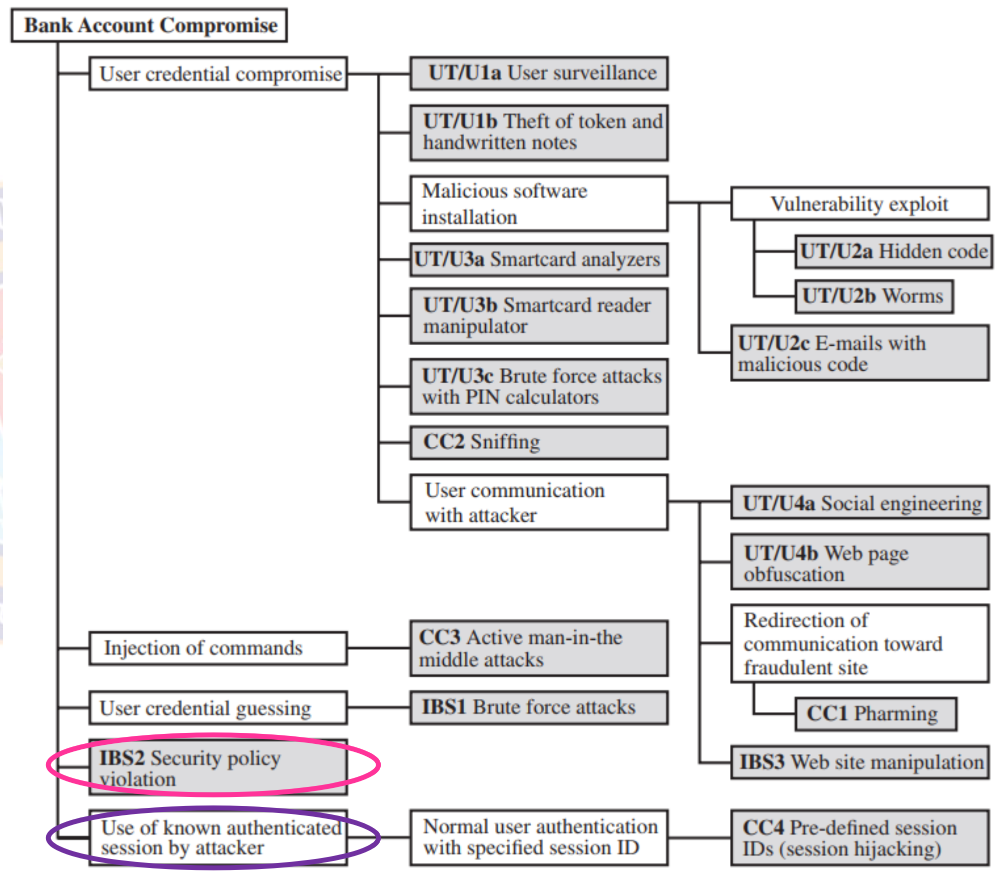
- Injection of commands
  - Involves intercepting communication between the UT and the IBS
  - Involves impersonating the valid user to gain access to the banking system.
- User credential guessing
  - Involves brute force attacks against banking authentication schemes by
    - sending random usernames and passwords
  - The attack mechanism can be by using
    - distributed zombie personal computers,
    - hosting automated programs for username- or password-based calculation



UT/U: User terminal and user, IBS: Internet Banking Server

Attack Trees – Example

- Security policy violation
  - An employee may expose a customer's account by
    - Sharing passwords
    - Using weak access control and logging mechanisms
- Use of known authenticated session
  - Persuading or forcing the user to connect to the IBS with a preset session ID
  - Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity



Attack Surfaces and Attack Trees

Attack Trees

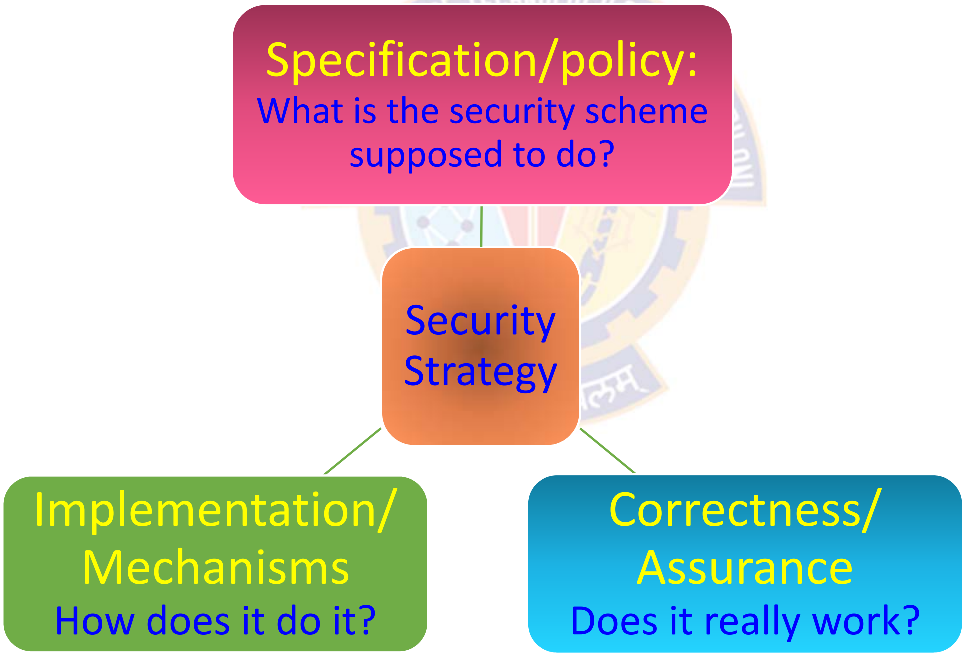
- Attack trees are used to effectively exploit the information available on attack patterns
- Organizations such as CERT developed body of knowledge about
  - general attack strategies and
  - specific attack patterns
- These organizations publish security advisories
- Security analysts can use the attack tree to document security attacks in a structured form that reveals key vulnerabilities
- The attack tree can guide both:
  - the design of systems and applications, and
  - the choice and strength of countermeasures

CERT = The Indian Computer Emergency Response Team

Computer Security Strategy

Comprehensive Security Strategy

- A comprehensive security strategy involves three aspects:



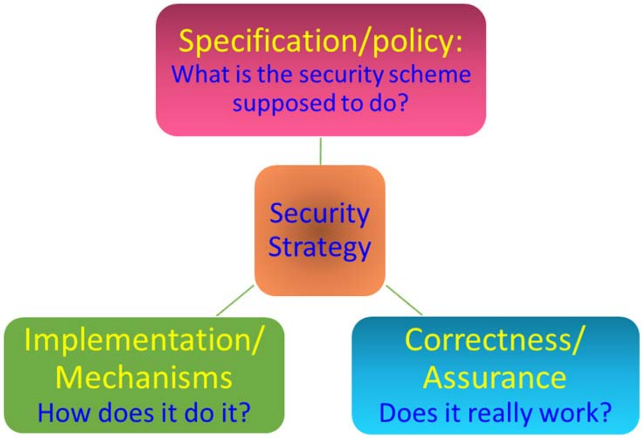
Computer Security Strategy

Security Policy

- Developing a security policy is the first step in devising security services and mechanisms
- A security policy
  - Is a statement of rules and practices that specify the type of security services required to protect sensitive and critical system resources
  - Describes the desired system behavior
  - Includes the requirements for confidentiality, integrity, and availability
  - Formal security policies are enforced by the system's technical controls, management controls, and operational controls

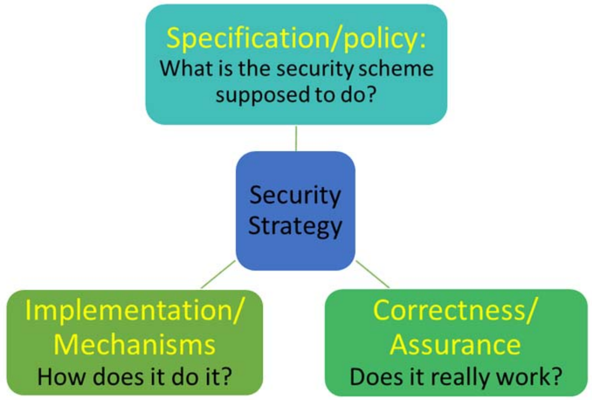
Security Policy

- In developing a security policy, a security manager needs to consider the following factors and tradeoffs:
  - Factors
    - The value of the assets being protected
    - The vulnerabilities of the system
    - Potential threats and the likelihood of attacks
  - Trade-offs
    - Ease of use versus level of security
    - Cost of security versus cost of failure and recovery



Computer Security Strategy

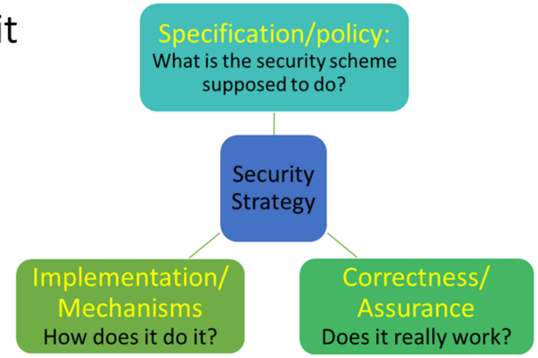
Security Policy – Trade-offs



- Ease of use versus security
  - Virtually all security measures involve some penalty in the area of ease of use
  - For example:
    - Access control mechanisms require users to remember passwords and perhaps perform other access control actions
    - Firewalls and other network security measures may reduce available transmission capacity or slowdown response time
    - Virus-checking software
      - reduces available processing power and
      - introduces the possibility of system crashes or malfunctions due to improper interaction between the security software and the operating system

Security Policy – Trade-offs

- Cost of security versus cost of failure and recovery
  - Costs of implementing and maintaining security measures must be balanced against the cost of security failure and recovery
  - The cost of security failure and recovery must take into account:
    - the value of the assets being protected and the damages resulting from a security violation
    - the risk, which is the probability that a particular threat will exploit a particular vulnerability with a particular harmful result



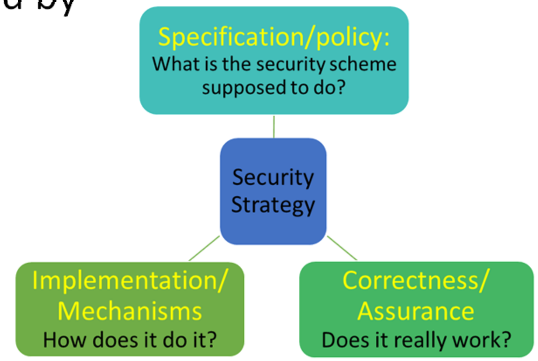
Security Implementation

- Security implementation involves four complementary courses of action:
  - Prevention
  - Detection
  - Response
  - Recovery

Computer Security Strategy

Security Implementation

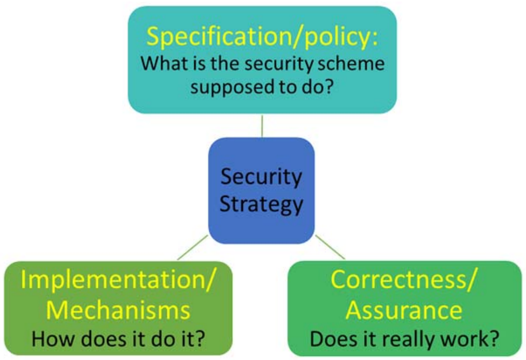
- Prevention
  - An ideal security scheme is one in which no attack is successful
    - This is impractical
  - There is a wide range of threats in which prevention is a reasonable goal
  - Example: Transmission of encrypted data
    - Attacks on confidentiality of the transmitted data can be prevented by
      - using secure encryption algorithm and
      - taking measures to prevent unauthorized access to encryption keys



Computer Security Strategy

Security Implementation

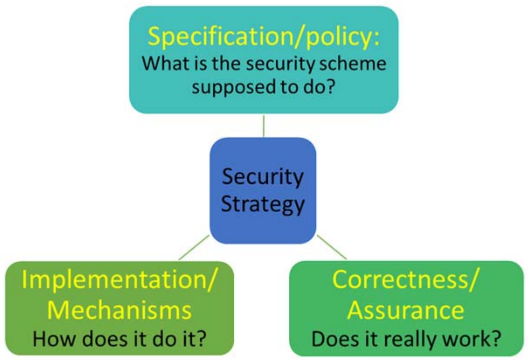
- Detection
  - Absolute prevention is not feasible, but it is practical to detect security attacks
  - For example:
    - Detecting the presence of unauthorized individuals logged into a system using intrusion detection systems
    - Detecting a denial of service attack
      - Communications or processing resources are consumed so that they are unavailable to legitimate users



Computer Security Strategy

Security Implementation

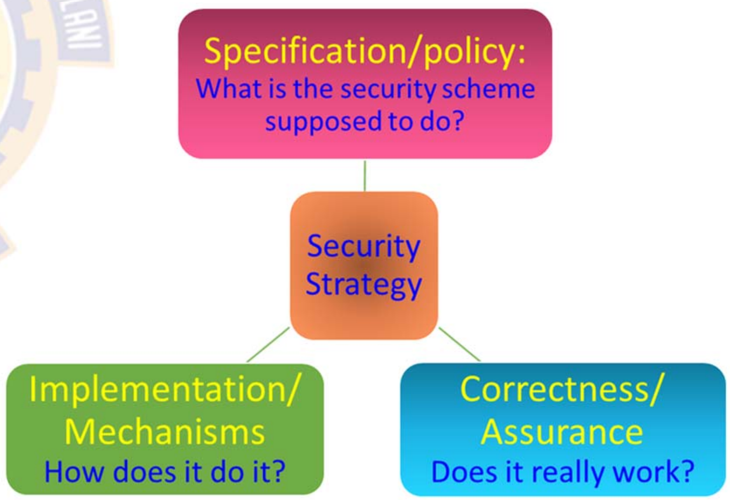
- Response:
  - Once an attack (E.g., denial of service) is detected, the system can respond by halting the attack and preventing further damage
- Recovery:
  - Assets (E.g., data) can be recovered using backup systems
  - If data integrity is compromised, a prior, correct copy of the data can be reloaded



Computer Security Strategy

Assurance and Evaluation

- The "consumers" of computer security services and mechanisms (e.g., system managers, vendors, customers, and end users) want to feel that the security measures work as intended
- This bring us to the concepts of:
  - Assurance and Evaluation

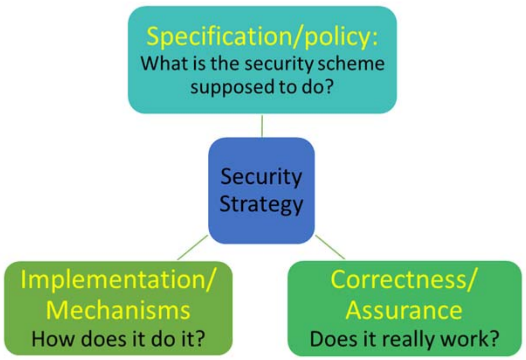


Computer Security Strategy

Assurance and Evaluation

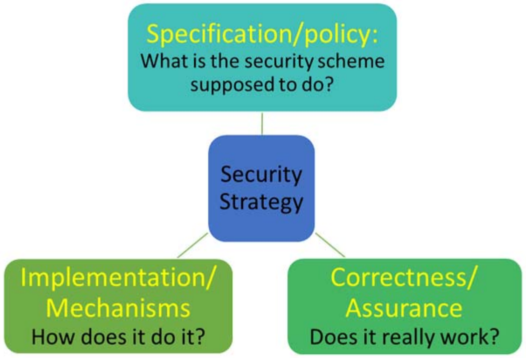
- Assurance
  - *"The degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes."*

    -- NIST95
  - This encompasses both system design and system implementation
  - Assurance deals with the questions such as:
    - "Does the security system design meet its requirements?"
    - "Does the security system implementation meet its specifications?"
  - Note:
    - Assurance is expressed as a degree of confidence, not in terms of a formal proof that a design or implementation is correct
    - It is not possible to provide absolute proof that designs and implementations are correct



Assurance and Evaluation

- Evaluation
  - It is the process of examining a computer product or system with respect to certain criteria
  - Evaluation involves formal testing of the computer product and process
  - The core work involves development of evaluation criteria that can be applied to any security services and mechanisms
  - These evaluation criteria can also broadly used for making product comparisons



Thank You!