

The Need for Information Security

Information Security:

It means Defending information from unauthorized access, use, disclosure, modification, recording or destruction.

Need for Information Security

1. **Availability:** Information must be accessible and available to users. Fault tolerance and recovery mechanism are put into place to ensure the continuity of the availability of resources.
2. **Integrity:** When a security mechanism provides integrity, it protects data or a resource, from being altered in an unauthorized fashion.
3. **Confidentiality:** information should not to be disclosed to unauthorized individuals.

Protecting the Ability to Function

- ▶ Management is responsible
- ▶ Information security is
 - a management issue
 - a people issue
- ▶ Communities of interest must argue for information security in terms of impact and cost

Enabling Safe Operation

- ▶ Organizations must create integrated, efficient, and capable applications
- ▶ Organization need environments that safeguard applications
- ▶ Management must not abdicate to the IT department its responsibility to make choices and enforce decisions

Protecting Data

- ▶ One of the most valuable assets is data
- ▶ Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers
- ▶ An effective information security program is essential to the protection of the integrity and value of the organization's data

Safeguarding Technology Assets

- ▶ Organizations must have secure infrastructure services based on the size and scope of the enterprise
- ▶ Additional security services may have to be provided
- ▶ More robust solutions may be needed to replace security programs the organization has outgrown

Threats

- ▶ Management must be informed of the various kinds of threats facing the organization
- ▶ A threat is an object, person, or other entity that represents a constant danger to an asset
- ▶ By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

Threats

- ▶ The 2002 CSI/FBI survey found:
 - 90% of organizations responding detected computer security breaches within the last year
 - 80% lost money to computer breaches, totaling over \$455,848,000 up from \$377,828,700 reported in 2001
 - The number of attacks that came across the Internet rose from 70% in 2001 to 74% in 2002
 - Only 34% of organizations reported their attacks to law enforcement

TABLE 2-1 Threats to Information Security⁴

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Cyber Security

Computer Security is all about studying Cyber Attacks with a view to defending against them.

.

Before we Discussed the common attacks encountered ,it is appropriate to ask.

What are the main goals of an attackers

Goals of the Attackers??????

Motive / Goal

1. Theft of Sensitive Information
2. Disruption of services:-
3. Illegal access to or use of resources.

Common Attacks

1. Phishing and Pharming Attacks
2. Skimming Attacks.
3. Side Channel Attacks
4. Dictionary Attacks
5. Denial Of service.
6. Virus.
7. Worms
8. Trozans

Vulnerabilities

It is a Weakness in a procedure, protocol, hardware, or software within an organization that has the potential to cause damage.

.

There are atleast four important vulnerability classes in the domain of security

1. Human Vulnerabilities
2. Protocol Vulnerabilities
3. Software Vulnerabilities.
4. Configuration Vulnerabilities.

Control

1. Access Control
2. Data Protection.
3. Prevention and Detection
4. Response , Recovery and Forensics.



Trojan horse arrives via e-mail or software such as free games



Trojan horse is activated when the software or attachment is executed



Trojan horse releases its payload, monitors computer activity, installs back door, or transmits information to hacker

FIGURE 2-8 Trojan Horse Attack

Compromises to Intellectual Property

- ▶ Intellectual property is “the ownership of ideas and control over the tangible or virtual representation of those ideas”
- ▶ Many organizations are in business to create intellectual property
 - trade secrets
 - copyrights
 - trademarks
 - patents

Compromises to Intellectual Property

- ▶ Most common IP breaches involve software piracy
- ▶ Watchdog organizations investigate:
 - Software & Information Industry Association (SIIA)
 - Business Software Alliance (BSA)
- ▶ Enforcement of copyright has been attempted with technical security mechanisms

Attacks

- ▶ An attack is the deliberate act that exploits vulnerability
- ▶ It is accomplished by a threat-agent to damage or steal an organization's information or physical asset
 - An exploit is a technique to compromise a system
 - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
 - An attack is then the use of an exploit to achieve the compromise of a controlled system

Malicious Code


- ▶ This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information
 - ▶ The state of the art in attacking systems in 2002 is the multi-vector worm using up to six attack vectors to exploit a variety of vulnerabilities in commonly found information system devices
- 

TABLE 2-2 Attack Replication Vectors

Vector	Description
IP scan and attack	Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection
Shares	Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach
Mass mail	By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems
Simple Network Management Protocol (SNMP)	In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of 2002

Attack Descriptions

- ▶ IP Scan and Attack – Compromised system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits
- ▶ Web Browsing – If the infected system has write access to any Web pages, it makes all Web content files infectious, so that users who browse to those pages become infected
- ▶ Virus – Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection

Attack Descriptions

- ▶ Unprotected Shares – using file shares to copy viral component to all reachable locations
- ▶ Mass Mail – sending e-mail infections to addresses found in address book
- ▶ Simple Network Management Protocol – SNMP vulnerabilities used to compromise and infect
- ▶ Hoaxes – A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached

Attack Descriptions

- ▶ Back Doors – Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource
- ▶ Password Crack – Attempting to reverse calculate a password
- ▶ Brute Force – The application of computing and network resources to try every possible combination of options of a password
- ▶ Dictionary – The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

Attack Descriptions

- ▶ Denial-of-service (DoS) –
 - attacker sends a large number of connection or information requests to a target
 - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
 - may result in a system crash, or merely an inability to perform ordinary functions
- ▶ Distributed Denial-of-service (DDoS) – an attack in which a coordinated stream of requests is launched against a target from many locations at the same time

In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.

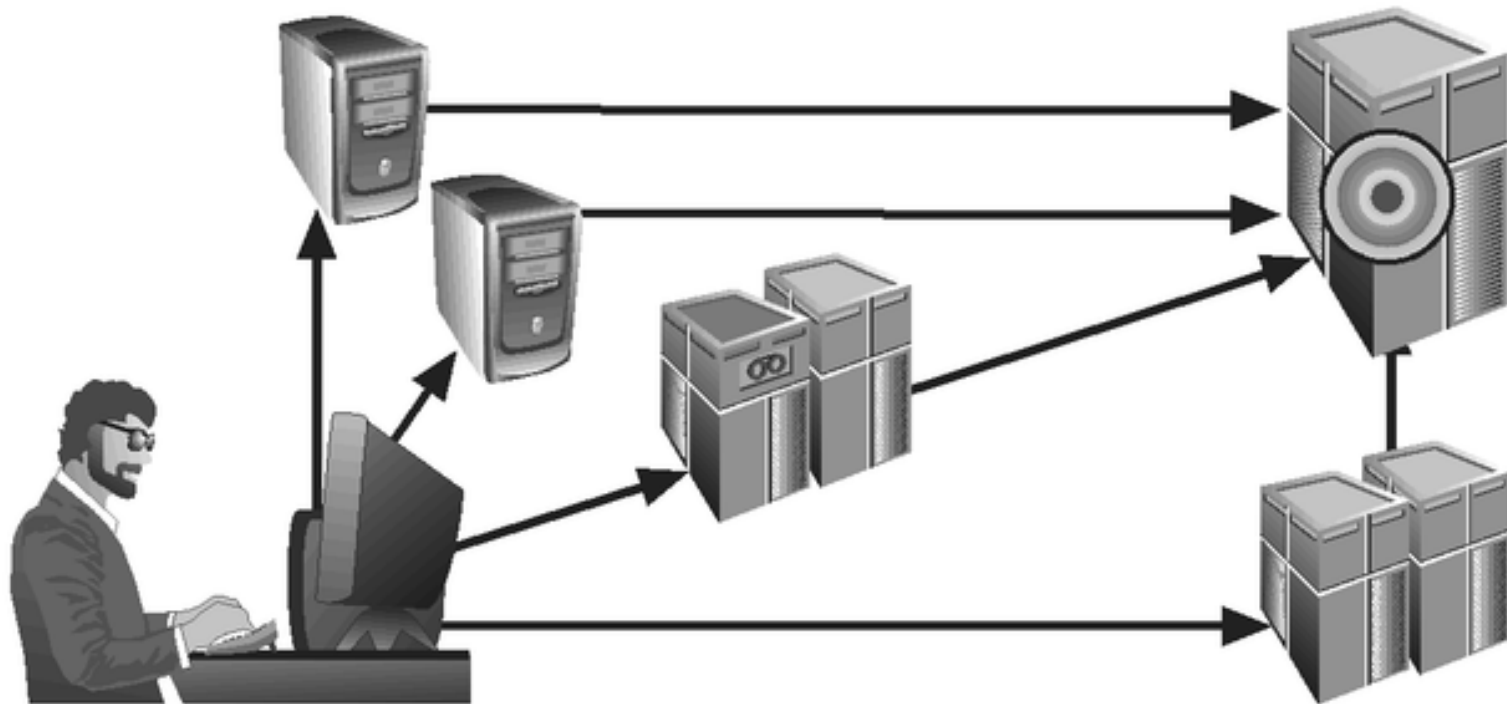


FIGURE 2-9 Denial-of-Service Attacks

Attack Descriptions

- ▶ Spoofing – technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- ▶ Man-in-the-Middle – an attacker sniffs packets from the network, modifies them, and inserts them back into the network
- ▶ Spam – unsolicited commercial e-mail – while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks

Data: Payload	IP source: 192.168.0.25	IP destination: 100.0.0.75
---------------	----------------------------	-------------------------------

Original IP packet
from hacker's system



Data: Payload	IP source: 100.0.0.80	IP destination: 100.0.0.75
---------------	--------------------------	-------------------------------

Spoofed (modified)
IP packet



Hacker modifies
source address to
spooof firewall

Data: Payload	IP source: 100.0.0.80	IP destination: 100.0.0.75
---------------	--------------------------	-------------------------------



Firewall allows
packet in, mistaking
if for legitimate traffic

Data: Payload	IP source: 100.0.0.80	IP destination: 100.0.0.75
---------------	--------------------------	-------------------------------



Spoofed packet
slips into intranet
to wreak havoc

FIGURE 2-10 IP Spoofing

1) Company A attempts to establish an encrypted session with Company B.



3) Company B sends all messages to the hacker who receives, decrypts, copies, and forwards copies (possibly modified) to Company B.



2) Hacker intercepts transmission, and poses as Company B. Hacker exchanges his own keys with Company A. Hacker then establishes a session with Company B, posing as Company A.



FIGURE 2-11 Man-in-the-Middle Attack

Attack Descriptions

- ▶ Mail-bombing – another form of e-mail attack that is also a DoS, in which an attacker routes large quantities of e-mail to the target
- ▶ Sniffers – a program and/or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network
- ▶ Social Engineering – within the context of information security, the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker

Attack Descriptions

- ▶ “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.”
- ▶ “brick attack” – the best configured firewall in the world can't stand up to a well placed brick

Attack Descriptions

- ▶ **Buffer Overflow** –
 - application error occurs when more data is sent to a buffer than it can handle
 - when the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure
- ▶ **Timing Attack** –
 - relatively new
 - works by exploring the contents of a web browser's cache
 - can allow collection of information on access to password-protected sites
 - another attack by the same name involves attempting to intercept cryptographic elements to determine keys and encryption algorithms