***Content from different reference book suggested by Prof. Prakash Sir and mentioned in CNS Syllabus file, Presentations, Notes provided in 2023***

NOTES ON BASIS OF CNS PPT IT SECURITY SECURITY OF INFORMATION ASSETS 60 SLIDES

---

**CHEAT SHEET - Read PPT once**

Information Security Cheat Sheet

Author: Vinod Sencha, Core Faculty(IS), RTI Jaipur

Slide 2: Learning Objectives

- Understand security threats to data, hardware, and users.
- Familiarize with common types of hacking.
- Learn protective measures.

Slide 3: IT Security

- IT security aims to protect computer systems and networks from various threats.
- Four key functions of IT security for organizations:
  1. Protect the organization's ability to function.
  2. Enable safe operation of IT applications.
  3. Protect collected and used data.
  4. Safeguard technology assets.

Slide 4: IT Security Features

Integrity
Availability
Security
Confidentiality

- Confidentiality: Ensures information is shared only among authorized entities.
- Integrity: Assures information authenticity and completeness.
- Availability: Guarantees systems are accessible when needed.

Slide 5: Vulnerabilities

- Vulnerabilities are weaknesses that can be exploited by threat actors.
- Classified by asset class: Hardware, Software, Network, Personnel, Physical Site, Organizational.

Slide 6: Threats

- Threats are potential negative actions facilitated by vulnerabilities.
- Threats can lead to unauthorized access, data modification, or denial of service.
- Various security threats: Users, Hardware, Data, and more.

Slide 8: Threats (Keywords)

- Keywords related to threats include Spam, Cookie, Web Bugs, Malware, Virus, Worm, Spyware, Hacking, Social Engineering, DDoS, Cybercrime, and Cyber-terrorism.

Slide 9: Attack Descriptions

- Denial-of-Service (DoS): Overwhelming a target with connection or information requests.
- Distributed DoS (DDoS): Coordinated attack from multiple locations.
- Spoofing: Sending messages with fake sender information.
- Man-in-the-Middle: Intercepting and modifying network traffic.
- Ping of Death: Sending oversized packets to crash a system.
- Buffer Overflow: Exploiting a buffer's size limit to execute code.
- Timing Attack: Exploiting browser cache to collect sensitive data.

Slide 13: Protective Measures

1. Bolster Access Control: Strong password policies, reset default passwords, and create access control policies.
2. Keep Software Updated: Regularly update software to fix vulnerabilities.
3. Standardize Software: Use standardized software, control software installations.
4. Use Network Protection Measures: Install firewalls, access controls, IDS/IPS, network segmentation, VPNs.
5. Employee Training: Educate employees on network security and threat identification.
6. Schedule Backups: Regularly backup data to external drives or the cloud.

Slide 17: Acts of Human Error or Failure

- Human errors can lead to data breaches and loss.
- Inexperience, improper training, incorrect assumptions, and other factors contribute to human errors.

Slide 20: Compromises to Intellectual Property

- Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- Software piracy is a common IP breach.
- Watchdog organizations investigate IP breaches.

Slide 24: Espionage/Trespass

- Espionage involves unauthorized access to gain information.
- Shoulder surfing can occur when someone accesses confidential data.
- Hackers use various techniques to breach systems, including social engineering.

Slide 26: Information Extortion

- Information extortion involves stealing data and demanding compensation for its return or non-use.
- Often seen in credit card number theft.

Slide 27: Sabotage or Vandalism

- Deliberate acts to sabotage or damage systems, including web defacing.
- Rising threat of hacktivism and cyber-terrorism.

Slide 31: Technical Hardware Failures or Errors

- Hardware flaws or errors can lead to system failures.
- Some defects are terminal, while others are intermittent.

Slide 33: Technological Obsolescence

- Outdated technology can result in unreliable systems.
- Proper planning and action by management can prevent obsolescence.

Slide 38: Deliberate Software Attacks

- Malicious code, such as viruses, worms, and Trojans, can compromise systems.
- Protection involves educating users, updating antivirus software, and implementing firewalls.

Slide 40: Forces of Nature

- Natural disasters like fire, flood, and earthquakes can disrupt systems.
- Contingency plans and controls are essential to limit damage.

Slide 45: Attaks

- An attack exploits vulnerabilities and compromises a controlled system.
- Exploits can lead to the compromise of systems.

Slide 50: Attack Descriptions

- Various attack types include IP scans, web browsing, viruses, Trojan horses, email bombing, sniffers, and social engineering.

Slide 56: Attack Descriptions

- Continued descriptions of attacks, including buffer overflows, ping of death, spoofing, and spam.

Slide 58: Attack Descriptions

- Attacks like timing attacks and IP scan attacks are explained.

Slide 60: Attack Descriptions

- Descriptions of attacks involving information extraction, including password cracks, brute force, and dictionary attacks.

This cheat sheet summarizes key concepts related to information security, threats, vulnerabilities, and protective measures.

---

**NOTES**

Detailed study notes based on the information you've provided from Vinod Sencha's presentation on "Security of Information Assets." Here are comprehensive notes for your exam preparation:

Slide 2 - Learning Objectives
- Security threats to data, hardware, and users.
- Common types of hacking.
- Protective measures.

Slide 3 - IT Security
- IT security is the protection of computer systems and networks from:
  - Information disclosure
  - Theft of hardware, software, or electronic data
  - Disruption or misdirection of services
- IT security functions:
  1. Protects an organization's ability to function.
  2. Enables safe operation of applications on IT systems.
  3. Protects collected and used data.
  4. Safeguards technology assets.

Slide 4 - IT Security: Features
- Confidentiality:
  - Ensures information is shared only with authorized entities.
- Integrity:
  - Assures information is authentic and complete.
  - Maintains data accuracy and consistency throughout its lifecycle.
- Availability:
  - Ensures systems for delivering, storing, and processing information are accessible when needed by authorized users.

Slide 5 - Vulnerabilities
- Vulnerability Definition: A weakness that can be exploited by a threat actor to perform unauthorized actions.
- Classified by asset class:
  - Hardware: Susceptibility to factors like humidity, dust, overheating.
  - Software: Insufficient testing, insecure coding, lack of audit trail, design flaws.
  - Network: Unprotected communication lines, insecure network architecture.
  - Personnel: Inadequate recruiting, security awareness, insider threats.
  - Physical Site: Exposure to natural disasters, power source interruptions.
  - Organizational: Lack of audits, continuity plans.

Slide 6 - Threats
- Threats are potential negative actions or events facilitated by vulnerabilities.
- Types of security threats:

- Users: Identity theft, loss of privacy, exposure to spam, physical injuries.
- Hardware: Power-related problems, theft, vandalism, natural disasters.
- Data: Malware, hacking, cybercrime, cyberterrorism.

Slide 8 - Threats (Keywords)

- Spam: Unsolicited commercial email.
- Cookie: A small text file on a web server.
- Web Bugs: Small gifs embedded in webpages/emails.
- Malware: Malicious software (Viruses, Worms, Spyware, Trojan Horses, Botnets).
- Shoulder Surfing: Unauthorized viewing of screens or keyboards.
- Hacking, Sniffing, Social Engineering, Spoofing, DDoS: Various cyber threats.

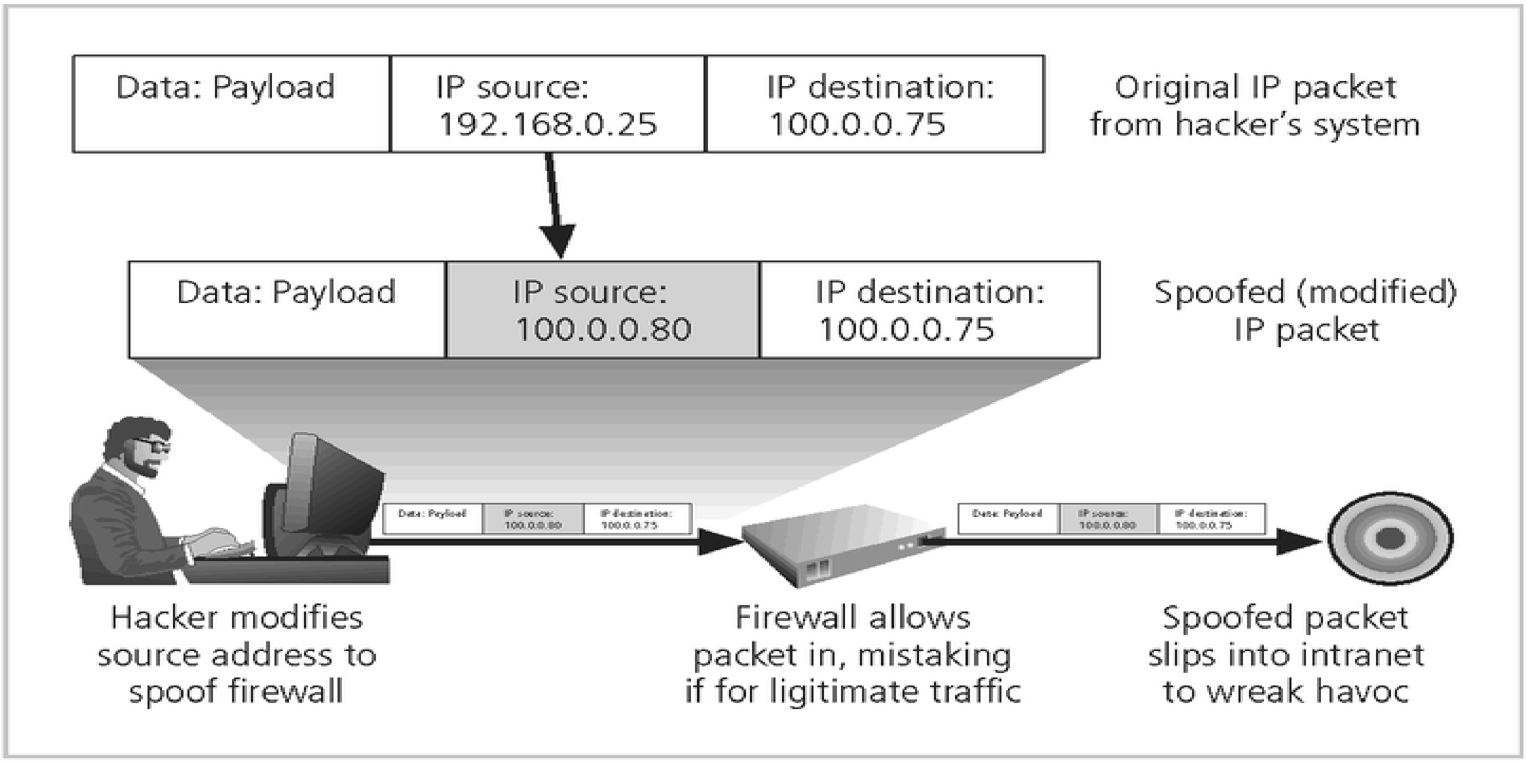

Data: Payload
IP source: 192.168.0.25
IP destination: 100.0.0.75
Original IP packet from hacker's system
Data: Payload
IP source: 100.0.0.80
IP destination: 100.0.0.75
Spoofed (modified) IP packet
Data: Payload
IP source: 100.0.0.80
IP destination: 100.0.0.75
Data: Payload
IP source: 100.0.0.80
IP destination: 100.0.0.75
Hacker modifies source address to spoof firewall
Firewall allows packet in, mistaking if for ligitimate traffic
Spoofed packet slips into intranet to wreak havoc

**FIGURE 2-10** IP Spoofing

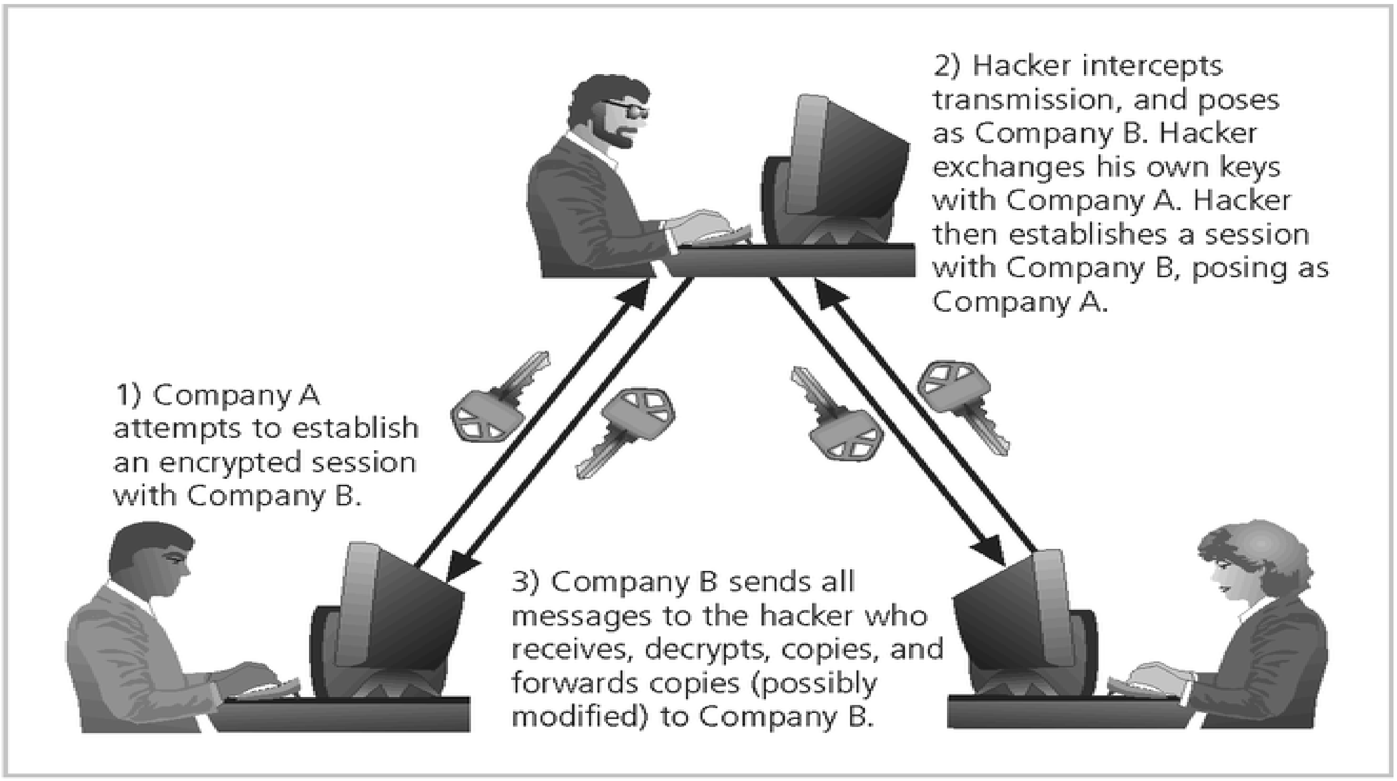

2) Hacker intercepts transmission, and poses as Company B. Hacker exchanges his own keys with Company A. Hacker then establishes a session with Company B, posing as Company A.
1) Company A attempts to establish an encrypted session with Company B.
3) Company B sends all messages to the hacker who receives, decrypts, copies, and forwards copies (possibly modified) to Company B.

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

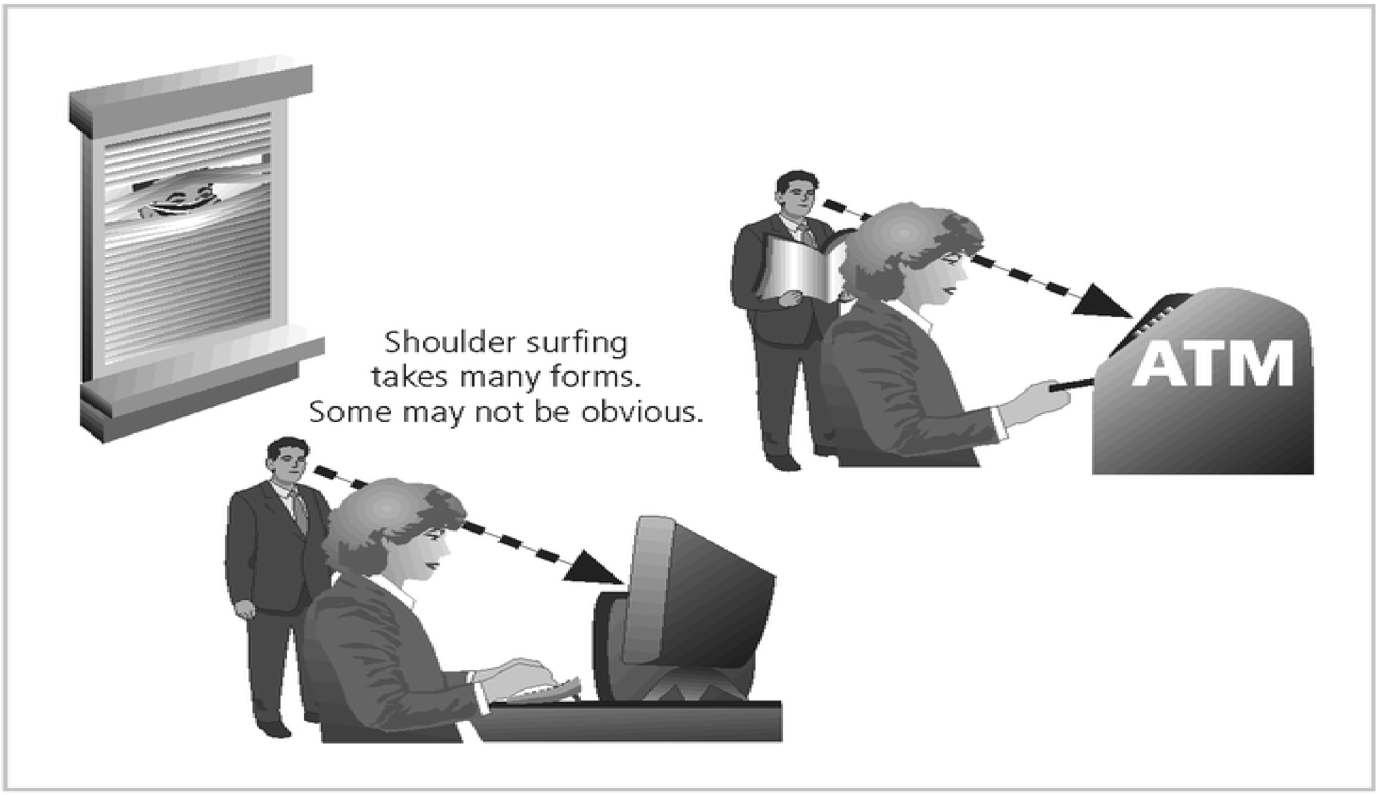
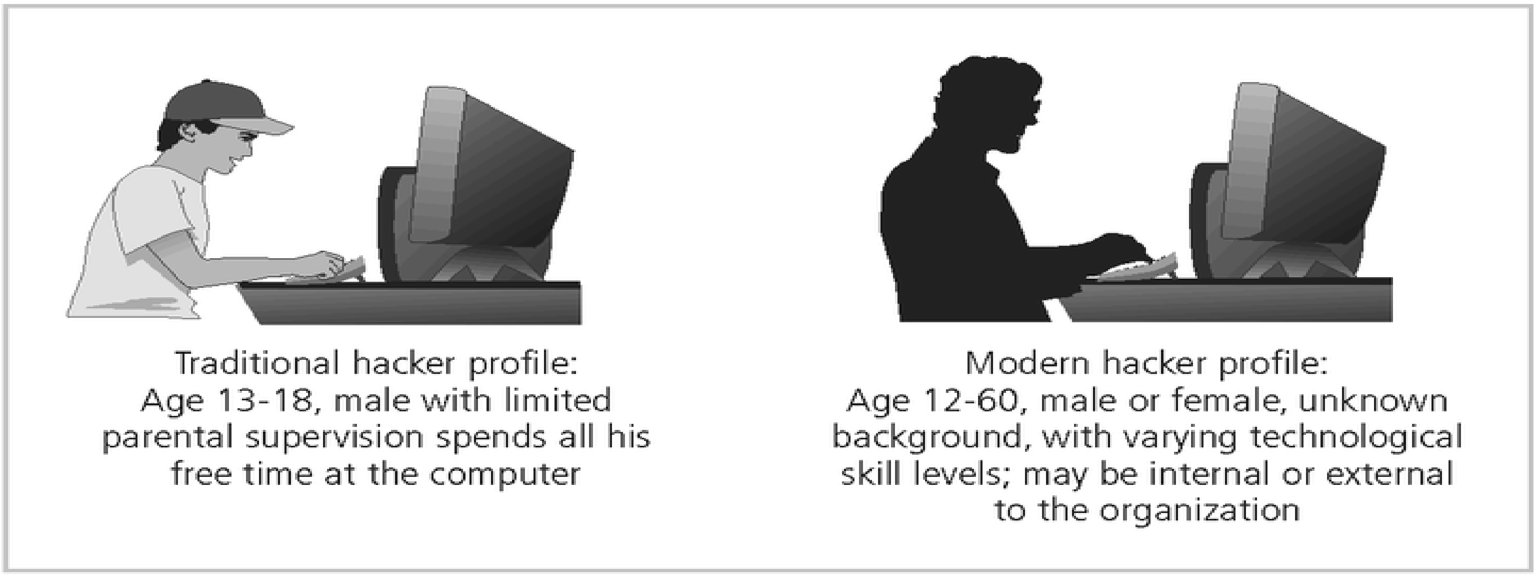


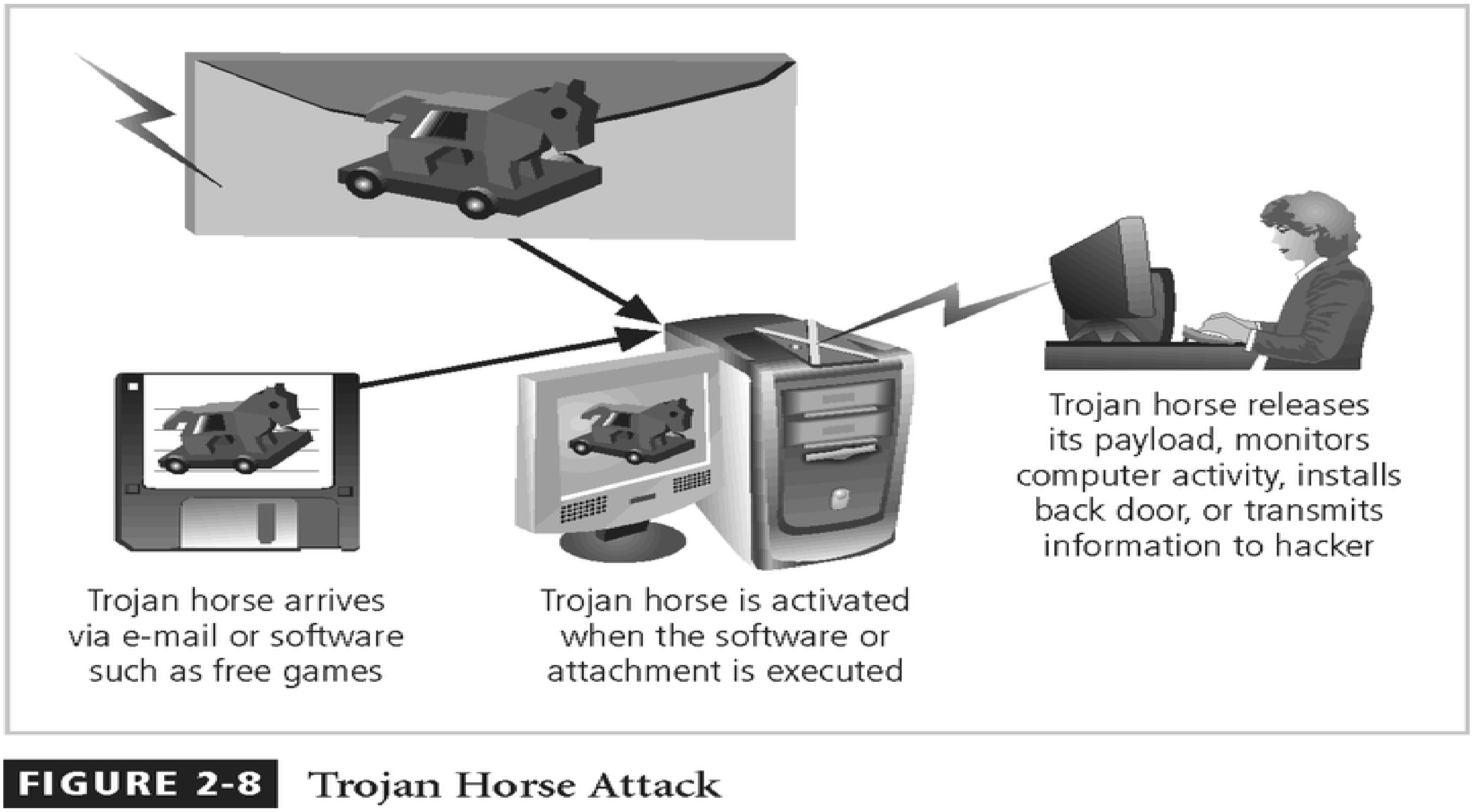
**FIGURE 2-2** Shoulder Surfing



Traditional hacker profile: Age 13-18, male with limited parental supervision spends all his free time at the computer

Modern hacker profile: Age 12-60, male or female, unknown background, with varying technological skill levels; may be internal or external to the organization

**FIGURE 2-3** Hacker Profiles



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

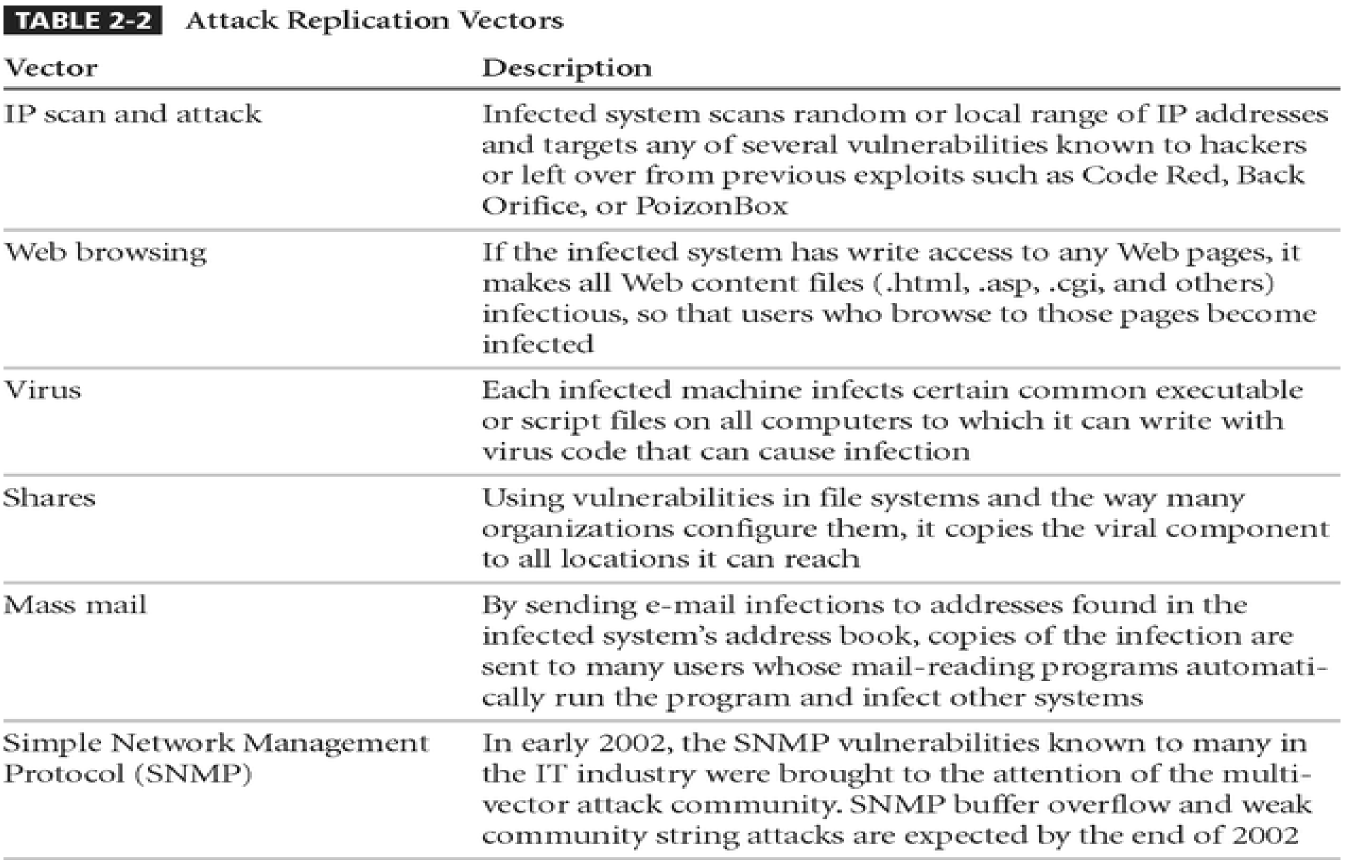


**TABLE 2-2** Attack Replication Vectors

| 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 multivector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of 2002 |

Slide 9 - Attack Descriptions
- Denial-of-Service (DoS): Overloads a system with requests, disrupting service.
- Distributed Denial-of-Service (DDoS): Coordinated attack from multiple locations.

Slide 11 - Attack Descriptions
- Spoofing: Pretends to be a trusted source.
- Man-in-the-Middle: Intercepts and modifies network traffic.

Slide 13 - Protective Measures
- Bolster Access Control: Strong passwords, regular resets, access control policies.
- Keep Software Updated: Regularly update antivirus, operating systems.

Slide 15 - Protective Measures
- Standardize Software: Use approved software, prevent unauthorized installations.
- Use Network Protection Measures: Firewall, IDS/IPS, network segmentation, VPN.

Slide 16 - Protective Measures
- Employee Training: Security awareness, threat identification.
- Schedule Backups: Regular backups to external drives or cloud.

Slide 17 - Acts of Human Error or Failure
- Include errors due to inexperience, improper training, incorrect assumptions.
- Employees are the greatest threats to information security.

Slide 19 - Compromises to Intellectual Property
- Intellectual property includes trade secrets, copyrights, trademarks, patents.

- Most common breaches involve software piracy.

Slide 21 - Espionage/Trespass
- Espionage includes unauthorized accessing of information.
- Shoulder surfing and hacking are methods of espionage.

Slide 24 - Espionage/Trespass
- Expert hackers and script kiddies are two skill levels among hackers.
- Hackers use skill, guile, or fraud to steal property or information.

Slide 26 - Information Extortion
- Information extortion involves stealing information and demanding compensation for its return or non-use.

Slide 27 - Sabotage or Vandalism
- Sabotage or vandalism aims to damage or destroy assets or reputation.
- Hacktivism and cyber-terrorism are extreme forms of sabotage.

Slide 29 - Deliberate Acts of Theft
- Illegal taking of another's property, including physical, electronic, or intellectual assets.
- Theft of data can result in its unauthorized use.

Slide 30 - Internet Service Issues
- Loss of internet service can affect an organization's availability.
- Outsourcing web servers transfers responsibility for internet service.

Slide 31 - Communications and Other Services
- Other utility services can impact information availability.
- Loss of these services can disrupt an organization's operations.

Slide 32 - Power Irregularities
- Voltage fluctuations can damage electronic equipment.
- Proper controls are needed to manage power quality.

Slide 34 - Deliberate Software Attacks
- Malicious code attacks include viruses, worms, Trojan horses, and spyware.
- Viruses attach themselves to executable files.
- Worms replicate and propagate without attaching to hosts.
- Trojan programs disguise themselves as useful software.

Slide 35 - Deliberate Software Attacks
- Backdoors and rootkits allow unauthorized access.
- Spyware and adware collect information or display advertisements.
- Protection involves educating users and updating antivirus software.

Slide 37 - Forces of Nature
- Forces of nature are unexpected and can disrupt information systems.
- Preparedness and contingency plans are essential to mitigate damage.

Slide 39 - Deviations in Quality of Service by Service Providers
- Service providers can impact information availability if services are not delivered as expected.
- Organizations must rely on multiple interdependent support systems.

Slide 41 - Technical Hardware Failures or Errors
- Hardware failures or errors can occur due to manufacturing flaws.
- Some errors are terminal, while others are intermittent.
- Software updates may resolve hardware issues.

Slide 43 - Technological Obsolescence
- Outdated technology can lead to unreliable systems.
- Proper planning and action are needed to prevent technology obsolescence.

Slide 46 - Malicious Code
- Malicious code attacks exploit vulnerabilities to damage or steal information.
- Attack vectors include IP scans, web browsing, viruses, and more.

Slide 51 - Attack Descriptions
- Buffer overflow is caused by sending more data to a buffer than it can handle.
- Attackers can use buffer overflows to execute unintended instructions.
- Protecting against buffer overflows is crucial.

Slide 54 - Attack Descriptions
- Sniffers monitor network data and can be used maliciously.
- Social engineering relies on manipulating individuals to gain access.
- Educating users about these threats is vital.

Slide 59 - Attack Descriptions
- Ping of Death attacks overwhelm systems by sending oversized packets.
- Timing attacks exploit browser cache contents.
- Awareness and

protection against these attacks are crucial.

These notes cover the key concepts from Vinod Sencha's presentation on security of information assets. Be sure to review and understand these topics thoroughly for your exam. Good luck!

---

**SUMMARY IN POINTS**

This presentation by Vinod Sencha discusses various aspects of information security and threats to IT systems. Here is a summary of the key points from each slide:

Slide 2 - Learning Objectives:
- The learning objectives of this presentation include understanding security threats to data, hardware, and users.
- Recognizing common types of hacking.
- Learning about protective measures for IT security.

Slide 3 - IT Security:
- IT security involves protecting computer systems and networks from information disclosure, theft, damage to hardware and software, as well as service disruption.
- IT security serves four key functions: protecting organizational function, enabling safe application operation, safeguarding data, and protecting technology assets.

Slide 4 - IT Security Features:
- IT security encompasses three core features: confidentiality (authorized access), integrity (authenticity and completeness of data), and availability (accessibility of systems and data).

Slide 5 - Vulnerabilities:
- Vulnerabilities are weaknesses that can be exploited, categorized into hardware, software, network, personnel, physical site, and organizational aspects.

Slide 6 - Threats:
- Threats are potential negative actions that exploit vulnerabilities, leading to unauthorized access, data disclosure, modification, or denial of service.
- Countermeasures are taken to protect against threats.

Slide 8 - Threats (Keywords):
- Various types of threats are introduced, including spam, cookies, web bugs, malware (viruses, worms, spyware, etc.), hacking, sniffing, social engineering, spoofing, DDoS attacks, cybercrime, and cyber-terrorism.

Slide 11 - Attack Descriptions:
- Attack descriptions include denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, spoofing, and man-in-the-middle attacks.

Slide 13 - Protective Measures:
- Measures to enhance IT security are discussed, such as bolstering access control, keeping software updated, standardizing software, using network protection measures, employee training, and scheduling backups.

Slide 17 - Acts of Human Error or Failure:
- Acts of human error or failure are highlighted, which can result from inexperience, improper training, incorrect assumptions, or other circumstances, making employees the greatest threat to information security.

Slide 19 - Compromises to Intellectual Property:
- Intellectual property breaches, including trade secrets, copyrights, trademarks, and patents, are mentioned, with software piracy being a common issue.

Slide 21 - Espionage/Trespass:
- Espionage and trespass involve unauthorized access to information, competitive intelligence, and security controls to mark organizational boundaries.

Slide 25 - Information Extortion:

- Information extortion involves stealing information and demanding compensation for its return or non-use.

Slide 27 - Sabotage or Vandalism:
- Sabotage or vandalism refers to deliberate acts aimed at disrupting operations, damaging assets, or harming an organization's image.

Slide 31 - Deliberate Software Attacks:
- Deliberate software attacks include viruses, worms, Trojan programs, and spyware, which can compromise systems and data.

Slide 38 - Protecting against Deliberate Software Attacks:
- Protecting against software attacks involves educating users, avoiding fear tactics, updating virus signatures, using firewalls, and securing passwords.

Slide 41 - Forces of Nature:
- Forces of nature, such as natural disasters, can disrupt information systems, requiring contingency plans and controls.

Slide 43 - Technical Hardware Failures or Errors:
- Technical hardware failures or errors can result from flaws in equipment, leading to unreliable service and the need for proper management.

Slide 45 - Technological Obsolescence:
- Technological obsolescence can lead to unreliable systems, necessitating proactive management and action.

Slide 47 - Attacks:
- Attacks are deliberate actions that exploit vulnerabilities, involving exploits, vulnerabilities, and compromises.

Slide 50 - Attack Descriptions:
- Further details on attack types, including IP scans, web browsing, and mail-bombing, are explained.

Slide 57 - Attack Descriptions:
- Social engineering, buffer overflow, and ping of death attacks are discussed as security threats.

Slide 59 - Attack Descriptions:
- Additional attack types, like sniffers, spam, and man-in-the-middle attacks, are described.

This presentation provides an extensive overview of information security, threats, and protective measures.

---

**DIAGRAMS - Refer PPT Diagrams also**
I've created text diagrams based on the information you provided. Each diagram represents a different slide from your content. Please note that text diagrams may not be as visually appealing as graphical diagrams but convey the information in a structured text format. Here they are:

Slide 2

```
By Vinod Sencha
Core Faculty(IS), RTI Jaipur
Security of Information
Assets

Learning Objectives
❖ Security threats to
   ❖ data
   ❖ hardware and
   ❖ users,
❖ common types of hacking,
❖ protective measures
```

Slide 3
```
IT Security

❖ IT security is the protection of computer systems and
  networks from information disclosure, theft of or damage to
  their hardware, software, or electronic data, as well as from the
  disruption or misdirection of the services they provide.
❖ IT security performs four important functions for an
  organization:
  - Protects the organization’s ability to function
  - Enables the safe operation of applications implemented on
    the organization’s IT systems
  - Protects the data the organization collects and uses
  - Safeguards the technology assets in use at the organization
```

Slide 4
```
IT Security: Features

Confidentiality:-
- Assurance that information is
  shared only among authorized
  persons or organizations.

Integrity:-
- Assurance that the information is authentic and complete.
- Maintaining and assuring the accuracy and consistency of
  data over its entire life-cycle.

Availability:-
```

- Assurance that the systems responsible for delivering, storing
  and processing information are accessible when needed, by
  those who need it.
```

Slide 5
```
Vulnerabilities

A vulnerability is a weakness which can be exploited by a threat actor, such
as an attacker, to cross privilege boundaries (i.e. perform unauthorized
actions) within a computer system. Vulnerabilities are classified according to the asset class they are related to:-

❖ Hardware: Susceptibility to humidity/dust; Unprotected storage; Over-heating.
❖ Software: Insufficient testing; insecure coding; lack of audit trail; Design flaw.
❖ Network: Unprotected communication lines; Insecure network architecture.
❖ Personnel: Inadequate recruiting process; Inadequate security awareness; insider threat.
❖ Physical site: Area subject to natural disasters (e.g. flood, earthquake); interruption to power source.
❖ Organizational: Lack of regular audits; lack of continuity plan.
```

Slide 6
```
Threats

A threat is a potential negative action or event facilitated by
a vulnerability that results in an unwanted impact to a
computer system or application. Any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. A countermeasure is any step you take to ward off a threat to protect user, data, or computer from harm.

Various Security threats:-
❖ Users: Identity Theft; Loss of Privacy; Exposure to Spam; Physical Injuries.
❖ Hardware: Power-related problems; theft; vandalism; and natural disasters.
❖ Data: Malwares; Hacking; Cybercrime; and Cyber-terror.
```

Slide 7
```
Threats to Information Security
```
```

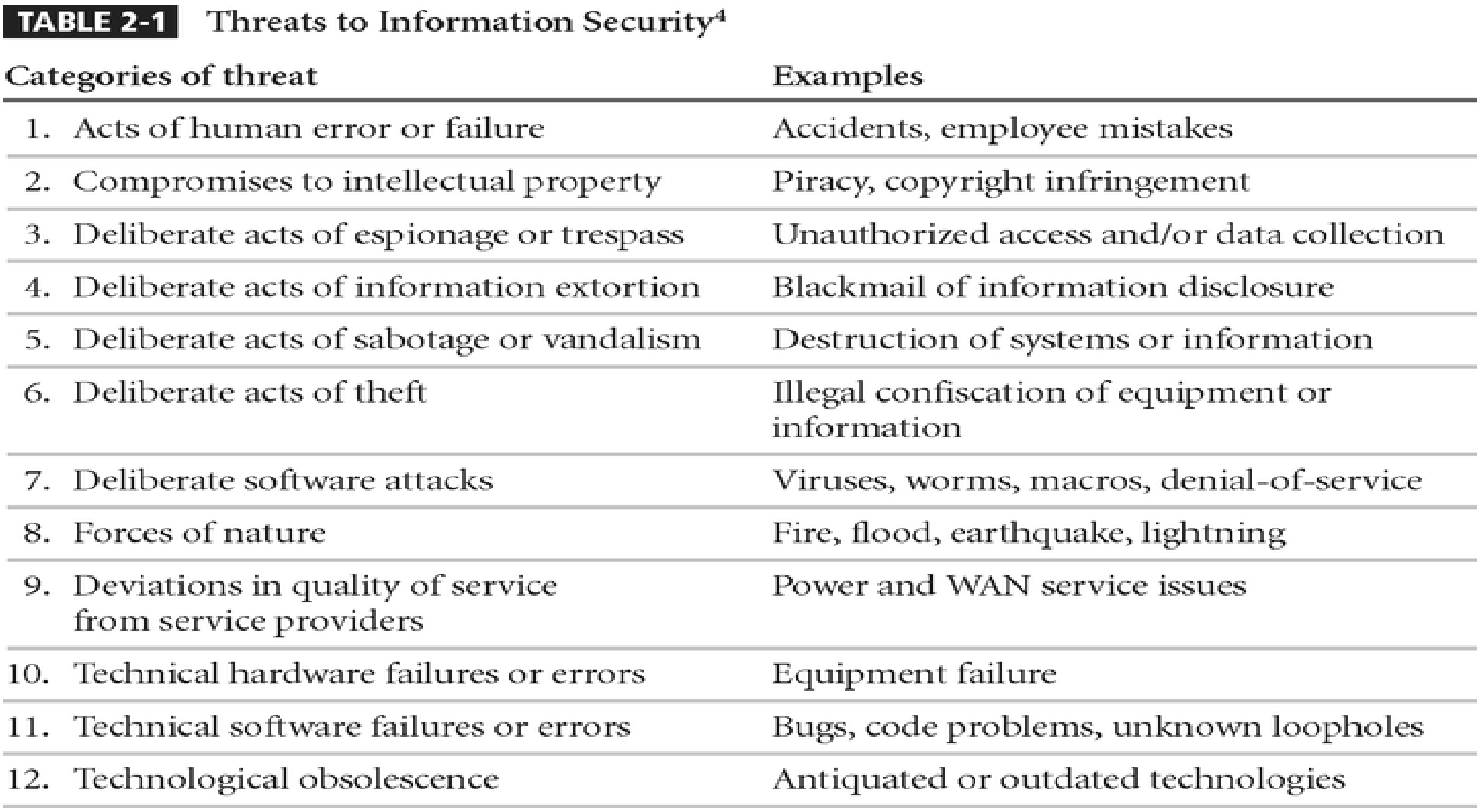


**TABLE 2-1** Threats to Information Security[4]

| 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 |

Slide 8

```
Threats(Keywords)

❖ Spam: Unsolicited commercial e-mail/Junk e-mail
❖ Cookie: Small text file that a Web server puts on a computer
❖ Web Bugs: A small gif embedded in a webpage/email
❖ Malwares: Malicious Software
❖ Virus (requires Some executables), Worms (Self-executables), Spyware, Trojan Horses, Botnet (Robot Network)
❖ Shoulder Surfing
❖ Hacking: Sniffing (finding user’s password - Password Sharing, Password Guessing, or Password Capture)
❖ Social Engineering: Dumpster Diving, Phishing (Email) & Vishing (Phone Calls)
❖ Spoofing
❖ DDoS: Distributed Denial of Services.
❖ Cybercrime; and Cyber-terrorism.
```

Slide 9

```
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

These text diagrams represent the content you provided in a structured format. You can use these as reference points or incorporate them into your presentation as needed.

Creating text diagrams based on the information you provided:

Slide 2: Learning Objectives
```
Security threats to:
  - Data
  - Hardware
  - Users
Common types of hacking
Protective measures
```

Slide 3: IT Security
```
IT security is the protection of:
  - Computer systems
  - Networks
from:
  - Information disclosure
  - Theft of or damage to hardware, software, or electronic data
  - Disruption or misdirection of services.
IT security functions:
  - Protects the organization's ability to function
  - Enables safe operation of applications
  - Protects data collected and used
  - Safeguards technology assets in use.
```

Slide 4: IT Security: Features
```
Confidentiality:
  - Assurance that information is shared only among authorized persons or organizations.
Integrity:
  - Assurance that information is authentic and complete.
Availability:
```

  - Assurance that systems responsible for delivering, storing, and processing information are accessible when needed.
```

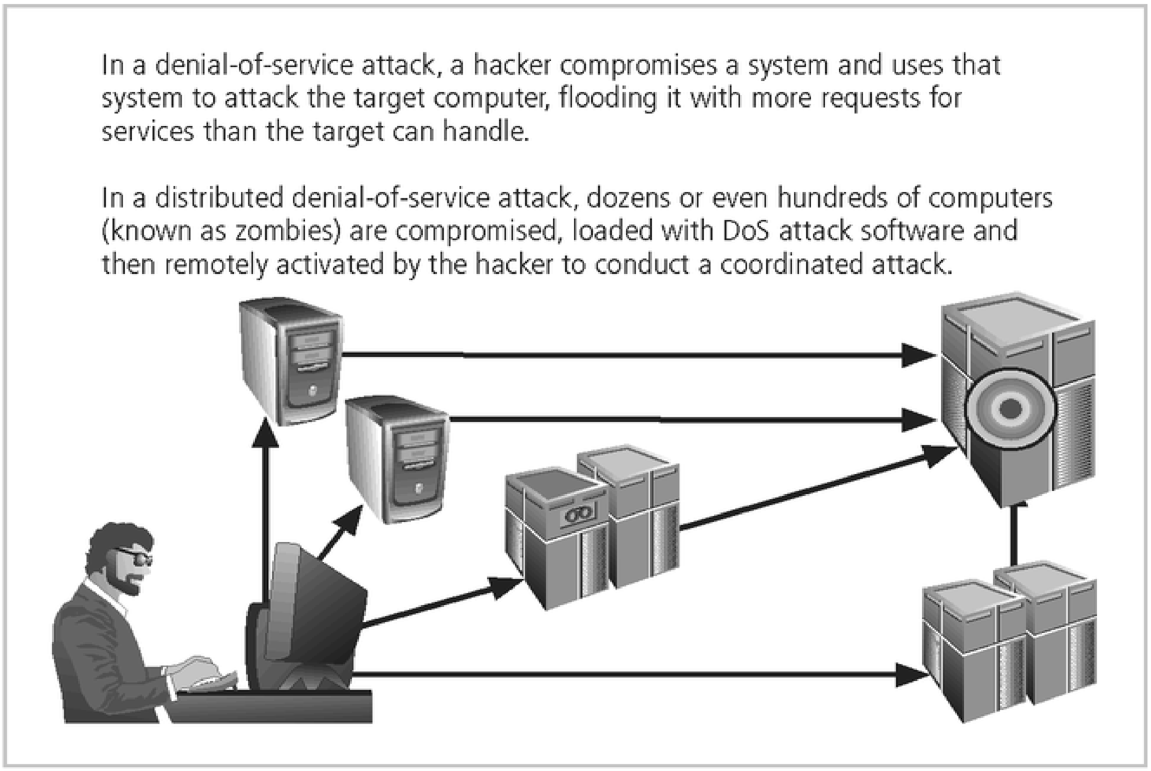
Slide 5: Vulnerabilities
```
Vulnerability is a weakness exploitable by a threat actor, classified by asset class:
Hardware:
  - Susceptibility to humidity/dust
  - Unprotected storage
  - Overheating.
Software:
  - Insufficient testing
  - Insecure coding
  - Lack of audit trail
  - Design flaw.
Network:
  - Unprotected communication lines
  - Insecure network architecture.
Personnel:
  - Inadequate recruiting process
  - Inadequate security awareness
  - Insider threat
Physical site:
  - Area subject to natural disasters
  - Interruption to power source.
Organizational:
  - Lack of regular audits
  - Lack of continuity plan.
```

Slide 6: Threats
```
Threat is a potential negative action facilitated by a vulnerability, resulting in unwanted impact on a computer system or application.
Various security threats:
Users:
  - Identity Theft
  - Loss of Privacy
  - Exposure to Spam
  - Physical Injuries.
Hardware:
  - Power-related problems
  - Theft
  - Vandalism
  - Natural disasters.
Data:

  - Malwares
  - Hacking
  - Cybercrime
  - Cyber-terror.
```

Slide 7: Threats to Information Security

Slide 8: Threats (Keywords)
```
Spam: Unsolicited commercial e-mail/Junk e-mail
Cookie: Small text file that a Web server puts on a computer
Web Bugs: A small gif embedded in a webpage/email
Malwares: Malicious Software
Virus, Worms, Spyware, Trojan Horses, Botnet (Robot Network)
Shoulder Surfing
Hacking, Sniffing, Social Engineering, Spoofing
DDoS: Distributed Denial of Services
Cybercrime and Cyber-terrorism.
```



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

Slide 9: Attack Descriptions
```
Denial-of-service (DoS): Attacker sends numerous connection or information requests to overload the target.
Distributed Denial-of-service (DDoS): Coordinated attack from multiple locations.

Slide 11: Attack Descriptions
```
```

Spoofing: Intruder sends messages with a trusted host's IP address.
Man-in-the-Middle: Attacker intercepts, modifies, and reinserts network packets.
```
Slide 14: Protective Measures
```
1. Bolster Access Control:
   - Strong password system
   - Reset all default passwords
   - Create a strong access control policy.
2. Keep All Software Updated:
   - Update anti-virus software and operating systems
   - Use automatic software updates.
```

Slide 15: Protective Measures
```
3. Standardize Software:
   - Standardize operating system, browser, media player, plug-ins.
   - Prevent unauthorized software installation.
4. Use Network Protection Measures:
   - Install a firewall
   - Ensure proper access controls
   - Use IDS/IPS
   - Implement network segmentation
   - Use a VPN.
```

Slide 16: Protective Measures
```
5. Employee Training:
   - Ensure employees understand network security.
   - Teach them to identify threats.
   - Educate on how to report and prevent security breaches.
6. Schedule Backups:
   - Regularly backup data to external hard drives or the cloud.
   - Consider incremental backups.
```
Create your own diagrams or from ppt

---

**SIMULATED QA**

Q1: What are the learning objectives mentioned in Vinod Sencha's presentation on IT security?
A1: The learning objectives mentioned in the presentation are:
- Security threats to data, hardware, and users.
- Common types of hacking.
- Protective measures for information security.

Q2: What are the four important functions of IT security for an organization as outlined in the presentation?
```

A2: The four important functions of IT security for an organization, as outlined in the presentation, are:
1. Protecting the organization's ability to function.
2. Enabling the safe operation of applications implemented on the organization's IT systems.
3. Protecting the data that the organization collects and uses.
4. Safeguarding the technology assets in use at the organization.

Q3: How are vulnerabilities classified in the presentation, and what are some examples of each type?
A3: Vulnerabilities are classified according to the asset class they are related to in the presentation:
- Hardware vulnerabilities: Examples include susceptibility to humidity/dust, unprotected storage, and over-heating.
- Software vulnerabilities: Examples include insufficient testing, insecure coding, lack of audit trail, and design flaws.
- Network vulnerabilities: Examples include unprotected communication lines and insecure network architecture.
- Personnel vulnerabilities: Examples include inadequate recruiting processes, inadequate security awareness, and insider threats.
- Physical site vulnerabilities: Examples include areas subject to natural disasters (e.g., flood, earthquake) and interruption to the power source.
- Organizational vulnerabilities: Examples include the lack of regular audits and a continuity plan.

Q4: What are some of the common types of security threats mentioned in the presentation?
A4: Some common types of security threats mentioned in the presentation include:
- Users: Identity theft, loss of privacy, exposure to spam, and physical injuries.
- Hardware: Power-related problems, theft, vandalism, and natural disasters.
- Data: Malware, hacking, cybercrime, and cyber-terrorism.

Q5: Can you list some keywords associated with security threats from the presentation?
A5: Keywords associated with security threats from the presentation include:
- Spam
- Cookie
- Web Bugs
- Malware (Virus, Worms, Spyware, Trojan Horses, Botnet)
- Shoulder Surfing
- Hacking
- Sniffing
- Social Engineering
- Spoofing
- DDoS (Distributed Denial of Service)
- Cybercrime
- Cyber-terrorism

Q6: What are the protective measures mentioned in the presentation for enhancing information security?
A6: Protective measures mentioned in the presentation for enhancing information security include:
1. Bolstering access control with strong passwords and regular resets.
2. Keeping all software updated, including antivirus software and operating systems.
3. Standardizing software to prevent unauthorized installations.
4. Using network protection measures like firewalls, IDS/IPS, network segmentation, and VPNs.

5. Providing employee training to increase security awareness.
6. Scheduling backups to ensure data recovery.
7. Addressing acts of human error or failure through proper training and controls.
8. Protecting intellectual property through security measures and copyright enforcement.
9. Guarding against espionage, trespass, and information extortion.
10. Preparing for forces of nature and other physical threats.
11. Ensuring quality of service by service providers.
12. Mitigating power irregularities.
13. Defending against deliberate software attacks, malware, and spyware.
14. Educating users and avoiding fear tactics.
15. Handling technological obsolescence.
16. Dealing with technical hardware failures or errors.
17. Protecting against deviations in the quality of service.
18. Addressing attacks, including malicious code, buffer overflows, and timing attacks.

Q7: What are some examples of deliberate software attacks discussed in the presentation?
A7: Examples of deliberate software attacks discussed in the presentation include:
- Viruses
- Worms
- Trojan Horses
- Logic bombs
- Backdoors or trap doors
- Denial-of-service (DoS) and Distributed Denial-of-Service (DDoS) attacks
- Spoofing
- Man-in-the-Middle attacks
- Spam
- Sniffers
- Social Engineering
- Buffer Overflow attacks
- Ping of Death Attacks
- Timing Attacks

Q8: What are some recommended protective measures against deliberate software attacks?
A8: Some recommended protective measures against deliberate software attacks mentioned in the presentation include:
- Educating users about security awareness.
- Updating virus signature files and using antivirus software.
- Implementing firewalls and intrusion detection systems.
- Standardizing software to prevent unauthorized installations.
- Protecting against email-based attacks like spam and phishing.
- Implementing strong access controls and password policies.
- Guarding against buffer overflows and code vulnerabilities.
- Avoiding fear tactics when educating users.

Q9: How does the presentation emphasize the importance of user education and awareness in information security?

A9: The presentation emphasizes the importance of user education and awareness in information security by stating that "people are the weakest link" and highlighting the significance of training users to identify threats. It encourages educating employees about network security, helping them understand the risks, and ensuring they can recognize potential security threats.

Q10: What are some threats related to forces of nature that the presentation mentions?
A10: Threats related to forces of nature mentioned in the presentation include:
- Fire
- Flood
- Earthquake
- Lightning
- Volcanic eruption
- Insect infestation
These forces of nature can disrupt the availability of information and systems and are considered dangerous due to their unexpected and unpredictable nature.

---

**QA for 8 marks**
Here are questions and answers based on the provided content:

Q1: What are the learning objectives related to IT security mentioned in the slides?

A1: The learning objectives related to IT security mentioned in the slides are:
- Security threats to data, hardware, and users.
- Common types of hacking.
- Protective measures.

Q2: Define IT security and its functions for an organization.

A2: IT security, also known as Information Technology security, is the protection of computer systems and networks from various threats, including information disclosure, theft, damage to hardware or software, and disruptions to services. It performs four critical functions for an organization:
1. Protects the organization's ability to function.
2. Enables the safe operation of applications on IT systems.
3. Protects the data collected and used by the organization.
4. Safeguards the technology assets in use at the organization.

Q3: What are the three key aspects of IT security mentioned in the content?

A3: The three key aspects of IT security mentioned in the content are:
1. Confidentiality: Ensuring that information is shared only among authorized persons or organizations.
2. Integrity: Assuring that the information is authentic and complete, maintaining accuracy and consistency throughout its life-cycle.
3. Availability: Assuring that the systems responsible for delivering, storing, and processing information are accessible when needed by those who need it.

Q4: How are vulnerabilities classified, and what are some examples of these vulnerabilities?

A4: Vulnerabilities are classified according to the asset class they are related to. Examples of these vulnerabilities include:
- Hardware vulnerabilities: Susceptibility to humidity, dust, overheating, etc.
- Software vulnerabilities: Insufficient testing, insecure coding, lack of audit trails, design flaws.
- Network vulnerabilities: Unprotected communication lines, insecure network architecture.
- Personnel vulnerabilities: Inadequate recruiting process, inadequate security awareness, insider threats.
- Physical site vulnerabilities: Exposure to natural disasters, interruption to power source.
- Organizational vulnerabilities: Lack of regular audits, lack of continuity planning.

Q5: Define the term "threat" in the context of information security and give some examples of security threats.

A5: In the context of information security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact on a computer system or application. Examples of security threats include:
- Users: Identity theft, loss of privacy, exposure to spam, physical injuries.
- Hardware: Power-related problems, theft, vandalism, natural disasters.
- Data: Malware, hacking, cybercrime, cyber-terror.

Q6: Provide some keywords associated with common security threats mentioned in the content.

A6: Some keywords associated with common security threats mentioned in the content include:
- Spam
- Cookie
- Web Bugs
- Malwares (Malicious Software)
- Virus
- Worms
- Spyware
- Trojan Horses
- Botnet (Robot Network)
- Hacking
- Sniffing
- Social Engineering
- Spoofing
- DDoS (Distributed Denial of Service)
- Cybercrime
- Cyber-terrorism

Q7: What are the characteristics and potential impact of a Denial-of-Service (DoS) attack?

A7: A Denial-of-Service (DoS) attack involves an attacker sending a large number of connection or information requests to a target system. The characteristics and potential impact of a DoS attack include:
- Overwhelming the target system with excessive requests.
- Disrupting the system's normal functioning.
- Potentially causing a system crash or rendering it unable to perform ordinary functions.
- Impacting the availability of services, leading to downtime.

Q8: Explain the concept of "spoofing" and "man-in-the-middle" attacks.

A8:
- Spoofing: Spoofing is a technique used by attackers to gain unauthorized access. In spoofing, the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. This can deceive the target into believing that the message is legitimate.

- Man-in-the-Middle: In a man-in-the-middle attack, an attacker intercepts and sniffs packets from the network. They then modify these packets and insert them back into the network. This allows the attacker to eavesdrop on communications between two parties without their knowledge.

Q9: What are some protective measures mentioned in the content to enhance IT security?

A9: Some protective measures mentioned in the content to enhance IT security include:
1. Bolstering access control with strong password systems.
2. Keeping all software updated to patch security vulnerabilities.
3. Standardizing software to control installations.
4. Using network protection measures such as firewalls, IDS/IPS, and VPNs.
5. Providing employee training to improve security awareness.
6. Scheduling regular data backups.
7. Implementing controls to prevent human errors and failures.
8. Protecting intellectual property through various means.
9. Preparing for forces of nature and other unexpected events.
10. Guarding against technical hardware failures or errors.
11. Addressing technological obsolescence.
12. Defending against attacks, such as malicious code, by educating users and implementing security measures.

Q10: What is the significance of educating users in the context of IT security?

A10: Educating users is significant in IT security because:
- Users are often the weakest link in an organization's security.
- They may inadvertently engage in actions that compromise security.
- Educated users are more likely to identify and report security threats.
- They can make informed decisions and recognize social engineering attempts.
- Security awareness programs can help create a culture of security within an organization.

Q11: How can organizations protect against deliberate software attacks, such as viruses and worms?

A11: Organizations can protect against deliberate software attacks like viruses and worms by:
1. Educating users about the risks and best practices.
2. Regularly updating antivirus software and virus signature files.
3. Using firewalls to filter incoming and outgoing traffic.
4. Avoiding downloading or opening files from untrusted sources.
5. Monitoring network traffic for suspicious activities.
6. Employing intrusion detection systems.

7. Applying patches and security updates promptly.
8. Implementing strong access controls and authentication mechanisms.
9. Conducting security audits and vulnerability assessments.

Q12: What are some examples of acts of human error or failure mentioned in the content?

A12: Examples of acts of human error or failure mentioned in the content include:
- Acts done without malicious intent, often caused by inexperience, improper training, incorrect assumptions, or other circumstances.
- Mistakes that can lead to the revelation of classified data, entry of erroneous data, accidental data deletion, storage of data in unprotected areas, or failure to protect information.
- Instances where employees, who are often the closest to organizational data, unintentionally compromise security.

Q13: How can organizations protect their intellectual property, and what are some forms of intellectual property mentioned?

A13: Organizations can protect their intellectual property by implementing security measures and controls. Forms of intellectual property mentioned in the content include:
- Trade secrets
- Copyrights
- Trademarks
- Patents

Protection measures may involve safeguarding proprietary information, implementing access controls, and legal actions against intellectual property theft, such as software piracy.

Q14:

What are some examples of attacks related to espionage or trespass in information security?

A14: Examples of attacks related to espionage or trespass in information security include:
- Unauthorized accessing of information.
- Competitive intelligence gathering.
- Shoulder surfing to view confidential information.
- Hackers using skill, guile, or fraud to steal property.
- Insider threats.
- Cyber-activist operations and cyber-terrorism.

Q15: How do attacks related to information extortion work, and what is the goal of these attacks?

A15: Attacks related to information extortion involve an attacker or a formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use. The goal of these attacks is to obtain financial gain or other concessions from the victim organization by exploiting their need for the stolen information's return or protection from misuse.

Q16: What is the difference between a Denial-of-Service (DoS) attack and a Distributed Denial-of-Service (DDoS) attack?

A16: The difference between a Denial-of-Service (DoS) attack and a Distributed Denial-of-Service (DDoS) attack is as follows:
- DoS Attack: In a DoS attack, a single attacker sends a large number of connection or information requests to a target system, overwhelming it. This can result in system crashes or an inability to perform ordinary functions.

- DDoS Attack: A DDoS attack involves a coordinated stream of requests launched against a target from multiple locations simultaneously. DDoS attacks are more powerful and harder to mitigate than simple DoS attacks because they come from various sources, making it challenging to block all incoming traffic.

Q17: What are some potential consequences of acts of theft, such as illegal taking of another's property, in information security?

A17: Some potential consequences of acts of theft in information security, such as the illegal taking of another's property, include:
- Loss of data integrity and confidentiality.
- Unauthorized access to sensitive information.
- Financial losses due to theft of assets.
- Reputational damage to the organization.
- Legal and regulatory repercussions.
- Impact on the organization's ability to function.

Q18: How can organizations protect against technical hardware failures or errors?

A18: Organizations can protect against technical hardware failures or errors by:
1. Regularly monitoring and maintaining hardware components.
2. Performing routine hardware inspections and testing.
3. Implementing redundancy and backup systems.
4. Conducting hardware diagnostics to identify potential issues.
5. Ensuring timely updates and patches for hardware drivers.
6. Training staff to recognize and report hardware issues.
7. Maintaining an inventory of hardware components for replacement.
8. Implementing hardware security measures to prevent physical tampering or theft.

Q19: What is the significance of planning for technological obsolescence in IT security?

A19: Planning for technological obsolescence is significant in IT security because:
- Outdated technology can become vulnerable to security threats and attacks.
- Organizations relying on obsolete systems risk losing data integrity and availability.
- Upgrading or replacing obsolete technology can be costly and disruptive.
- Proactive planning helps ensure that technology remains secure and functional over time.

Q20: What are some examples of attacks related to malicious code mentioned in the content?

A20: Examples of attacks related to malicious code mentioned in the content include:
- Viruses that attach themselves to executable files.
- Worms that replicate and propagate without host attachment.
- Trojan horses that disguise themselves as useful software but contain malicious elements.
- Spyware that secretly collects and transmits user information.
- Attacks exploiting vulnerabilities through buffer overflow, timing attacks, and more.

These attacks aim to compromise system security and steal or manipulate data.

Certainly! Here are some questions and answers related to the information provided:

Question 1: What are the key learning objectives regarding information security discussed in the presentation?

Answer 1: The key learning objectives regarding information security discussed in the presentation are:
- Understanding security threats to data, hardware, and users.
- Recognizing common types of hacking.
- Learning about protective measures to safeguard information assets.

Question 2: Define IT security and list the four important functions it performs for an organization.

Answer 2: IT security is the protection of computer systems and networks from information disclosure, theft, damage to hardware or software, and disruption of services. IT security performs four important functions for an organization:
1. Protects the organization's ability to function.
2. Enables the safe operation of applications on IT systems.
3. Protects the data collected and used by the organization.
4. Safeguards the technology assets in use by the organization.

Question 3: What are the three key features of IT security as discussed in the presentation?

Answer 3: The three key features of IT security are:
1. Confidentiality: Ensures that information is shared only among authorized individuals or organizations.
2. Integrity: Ensures that information is authentic and complete, maintaining accuracy and consistency throughout its life-cycle.
3. Availability: Assures that systems responsible for delivering, storing, and processing information are accessible when needed by authorized users.

Question 4: What is a vulnerability, and how are vulnerabilities classified in the presentation?

Answer 4: A vulnerability is a weakness that can be exploited by a threat actor to perform unauthorized actions within a computer system. Vulnerabilities are classified in the presentation based on the asset class they are related to, including hardware, software, network, personnel, physical site, and organizational vulnerabilities.

Question 5: Explain the concept of threats in information security and provide examples of various security threats mentioned in the presentation.

Answer 5: Threats in information security are potential negative actions or events facilitated by vulnerabilities that result in unwanted impacts on computer systems or applications. Various security threats mentioned in the presentation include:
- Users threats: Identity theft, loss of privacy, exposure to spam, physical injuries.
- Hardware threats: Power-related problems, theft, vandalism, natural disasters.
- Data threats: Malwares, hacking, cybercrime, and cyber-terrorism.

Question 6: Define and differentiate between Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.

Answer 6: Denial-of-Service (DoS) attack is when an attacker sends a large number of connection or information requests to a target, overwhelming the target system, and potentially causing it to crash or become unavailable.

Distributed Denial-of-Service (DDoS) attack is an advanced form of DoS attack in which a coordinated stream of requests is launched against a target from many locations simultaneously, making it even more challenging to mitigate.

Question 7: What are some protective measures discussed in the presentation to enhance information security?

Answer 7: Some protective measures discussed in the presentation to enhance information security include:
1. Bolstering access control with strong password systems.
2. Keeping all software updated to address vulnerabilities.
3. Standardizing software to prevent unauthorized installations.
4. Using network protection measures such as firewalls, IDS/IPS, and VPNs.
5. Providing employee training to improve security awareness.
6. Implementing regular backups to safeguard data.
7. Addressing acts of human error or failure through controls.

Question 8: What is the significance of educating users in the context of information security, and how can organizations avoid fear tactics when educating users?

Answer 8: Educating users is significant in improving information security because users can be the weakest link in the security chain. Organizations should provide security awareness programs and training to ensure that employees understand network security, can identify threats, and know how to respond. It's essential to avoid fear tactics and instead focus on promoting awareness and building on the knowledge users already have to create a positive and effective security culture.

---

**FLASHCARDS/KEY TERMS**

Card 1
Title: Security of Information Assets

Author: Vinod Sencha, Core Faculty (IS) at RTI Jaipur

---

Card 2
Title: Learning Objectives

- Security threats to:
  - Data
  - Hardware
  - Users
- Common types of hacking
- Protective measures

---

Card 3
Title: IT Security

- Definition: Protection of computer systems and networks from information disclosure, theft, damage to hardware, software, and electronic data, and service disruption.
- Four important functions:
  1. Protects the organization's ability to function.
  2. Enables safe operation of applications on IT systems.
  3. Protects collected data.
  4. Safeguards technology assets.

---

Card 4
Title: IT Security: Features

- Confidentiality: Ensures information is shared only among authorized individuals or organizations.
- Integrity: Ensures information is authentic and complete throughout its life-cycle.
- Availability: Ensures systems responsible for information delivery, storage, and processing are accessible when needed by authorized users.

---

Card 5
Title: Vulnerabilities

- Definition: Weaknesses exploitable by threat actors to perform unauthorized actions within a computer system.
- Classified by asset class:
  - Hardware vulnerabilities (e.g., overheating).
  - Software vulnerabilities (e.g., insecure coding).
  - Network vulnerabilities (e.g., insecure network architecture).
  - Personnel vulnerabilities (e.g., inadequate security awareness).

  - Physical site vulnerabilities (e.g., natural disasters).
  - Organizational vulnerabilities (e.g., lack of audits).

---

Card 6
Title: Threats

- Definition: Potential negative actions or events facilitated by vulnerabilities, resulting in unwanted impacts on computer systems or applications.
- Examples: Unauthorized access, destruction, disclosure, modification of data, and denial of service.
- Countermeasures: Steps taken to protect users, data, or computers from harm.

---

Card 7
Title: Threats to Information Security

---

Card 8
Title: Threats (Keywords)

- Spam
- Cookie
- Web Bugs
- Malwares (Viruses, Worms, Spyware, Trojan Horses, Botnet)
- Shoulder Surfing
- Hacking (Sniffing, Social Engineering, Spoofing)
- DDoS (Distributed Denial of Service)
- Cybercrime and Cyber-terrorism

---

Card 9
Title: Attack Descriptions

- Denial-of-service (DoS)
- Distributed Denial-of-service (DDoS)
- Spoofing
- Man-in-the-Middle
- IP Scan and Attack
- Web Browsing
- Virus
- Unprotected Shares
- Mass Mail
- Sniffers

- Social Engineering
- Buffer Overflow
- Ping of Death Attacks
- Timing Attack

---

Card 10
Title: Protective Measures

1. Bolster Access Control
2. Keep All Software Updated
3. Standardize Software
4. Use Network Protection Measures (Firewall, IDS/IPS, VPN)
5. Employee Training
6. Schedule Backups

---

Card 11
Title: Acts of Human Error or Failure

- Includes acts done without malicious intent.
- Caused by inexperience, improper training, incorrect assumptions, or other circumstances.
- Employees are often the greatest threats to information security due to their proximity to organizational data.

---

Card 12
Title: Compromises to Intellectual Property

- Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- Most common IP breaches involve software piracy.
- Organizations rely on their intellectual property, making it a valuable target.

---

Card 13
Title: Espionage/Trespass

- Broad category of activities that breach confidentiality.
- Unauthorized access to information.
- Different from competitive intelligence vs. espionage.
- Includes shoulder surfing and hacking.
- Rising threat of hacktivism and cyber-terrorism.

---

Card 14

Title: Information Extortion

- Definition: Stealing information and demanding compensation for its return or non-use.
- Often seen in credit card number theft and ransomware attacks.

---

Card 15

Title: Sabotage or Vandalism

- Deliberate acts to sabotage or vandalize computer systems or business operations.
- Can range from petty vandalism to organized sabotage.
- Web defacement can harm an organization's image.

---

Card 16

Title: Deliberate Acts of Theft

- Illegal taking of another's property, whether physical, electronic, or intellectual.
- Electronic theft can be challenging to detect and prevent.

---

Card 17

Title: Internet Service Issues

- Loss of internet service can severely impact information availability.
- Outsourcing web servers can transfer responsibility for internet service to external providers.

---

Card 18

Title: Communications and Other Services

- Other utility services can affect information availability.
- Services like telephone, water, trash pickup, etc., are crucial for business continuity.

---

Card 19

Title: Power Irregularities

- Voltage irregularities can lead to equipment damage and data loss.

- Types of irregularities: spike, surge, sag, brownout, fault, blackout.
- Proper power quality management is essential.

---

Card 20
Title: Deliberate Software Attacks

- Malicious code execution with the intent to damage or steal information.
- Includes viruses, worms, Trojan horses, and more.
- Can lead to system compromise and data loss.

---

Card 21
Title: Technical Hardware Failures or Errors

- Flaws in hardware distributed by manufacturers.
- Can cause system instability, unreliability, or loss of equipment.
- Errors can be terminal or intermittent.

---

Card 22
Title: Technological Obsolescence

- Outdated infrastructure can lead to unreliable systems.
- Management must recognize and address technology obsolescence to avoid risks.

---

Card 23
Title: Attacks (Summary)

- Attacks exploit vulnerabilities to compromise systems.
- Exploits are techniques used to compromise systems.
- Vulnerabilities are weaknesses in controlled systems.

---

Card 24
Title: Malicious Code

- Malicious code attacks involve viruses, worms, Trojan horses, and active web scripts.
- These attacks intend to destroy or steal information.

---

Card 25
Title: Attack Descriptions (Continued)

- IP Scan and Attack
- Web Browsing
- Virus
- Unprotected Shares
- Mass Mail
- Sniffers
- Social Engineering
- Buffer Overflow
- Ping of Death Attacks
- Timing Attack

---

Card 26
Title: Attack Descriptions (Continued)

- Denial-of-service (DoS)
- Distributed Denial-of-service (DDoS)
- Spoofing
- Man-in-the-Middle
- Spam
- Mail-bombing

---

Card 27
Title: Protective Measures (Summary)

- Access Control
- Software Updates
- Standardizing Software
- Network Protection Measures
- Employee Training
- Scheduled Backups

---

Card 28
Title: Acts of Human Error or Failure

- Often result from inexperience, improper training, or incorrect assumptions.
- Employees can be the weakest link in information security.
- Examples include revelation of classified

data and accidental data deletion.

---

Card 29
Title: Compromises to Intellectual Property

- Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- Software piracy is a common IP breach.
- Protecting intellectual property is crucial for many organizations.

---

Card 30
Title: Espionage/Trespass

- Espionage includes unauthorized access to confidential information.
- Different from competitive intelligence.
- Examples include shoulder surfing and hacking.
- Hacktivism and cyber-terrorism are rising threats.

---

Card 31
Title: Information Extortion

- Information extortion involves stealing data and demanding compensation for its return or non-use.
- Common in cases of ransomware and credit card data theft.

---

Card 32
Title: Sabotage or Vandalism

- Deliberate acts to sabotage or vandalize computer systems or business operations.
- Can harm an organization's image.
- Ranges from petty vandalism to cyber-terrorism.

---

Card 33
Title: Deliberate Acts of Theft

- Illegal taking of another's property, whether physical, electronic, or intellectual.
- Electronic theft poses unique challenges.
- Theft can result in the loss of valuable information.

---

Card 34
Title: Internet Service Issues

- Loss of internet service can disrupt business operations.
- Outsourcing web servers can transfer responsibility for internet service to external providers.

---

Card 35
Title: Communications and Other Services

- Various utility services, including telephone, water, trash pickup, etc., can impact business continuity.
- Service disruptions can affect the availability of information.

---

Card 36
Title: Power Irregularities

- Voltage irregularities like spikes, surges, sags, and brownouts can harm electronic equipment.
- Effective power quality management is crucial to prevent damage.

---

Card 37
Title: Deliberate Software Attacks

- Malicious code execution with the intent to damage or steal information.
- Includes viruses, worms, Trojan horses, and more.
- Can lead to system compromise and data loss.

---

Card 38
Title: Protective Measures

- Access Control
- Software Updates
- Standardizing Software
- Network Protection Measures
- Employee Training
- Scheduled Backups

---

Card 39
Title: Forces of Nature

- Natural disasters and unforeseen events that can disrupt lives and information systems.
- Examples include fire, flood, earthquake, and insect infestations.
- Preparation and contingency planning are essential.

---

Card 40
Title: Deviations in Quality of Service by Service Providers

- Situations where products or services aren't delivered as expected.
- Dependence on inter-dependent support systems.
- Issues related to internet service, communications, and power irregularities.

---

Card 41
Title: Technical Hardware Failures or Errors

- Failures or errors resulting from equipment flaws.
- Can lead to system instability or unreliability.
- Errors can be terminal or intermittent.

---

Card 42
Title: Technological Obsolescence

- Outdated technology can lead to unreliable systems.
- Management must address technology obsolescence to avoid risks.

---

Card 43
Title: Attacks

- Attacks exploit vulnerabilities to compromise systems.
- Exploits are techniques used to compromise systems.
- Vulnerabilities are weaknesses in controlled systems.

**- Read PPT once**