Fundamentals of Computer Security

Prepared by: Computer Security Section, WSCSD ITMS
### COMPUTER SECURITY
**ESSENTIAL TERMINOLOGIES**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Exploit</th>
<th>Vulnerability</th>
<th>Cracker, Attacker, or Intruder</th>
<th>Attack</th>
<th>Data Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>An action or event that has the potential to compromise and/or violate security</td>
<td>A defined way to breach the security of an IT system through vulnerability</td>
<td>Existence of a weakness, design or implementation error that can lead to an unexpected, undesirable event compromising the security of a system</td>
<td>An individual who breaks into computer systems in order to steal, change, or destroy information</td>
<td>Any action derived from intelligent threats to violate the security of the system</td>
<td>Any action of stealing the information from the users’ systems</td>
</tr>
</tbody>
</table>
ABOUT COMPUTER SECURITY

Security is a state of well-being of information and infrastructure.

Computer security refers to the protection of computer systems and the information a user stores or processes.

Users should focus on various security threats and countermeasures in order to protect their information assets.
Why Computer Security?

Computer Security is important for protecting the confidentiality, integrity, and availability of computer systems and their resources.

Computer administration and management have become more complex which produces more attack avenues.

Evolution of technology has focused on the ease of use while the skill level needed for exploits has decreased.

Network environments and network-based applications provide more attack paths.
Potential Losses Due to Computer Security Attacks

- Misuse of computer resources
- Data loss/theft
- Loss of trust
- Financial loss
- Unavailability of resources
- Identity theft
Confidentiality is “ensuring that information is accessible only to those authorized to have access” (ISO-17799)

Authenticity is “the identification and assurance of the origin of information”

Integrity is “ensuring that the information is accurate, complete, reliable, and is in its original form”

Availability is “ensuring that the information is accessible to authorized persons when required without delay”

Non-repudiation is “ensuring that a party to a contract or a communication cannot deny the authenticity of their signature on a document”
Applications/software products by default are preconfigured for ease of use, which makes the user vulnerable to various security flaws.

Similarly, increased functionality (features) in an application make it difficult to use in addition to being less secure.

Moving the ball toward security means moving away from the functionality and ease of use.
Fundamental Concepts of Computer Security

PRECAUTION
Adhering to the preventive measures while using computer system and applications

MAINTENANCE
Managing all the changes in the computer applications and keeping them up to date

REACTION
Acting timely when security incidents occur
<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1: Physical Security</td>
<td>Safeguards the personnel, hardware, programs, networks, and data from physical threats</td>
</tr>
<tr>
<td>Layer 2: Network Security</td>
<td>Protects the networks and their services from unauthorized modification, destruction, or disclosure</td>
</tr>
<tr>
<td>Layer 3: System Security</td>
<td>Protects the system and its information from theft, corruption, unauthorized access, or misuse</td>
</tr>
<tr>
<td>Layer 4: Application Security</td>
<td>Covers the use of software, hardware and procedural methods to protect applications from external threats</td>
</tr>
<tr>
<td>Layer 5: User Security</td>
<td>Ensures that a valid user is logged in and that the logged-in user is allowed to use an application/program</td>
</tr>
</tbody>
</table>
Computer Security Risks to Home Users

• Home computers are prone to various cyber attacks as they provide attackers easy targets due to a low level of security awareness
• Security risk to home users arise from various computer attacks and accidents causing physical damage to computer systems

Computer Attacks
• Malware attacks
• Email attacks
• Mobile code (Java/JavaScript/ActiveX) attacks
• Denial of service and cross-site scripting attacks
• Identity theft and computer frauds
• Packet sniffing
• Being an intermediary for another attack (zombies)

Computer Accidents
• Hard disk or other component failures
• Power failure and surges
• Theft of a computing device
WHAT TO SECURE IN RELATION TO COMPUTER SECURITY?

HARDWARE
Laptops, Desktop PCs, CPU, hard disk, storage devices, cables, etc

SOFTWARE
Operating system and software applications

INFORMATION
Personal identification such as Social Security Number (SSN), passwords, credit card numbers, etc

COMMUNICATIONS
Emails, instant messengers, and browsing activities
WHAT MAKES A HOME COMPUTER VULNERABLE?

- Low level of security awareness
- Increasing online activities
- Default computer and application settings
- Not following any standard security policies or guidelines

None or very little investment in security systems
<table>
<thead>
<tr>
<th>WHAT MAKES A COMPUTER SYSTEM SECURE?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SYSTEM ACCESS CONTROLS</strong></td>
</tr>
<tr>
<td>• Ensure that unauthorized users do not get into the system</td>
</tr>
<tr>
<td>• Force legal users to be conscious about security</td>
</tr>
<tr>
<td><strong>DATA ACCESS CONTROLS</strong></td>
</tr>
<tr>
<td>• Monitor system activities such as who is accessing the data and for what purpose</td>
</tr>
<tr>
<td>• Define access rules based on the system security levels</td>
</tr>
<tr>
<td><strong>SYSTEM AND SECURITY ADMINISTRATION</strong></td>
</tr>
<tr>
<td>• Perform regular system and security administration tasks such as configuring system settings, implementing security policies, monitoring system state, etc.</td>
</tr>
<tr>
<td><strong>SYSTEM DESIGN</strong></td>
</tr>
<tr>
<td>• Deploy various security characteristics in system hardware and software design such as memory segmentation, privilege isolation, etc.</td>
</tr>
</tbody>
</table>
Computer Security Awareness helps minimize the chance of computer attacks.

It helps users to protect sensitive information and computing resources from unauthorized access.

It helps users minimize losses in case of an accident that causes physical damage to computer systems.

It helps prevent the loss of information stored on the systems.

It helps users to prevent cybercriminals from using their systems in order to launch attacks on the other computer systems.
Computer Security Things to Remember

- Security is a state of well-being of information and infrastructures.
- Computer security is the protection of computing systems and the data that they store or access.
- Confidentiality, integrity, non-repudiation, authenticity, and availability are the elements of security.
- Security risk to home users arise from various computer attacks and accidents causing physical damage to computer systems.
- Computer security awareness helps minimize the chances of computer attacks and prevent the loss of information stored on the systems.
BASIC COMPUTER SECURITY CHECKLIST

- Use of strong passwords
- Use of anti-virus systems
- Regular update of operating system and other installed applications
- Regular backup of important files
- Use of encryption techniques and digital signatures
- Use of firewall and intrusion detection systems
- Following standard guidelines for internet activities
- Physical security of computing infrastructure
- Awareness of current security scenario and attack techniques