Module 1

Lecture One: Introduction to Computer Security

1.1 The meaning of computer security

The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft of or damage to the hardware
- To prevent theft of or damage to the information
- To prevent disruption of service

Computer security is security applied to computing devices such as computers and smartphones, as well as computer networks such as private and public networks, including the whole Internet. The field covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, and are of growing importance in line with the increasing reliance on computer systems of most societies worldwide. It includes physical security to prevent theft of equipment, and information security to protect the data on that equipment. It is sometimes referred to as "cyber security" or "IT security", though these terms generally do not refer to physical security (locks and such). Some important terms used in computer security are:

Vulnerability
Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface. Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems.

Backdoors
A backdoor in a computer system, is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected.

The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device. It may also fake information about disk and memory usage.

Denial-of-service attack
Unlike other exploits, denials of service attacks are not used to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times

to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. These types of attack are, in practice, very hard to prevent, because the behaviour of whole networks needs to be analyzed, not only the behaviour of small pieces of code. Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers", used as part of a botnet with, for example; a worm, trojan horse, or backdoor exploit to control them) are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion.

Direct-access attacks
An unauthorized user gaining physical access to a computer (or part thereof) can perform many functions, install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as key drives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system. Direct-access attacks are the only type of threat to Standalone computers (never connect to internet), in most cases.

Eavesdropping
Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and Narus Insight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers.

Spoofing
Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Tampering
Tampering describes an intentional modification of products in a way that would make them harmful to the consumer.

Repudiation
Repudiation describes a situation where the authenticity of a signature is being challenged.

Information disclosure
Information Disclosure (Privacy breach or Data leak) describes a situation where information, thought as secure, is released in an untrusted environment.

Elevation of privilege
Elevation of Privilege describes a situation where a person or a program want to gain elevated privileges or access to resources that are normally restricted to him/it.

Exploits
An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a software "bug" or "glitch" in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently

includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack. The term "exploit" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in Trojan horses and computer viruses.

Indirect attacks
An indirect attack is an attack launched by a third-party computer. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonymizing systems, such as the tor onion router system.

Computer crime
Computer crime refers to any crime that involves a computer and a network.

Top 10 Cyber Crime Prevention Tips

1. **Use Strong Passwords**
Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. **Secure your computer**
    - **Activate your firewall**
    Firewalls are the first line of cyber defence; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.
    - **Use anti-virus/malware software**
    Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.
    - **Block spyware attacks**
    Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.

3. **Be Social-Media Savvy**
Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

4. **Secure your Mobile Devices**
Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

5. **Install the latest operating system updates**
Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

6. **Protect your Data**
Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

7. **Secure your wireless network**
Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

8. **Protect your e-identity**
Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).

9. **Avoid being scammed**
Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

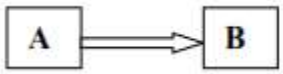
10. **Call the right person for help**
Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

Principles of Security

There are five principles of security. They are as follows:

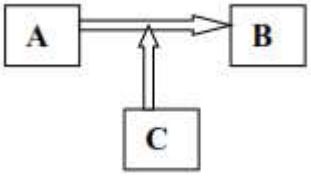
- *Confidentiality:*

The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the content of the message.



- *Integrity:*

The confidential information sent by A to B which is accessed by C without the permission or knowledge of A and B.



- *Authentication:*

Authentication mechanism helps in establishing proof of identification.

- Non-repudiation:

- *Access control:*

Access control specifies and control who can access what.

- *Availability:*

It means that assets are accessible to authorized parties at appropriate times.

Attacks

We want our security system to make sure that no data are disclosed to unauthorized parties.

- Data should not be modified in illegitimate ways
- Legitimate user can access the data

Types of attacks

Attacks are grouped into two types:

- *Passive attacks:* does not involve any modification to the contents of an original message
- *Active attacks:* the contents of the original message are modified in some ways.