SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : Fundamentals Of Cryptography

II YEAR / III SEMESTER

Unit I

Topic :Security Threats

Security Threats

Information Security threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion.

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behaves differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on system.

Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the **basis of Infection** Method are following:

1. **Virus –** They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

1. **Worms –** Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware.
2. **Trojan –** The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift.
3. **Bots –**: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad.

Malware on the **basis of Actions**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers.
2. **Spyware –** It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party.
3. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
4. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it.
5. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system
6. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

Malware on the **basis of Actions**

1. **Adware –** Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers.
2. **Spyware –** It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party.
3. **Ransomware –** It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
4. **Scareware –** It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it.
5. **Rootkits –** are designed to gain root access or we can say administrative privileges in the user system
6. **Zombies –** They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.