Program Security

IT5306 Principles of Information Security

Level III - Semester 5

© 2022 e-Learning Centre, UCSC

List of sub topics

1.1 Types of Malicious Software
1.2 Advanced Persistent Threat
1.3 Viruses and Worms
1.4 System Corruption
1.5 Attack Agents
1.6 Keyloggers, Phishing, and Spyware
1.7 Stealthing: Backdoors and Rootkits
1.8 Countermeasures

© 2022 e-Learning Centre, UCSC

1.1 Types of Malicious Software

- A malware is a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or - operating system or otherwise annoying or disrupting the activities of the victim.

- Although a range of aspects can be used to classify malware, one useful approach classifies malware into two broad categories, based on;

    1. how it spreads or **propagates** to reach the desired targets
    2. the actions or **payloads** it performs once a target is reached

© 2022 e-Learning Centre, UCSC

1.1 Types of Malicious Software (cont.)

- Propagation-based malware types:
  - Infected content - Viruses
  - Vulnerability exploit - worms
  - Social engineering - spam emails, trojans
- Payload-based malware types:
  - System corruption
  - Attack agents - Zombies, bots
  - Information theft - Keyloggers, phishing, spyware
  - Stealthing - Backdoors, rootkits.

© 2022 e-Learning Centre, UCSC

1.1 Types of Malicious Software (cont.)

- The development and deployment of malware requires considerable technical skill by software authors.
- This changed with the development of virus-creation toolkits, and then later on with more general attack kits.
- These toolkits now include a variety of propagation mechanisms and payload modules that even novices can use.
- Another significant development in malware activity over the last couple of decades is the change from attackers being individuals, often motivated to demonstrate their technical competence to their peers, to more organized and dangerous attack sources.
- These include politically motivated attackers, criminals, and organized crime; organizations that sell their services to companies and nations, and national government agencies.

© 2022 e-Learning Centre, UCSC

1.2 Advanced Persistent Threats

- Advanced Persistent Threats (APTs) are well-resourced, persistent application of a wide variety of intrusion technologies and malware to selected targets, usually business or political.
- APTs are typically attributed to state-sponsored organizations, with some attacks likely from criminal enterprises as well.
- APTs differ from other types of attack by their careful target selection, and persistent, often stealthy, intrusion efforts over extended periods.
- The aim of these attacks varies from theft of intellectual property or security and infrastructure related data to the physical disruption of infrastructure.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms

- Viruses are parasitic software fragments that attach themselves to some existing executable content.
- The fragment may be machine code that infects some existing application, utility, or system program, or even the code used to boot a computer system.
- More recently, the fragment has been some form of scripting code, typically used to support active content within data files such as Microsoft Word documents, Excel spreadsheets, or Adobe PDF documents.
- A computer virus is a piece of software that can "infect" other programs, or indeed any type of executable content, by modifying them. The modification includes injecting the original code with a routine to make copies of the virus code, which can then go on to infect other content.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

- A computer virus has three parts:
- **Infection mechanism:** The means by which a virus spreads or propagates, enabling it to replicate. The mechanism is also referred to as the infection vector.
- **Trigger:** The event or condition that determines when the payload is activated or delivered, sometimes known as a logic bomb.
- **Payload:** What the virus does, besides spreading. The payload may involve damage or may involve benign but noticeable activity.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

- During its lifetime, a typical virus goes through the following four phases:

- **Dormant phase:** The virus is idle and eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.

- **Propagation phase:** The virus places a copy of itself into other programs or into certain system areas on the disk.

- **Triggering phase:** The virus is activated to perform the function for which it was intended.

- **Execution phase:** The function is performed.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

- A virus classification by target:
- **Boot sector infector:** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
- **File infector:** Infects files that the operating system or shell consider to be executable.
- **Macro virus:** Infects files with macro or scripting code that is interpreted by an application.
- **Multipartite virus:** Infects files in multiple ways. Typically, the multipartite virus is capable of infecting multiple types of files, so that virus eradication must deal with all of the possible sites of infection.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

- A virus classification by concealment strategy:
- **Encrypted virus:** A form of virus that uses encryption to obscure it's content.
- **Stealth virus:** A form of virus explicitly designed to hide itself from detection by anti-virus software.
- **Polymorphic virus:** A form of virus that creates copies during replication that are functionally equivalent but have distinctly different bit patterns.
- **Metamorphic virus:** As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, using multiple transformation techniques, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

Macro viruses:

- Macro viruses infect scripting code used to support active content in a variety of user document types
- Macro viruses are particularly threatening for a number of reasons:
  - They are platform independent.
  - They infect documents, not executable portions of code.
  - They easily are spread, as the documents they exploit are shared in normal use.
  - Traditional file system access controls are of limited use in preventing their spread, since users are expected to modify them.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

Computer Worms:

- A worm is a program that actively seeks out more machines to infect.
- Worm programs exploit software vulnerabilities to gain access to each new system. They can use network connections to spread from system to system. They can also spread through shared media.
- To replicate itself, a worm uses some means to access remote systems:
  - Electronic mail or instant messenger facility
  - File sharing
  - Remote execution capability
  - Remote file access or transfer capability
  - Remote login capability

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

- A network worm must identify potential systems running the vulnerable service, and then infect them.

- Some of the network address scanning strategies for a network worm:
  - **Random:** Each compromised host probes random addresses in the IP address space, using a different seed.

  - **Hit-List:** The attacker first compiles a long list of potential vulnerable machines. Each infected machine is provided with a portion of the list to scan.

  - **Topological:** This method uses information contained on an infected victim machine to find more hosts to scan.

  - **Local subnet:** If a host can be infected behind a firewall, that host then looks for targets in its own local network.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)

- Computer viruses and worms exhibit similar self-replication and propagation behavior to biological viruses.

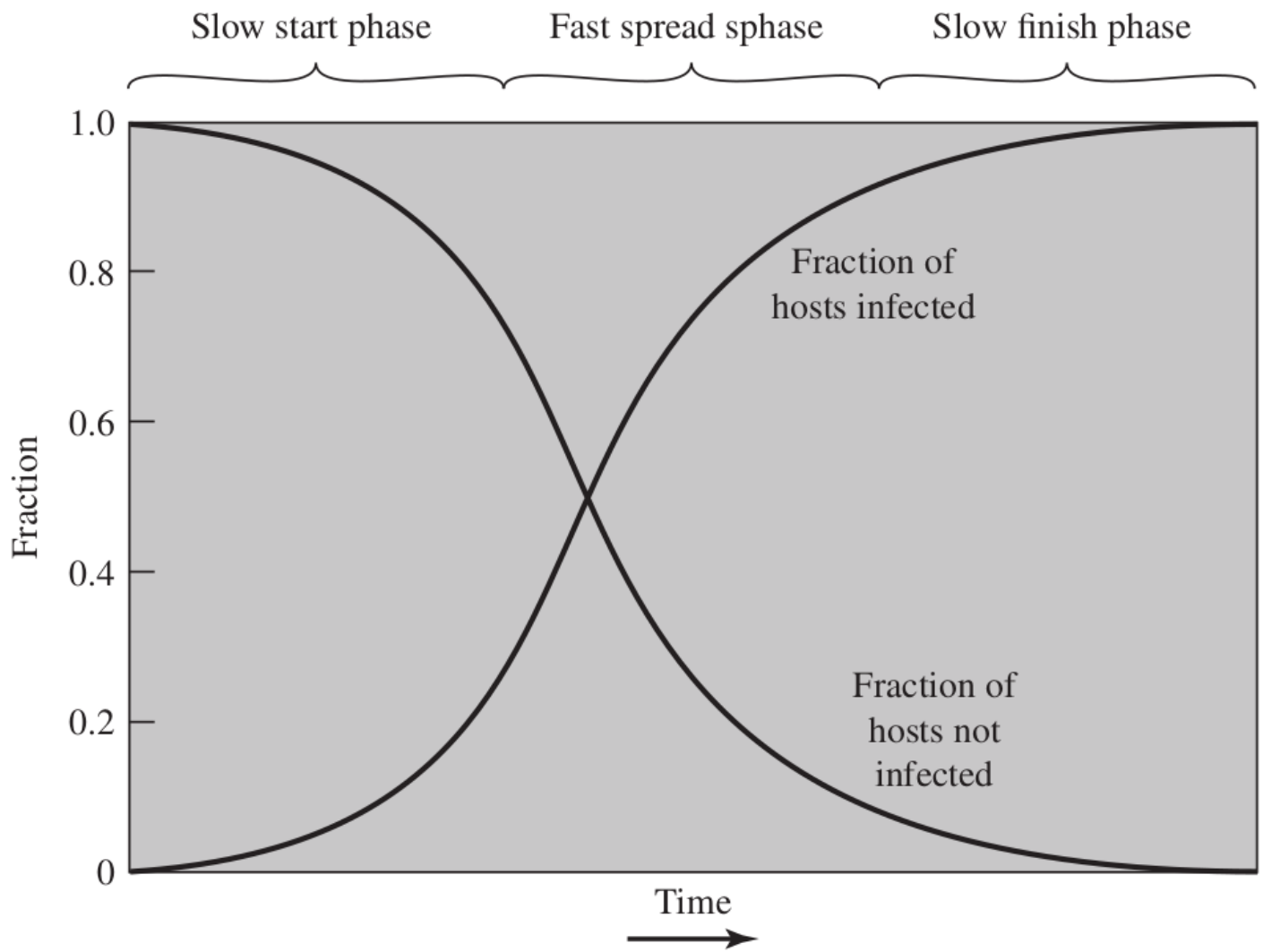
$$\mathrm{d}\, I(t) / dt = \beta\, I(t)\, S(t)$$

  - $I(t)$ = number of individuals infected as of time t
  - $S(t)$ = number of susceptible individuals (susceptible to infection but not yet infected) at time t
  - β = infection rate
  - N = size of the population, $N = I(t) + S(t)$

- Initially, the number of hosts increases exponentially. With time, infecting hosts waste some time attacking already infected hosts, which reduces the rate of infection. When most vulnerable computers have been infected, the worm seeks out those remaining hosts that are difficult to identify.

© 2022 e-Learning Centre, UCSC

1.3 Viruses and Worms (cont.)



© 2022 e-Learning Centre, UCSC

1.4 System Corruption

- Once malware is active on the target system, the next concern is what actions it will take on this system — that is, what payload does it carry. Possible outcomes are:
  - destroying data on the infected system when certain trigger conditions were met.
  - displaying unwanted messages or content on the user's system when triggered.
  - inflicting physical damage on the system.

- Some malware encrypts the user's data, and demands payment in order to access the key needed to recover this information, i.e., ransomware.

- The user needed to pay a ransom, or to make a purchase from certain sites, in order to receive the key to decrypt this data.

© 2022 e-Learning Centre, UCSC

1.5 Attack Agents

- Attack agents are the malware that subverts the computational and network resources of the infected system for use by the attacker.
- Such a system is known as a bot (robot), zombie or drone.
- They secretly takes over another Internet-attached computer and then uses that computer to launch or manage attacks that are difficult to trace to the bot's creator.
- A collection of bots often is capable of acting in a coordinated manner; such a collection is referred to as a botnet.

© 2022 e-Learning Centre, UCSC

1.5 Attack Agents (cont.)

- Uses of Bots:
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Sniffing traffic
  - Keylogging
  - Spreading new malware
  - Installing advertisement add-ons and browser helper objects (BHOs)
  - Attacking IRC chat networks
  - Manipulating online polls/games
- Another potential use of botnets that emerged in the recent times is using them for cryptocurrency mining.

© 2022 e-Learning Centre, UCSC

1.5 Attack Agents (cont.)

- A worm propagates itself and activates itself, whereas a bot is controlled by some form of command-and-control (C&C) server network.
- This contact does not need to be continuous, but can be initiated periodically when the bot observes it has network access.
- The bots can contact the C&C through various means, such as HTTP protocol and peer-to-peer communication protocols.

© 2022 e-Learning Centre, UCSC

1.6 Keyloggers, Phishing, and Spyware

- Some malware gathers data stored on the infected system for use by the attacker.
- A common target is the user's login and password credentials to banking, gaming, and related sites, which the attacker then uses to impersonate the user to access these sites for gain.
- Less commonly, the payload may target documents or system configuration details for the purpose of reconnaissance or espionage.
- These attacks target the confidentiality of this information.

© 2022 e-Learning Centre, UCSC

1.6 Keyloggers, Phishing, and Spyware (cont.)

- Users send their login and password credentials to banking, gaming, and related sites over encrypted communication channels (e.g., HTTPS or POP3S), which protects them from capture by monitoring network packets.

- To bypass this, an attacker can install a **keylogger**, which captures keystrokes on the infected machine to allow an attacker to monitor this sensitive information.

- **Spyware** monitors a wide range of activity on the system. This may include monitoring the history and content of browsing activity, redirecting certain Web page requests to fake sites controlled by the attacker, and dynamically modifying data exchanged between the browser and certain Web sites of interest.

- All of which can result in significant compromise of the user's personal information.

© 2022 e-Learning Centre, UCSC

1.6 Keyloggers, Phishing, and Spyware (cont.)

- Another approach used to capture a user's login and password credentials is to include a URL in a spam email that links to a fake Website controlled by the attacker, but which mimics the login page of some banking, gaming, or similar site.
- This is normally included in some message suggesting that urgent action is required by the user to authenticate their account, to prevent it being locked.
- If the user is careless, and does not realize that they are being conned, then following the link and supplying the requested details will certainly result in the attackers exploiting their account using the captured credentials.
- This form of attacks are known as **phishing** attacks.

© 2022 e-Learning Centre, UCSC

1.6 Keyloggers, Phishing, and Spyware (cont.)

- A more dangerous variant of phishing is called **spear-phishing** attack.
- This again is an email claiming to be from a trusted source. However, the recipients are carefully researched by the attacker, and each email is carefully crafted to suit its recipient specifically, often quoting a range of information to convince them of its authenticity.
- This greatly increases the likelihood of the recipient responding as desired by the attacker.
- This type of attack is particularly used in industrial and other forms of espionage by well-resourced organizations.

© 2022 e-Learning Centre, UCSC

1.7 Stealthing: Backdoors and Rootkits

- Stealthing concerns techniques used by malware to hide its presence on the infected system, and to provide covert access to that system.
- A **backdoor**, also known as a trapdoor, is a secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures.
- Programmers have used backdoors legitimately for many years to debug and test programs; such a backdoor is called a maintenance hook.
- Backdoors become threats when unscrupulous programmers use them to gain unauthorized access.

© 2022 e-Learning Centre, UCSC

1.7 Stealthing: Backdoors and Rootkits (cont.)

- **A rootkit** is a set of programs installed on a system to maintain covert access to that system with administrator (or root) 3 privileges, while hiding evidence of its presence to the greatest extent possible.
- This provides access to all the functions and services of the operating system.
- A rootkit can make many changes to a system to hide its existence, making it difficult for the user to determine that the rootkit is present and to identify what changes have been made.

© 2022 e-Learning Centre, UCSC

1.7 Stealthing: Backdoors and Rootkits (cont.)

- A rootkit can have following features:
  - Persistent: Activates each time the system boots.
  - Memory based: Has no persistent code and therefore cannot survive a reboot.
  - User mode: Intercepts calls to APIs (application program interfaces) and modifies returned results.
  - Kernel mode: Can intercept calls to native APIs in kernel mode.
  - Virtual machine based: Installs a lightweight virtual machine monitor, and then runs the OS above it.
  - External mode: The malware is located outside the normal operation mode of the targeted system, e.g., BIOS.

© 2022 e-Learning Centre, UCSC

1.8 Countermeasures

- The ideal solution to the threat of malware is prevention: Do not allow malware to get into the system in the first place, or block the ability of it to modify the system.

- This goal is, in general, nearly impossible to achieve, although taking suitable countermeasures to harden systems and users in preventing infection can significantly reduce the number of successful malware attacks.

- Four main elements of prevention:
  - policy (eg keep backups..)
  - awareness
  - vulnerability mitigation
  - threat mitigation

© 2022 e-Learning Centre, UCSC