Malware: Malicious Software

Viruses, Worms, Trojans, Rootkits

- **Malware** can be classified into several categories, depending on propagation and concealment
- **Propagation**
  - **Virus**: human-assisted propagation (e.g., open email attachment)
  - **Worm**: automatic propagation without human assistance
- **Concealment**
  - **Rootkit**: modifies operating system to hide its existence
  - **Trojan**: provides desirable functionality but hides malicious operation
- Various types of payloads, ranging from annoyance to crime
Insider Attacks

• An **insider attack** is a security breach that is caused or facilitated by someone who is a part of the very organization that controls or builds the asset that should be protected.

• [GT] textbook defines malware as an insider attack, because it depends on a security hole in a software system, which must have been created by a programmer.

Backdoors

• A **backdoor**, which is also sometimes called a **trapdoor**, is a hidden feature or command in a program that allows a user to perform actions he or she would not normally be allowed to do.

• When used in a normal way, this program performs completely as expected and advertised.

• But if the hidden feature is activated, the program does something unexpected, often in violation of security policies, such as performing a privilege escalation.

• Backdoors are left in software for debugging, error-handling, updates, administration, etc.
Logic Bombs

• A logic bomb is a program that performs a malicious action as a result of a certain logic condition.
• The classic example of a logic bomb is a programmer coding up the software for the payroll system who puts in code that makes the program crash should it ever process two consecutive payrolls without paying him.
• Another classic example combines a logic bomb with a backdoor, where a programmer puts in a logic bomb that will crash the program on a certain date.

The Omega Engineering Logic Bomb

• An example of a logic bomb that was actually triggered and caused damage is one that programmer Tim Lloyd was convicted of using on his former employer, Omega Engineering Corporation. On July 31, 1996, a logic bomb was triggered on the server for Omega Engineering’s manufacturing operations, which ultimately cost the company millions of dollars in damages and led to it laying off many of its employees.
The Omega Bomb Code

• The Logic Behind the Omega Engineering Time Bomb included the following strings:
• 7/30/96
  – Event that triggered the bomb
• F:
  – Focused attention to volume F, which had critical files
• F:\LOGIN\LOGIN 12345
  – Login a fictitious user, 12345 (the back door)
  – That user had supervisor permissions and no password!
• CD \PUBLIC
  – Moves to the public folder of programs
• FIX.EXE /Y F:*.*
  – Run a program, called FIX, which actually deletes everything
• PURGE F:\ALL
  – Prevent recovery of the deleted files

Defenses against Insider Attacks

• Avoid single points of failure.
• Use code walk-throughs.
• Use archiving and reporting tools.
• Limit authority and permissions.
• Physically secure critical systems.
• Monitor employee behavior.
• Control software installations.
“Kleptography” [Moti Yung]: Logic Bombs in Cryptography

• A cryptographic algorithm can be implemented in a way which looks correct but it gives backdoors to its creator, e.g.
  – encrypts private key under creator’s public key
  – embeds this ciphertext into the public key
  – adversary can then decrypt the private key from the public key
• Kleptographic implementation is undetectable w/o examining (and understanding) sourcecode
• Can you trust off-the-shelf crypto implementation?

Computer Viruses

• A computer virus is computer code that can replicate itself by modifying other files or programs to insert code that is capable of further replication.
• This self-replication property is what distinguishes computer viruses from other kinds of malware, such as logic bombs.
• Another distinguishing property of a virus is that replication requires some type of user assistance, such as clicking on an email attachment or sharing a USB drive.
Biological Analogy

- Computer viruses share some properties with Biological viruses

Early History

- 1972 sci-fi novel “When HARLIE Was One” features a program called VIRUS that reproduces itself
- First academic use of term virus by PhD student Fred Cohen in 1984, who credits advisor Len Adleman with coining it
- In 1982, high-school student Rich Skrenta wrote first virus released in the wild: Elk Cloner, a boot sector virus
- (c)Brain, by Basit and Amjood Farooq Alvi in 1986, credited with being the first virus to infect PCs
Virus Phases

- **Dormant phase.** During this phase, the virus just exists—the virus is laying low and avoiding detection.
- **Propagation phase.** During this phase, the virus is replicating itself, infecting new files on new systems.
- **Triggering phase.** In this phase, some logical condition causes the virus to move from a dormant or propagation phase to perform its intended action.
- **Action phase.** In this phase, the virus performs the malicious action that it was designed to perform, called **payload**.
  - This action could include something seemingly innocent, like displaying a silly picture on a computer’s screen, or something quite malicious, such as deleting all essential files on the hard drive, or sending these files to an outside location.

Infection Types

- **Overwriting**
  - Destroys original code
- **Pre-pending**
  - Keeps original code, possibly compressed
- **Infection of libraries**
  - Allows virus to be memory resident
  - E.g., kernel32.dll
- **Macro viruses**
  - Infects MS Office documents
  - Often installs in main document template
Degrees of Complication

• Viruses have various degrees of complication in how they can insert themselves in computer code.

Concealment

• Detection
  – Virus “Signature”

• Encrypted virus
  – Decryption engine + encrypted body
  – Randomly generate encryption key
  – Detection looks for decryption engine

• Polymorphic virus
  – Each virus copy uses a different encryption key

• Metamorphic virus
  – Different virus bodies
  – Approaches include code permutation and instruction replacement
  – Challenging to detect