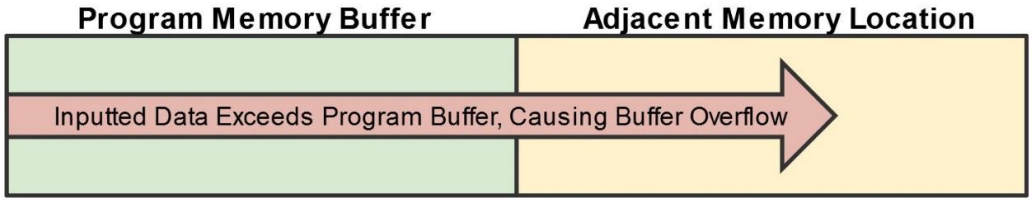
Buffer Overflows

Buffer Overflows

- A **buffer overflow** is a programming error that occurs when a program (or system process) attempts to write more data to a fixed-length block of memory (buffer) than the buffer is allocated to store.
- The overflow is then written to adjacent memory locations, which can be exploited with malicious code with the intent to cause an application or system crash or to introduce malware to the system.
- Buffer overflow protections include data input validation, Windows run-time protections, and secure development practices.



Viruses and Polymorphic Viruses

Viruses

- A virus is a set of malicious code that infects a host.
- It's executed when typically when an application is executed.
- **It will replicate, and when an activation trigger occurs**, it will deliver the objective, which is usually malicious.
  - Install Spyware
  - Steal Sensitive Data
  - Corrupt your Operating System
- Email is the most popular method used to spread viruses.

Types of Viruses

- **Boot Sector Viruses**
  - Infects Boot Sector of Hard Drive
- **Program Viruses**
  - Embedded into a Program
- **Script Viruses**
  - Web-Based Script
- **Macro Viruses**
  - Microsoft Office Macros
- **Polymorphic Viruses**
  - Mutating Viruses

Polymorphic Viruses

- A polymorphic virus is a shape-shifting virus.
- Creates modified, self-encrypting versions of itself to avoid virus definition detection.

Worms

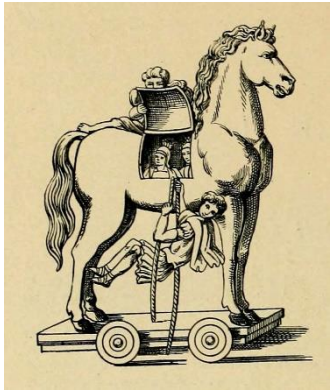
Worms

- Malicious software that travels throughout a network **without the assistance of a host application or user interaction**.
- One of the significant problems caused by worms is that they **consume network bandwidth**.
- Can replicate themselves hundreds of times and spread to all the systems in the network, causing each of these systems to also spread the worm.
- Network performance can slow to a crawl.
- Can travel autonomously over the network.
- **A worm does not need a host application and doesn't require a user to execute it**.

Trojan Horses

Trojan Horse

- A Trojan horse is a program that **looks like something desirable**, such as a screen saver but includes other malicious code.
- It deceives users into executing it and installing malware onto their computer:
  - Free Anti-virus software
  - Free Computer Cleanup software



Logic Bombs

Logic Bombs

- A logic bomb is a string of code embedded into an application that will execute in response to an event.
- The event may be:
  - When a specific date is reached
  - A user launches a specific program
  - Any condition the programmer decides on

Spyware and Adware

Spyware

- Spyware is malware that's installed on a user's system **without your awareness or consent**.
- It runs quietly in the background, collecting information or monitoring your activities, such as:
  - Keystrokes
  - Screenshots
  - Authentication Credentials
  - Personally Identifiable Information
  - Web Form Data

Adware

- **Adware** is unwanted software that's designed to show advertisements or collect marketing-type data about you.
- Just like spyware, you typically won't know adware is running on your computer until you notice unusual advertising pop-ups.

Ransomware

Ransomware

- **Ransomware** prevents users from accessing their system or personal files and demands a ransom payment in order to regain access:
  - Encrypts some or all of a user's files.
  - Demands cryptocurrency payment in exchange for the decryption key.
- WannaCry attack in 2017 infected more than 230,000 computers worldwide, demanding $300 in bitcoin payment per computer.
- In 2021, ransomware attacks are up 350%
  - Acer was hit with $50 million ransomware by the REvil hacker group.

Rootkits

Rootkit

- Malware that is designed to gain root (administrative) access on a system by exploiting known vulnerabilities that enable privilege escalation.
- Modify core system files and be invisible to the operating system so they can persist without detection:
  - Governmental organization spying on another government
  - Corporate espionage
  - Hacker(s) stealing customer data

Zero Day Attacks

Zero Day Attacks

- Zero-day attacks are cyber attacks against software flaws that are unknown and have no patch or fix.
- Occurs on the same day a weakness is discovered and is exploited before a fix becomes available from its creator.
- **Bug bounty** programs are offered by software developers by which individuals can receive recognition and **compensation for reporting bugs**, especially those pertaining to exploits and vulnerabilities.

Protecting Against Malware

Protecting Against Malware

- Keep your computer and software updated.
- Use a non-administrator account (when possible).
- Use trusted endpoint protection / anti-malware software.
- Be careful about opening email attachments and images.
- Think twice before clicking links and downloading files.
- Don’t trust browser pop-up windows telling you to download software.