

# CSC369 Week 11 Notes

Hyungmo Gu

June 1, 2020

- Security
  - Computer Security
    - \* Techniques for **computing** in the presence of adversaries
    - \* Four requirements of security
      1. **Confidentiality:**
        - Preventing unauthorized release of info
      2. **Integrity:**
        - Preventing unauthorized modification of info
      3. **Availability:**
        - Ensuring access to legitimate users
      4. **Authenticity:**
        - Verifying the identity of a user
    - \* Protection is about providing all of the above on a single machine
      - Is usually considered the responsibility of the OS
  - Cryptography
    - \* Techniques for communicating in the presence of adversaires
- Types of Threats
  1. **Interception or eavesdropping:**
    - Attacker gains knowledge they should not have access to
    - is attack on *confidentiality*
    - Reading or copying files that attacker should not have access to
    - Intercepting network packets
  2. **Modification:**
    - Attacker alters existing files, programs, packets, etc.
    - is attack on *integrity*
    - e.g. Starcraft map hack



### 3. Theft of Service:

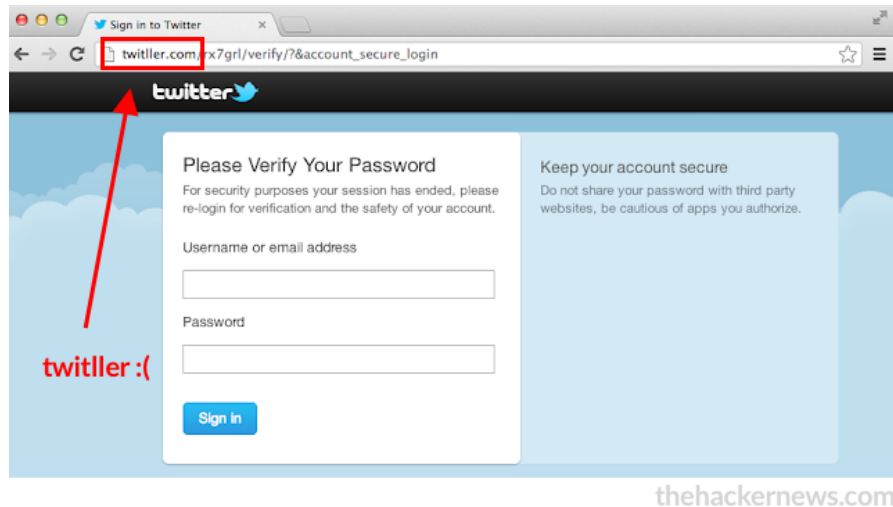
- Happens when attacker installs daemon
- Is attack on *availability*
- e.g. installing Daemon Tools Lite to run favourite Starcraft without CD Key (Don't do it!!)



wikipedia.org

### 4. Fabrication:

- Attacker creates counterfeit objects (files, messages, etc) which appears to come from a trusted source
- Is attack on *authenticity*
- e.g. Fake Twitter website



- Vulnerabilities in the System
  - Physical Access
    - \* Unauthorized physical access makes it a lot easier to gain unauthorized digital access
    - \* e.g. Setting 0000 as PIN number to Moe's Smartphone
  - Humans
    - \* Who should you trust and how much?
    - \* e.g. An employee giving others an access to Google's search algorithm source code
  - Operating Systems
    - \* Flaws in the system allows security protocols to be circumvented
  - Networks
    - \* Data traveling over unsecured communication lines, across multiple administrative domains
    - \* e.g. Sending password data through HTTP, and not HTTPS (Data is sent without encryption)
- Malicious Software (Malware)
  - **Trap Doors**
    - \* Is a program containing secret entry point that allows attacker to bypass security
  - **Logic Bombs**
    - \* Is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met <sup>[1]</sup>
    - \* e.g. Viruses that activate on certain dates <sup>[1]</sup>
  - **Trojan Horses**

- \* Misleads user of its true intent <sup>[2]</sup>
- \* Tricks users into running it
- \* Gives full access to a stranger
- \* e.g. Fake Mac flash player <sup>[3]</sup>



## – Viruses

Is a program that can “infect” other programs by copying itself onto them

## – Worms

- \* Is a program that spreads via network connections
- \* Relies on security failures on the target computer <sup>[4]</sup>
- \* Uses infected machine as a host to scan and infect other computers <sup>[4]</sup>
- \* Does not need to attach to another program like viruses

## References

- 1) Wikipedia: Logic Bomb, link
- 2) Wikipedia: Trojan Horse, link
- 3) Hongkiat: 10 Deadliest Computer Viruses of All Time, link
- 4) Wikipedia: Computer worm, link

- Stack & Buffer Overflow Attacks

- Security Design Principles
- Principle of Least Privilege
- Access Control Lists
- SSL