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 tey 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

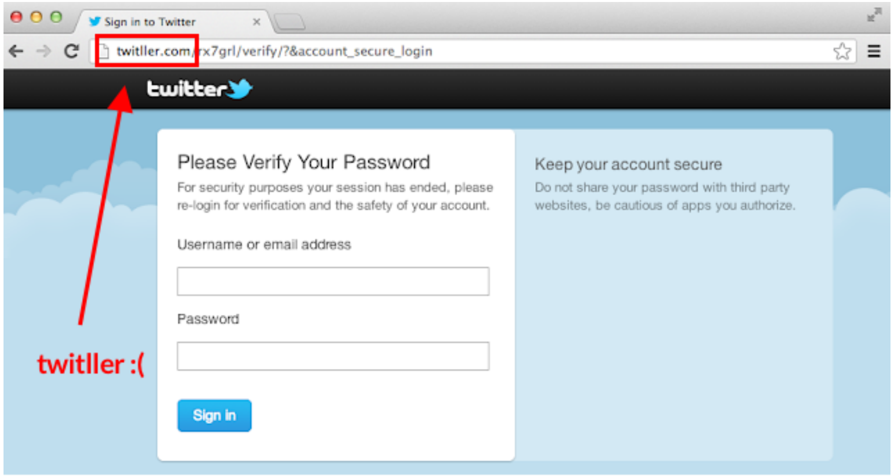
ValiantChaos Maphack v1.2.9
Cracked by roile3k a.k.a. Sheppard

www.kitguru.net

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



Sign in to Twitter
twitller.com/rx7grl/verify/?&account_secure_login
twitter
Username or email address
Password
Sign in
twitller :(

Please Verify Your Password

For security purposes your session has ended, please re-login for verification and the safety of your account.

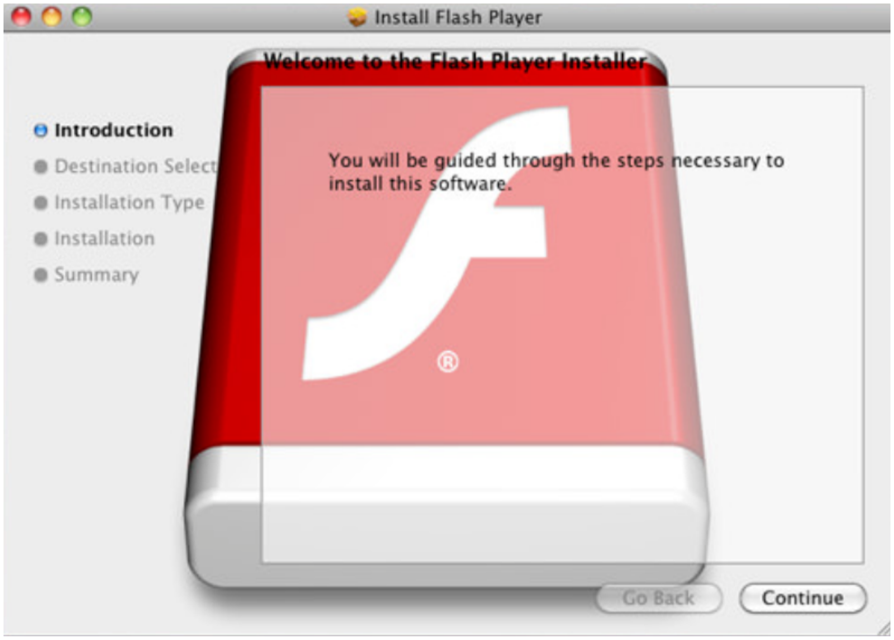
Keep your account secure

Do not share your password with third party websites, be cautious of apps you authorize.

thehackernews.com

- Vulnerabilities in the System
  - Physical Access
    - Unauthorized physical acccess 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 treveling 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 peiece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met [1]
    - e.g. Viruses that activate on certain dates [1]
  - **Trojan Horses**

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



You will be guided through the steps necessary to install this software.

www.hongkiat.com

  - **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 [4]
    - Uses infected machine as a host to scan and infect other computers [4]
    - 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

- Happens when a program writes more data to a buffer located on the stack than what is actually allocated [1]
- Is most common means of gaining unauthorized access to a system

Example:

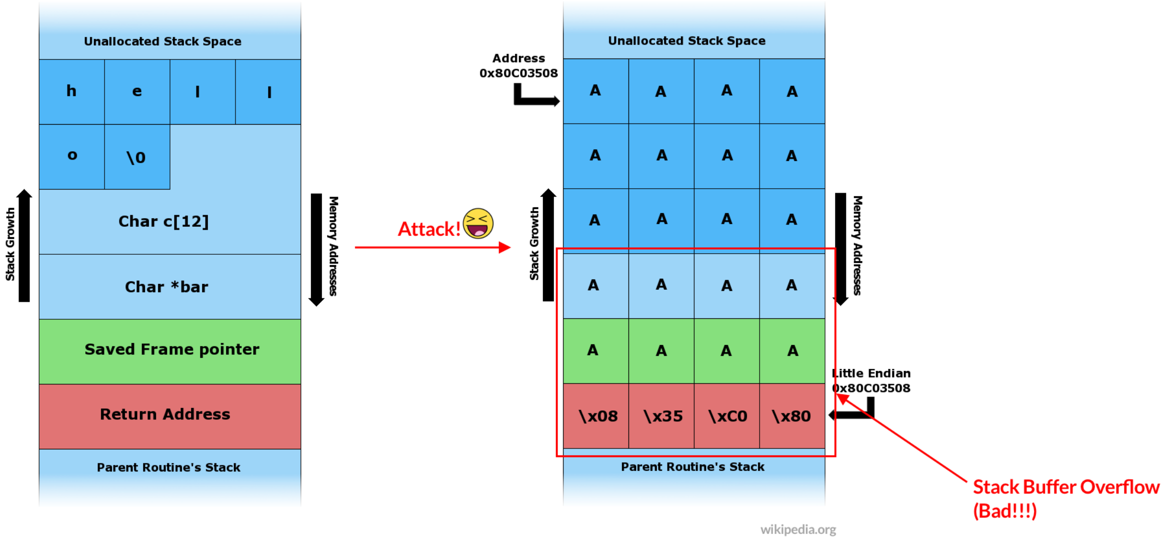
```c
#include <string.h>

void foo(char *bar)
{
    char c[12]; // <- Overflow with value more than 12 characters in length

    strcpy(c, bar);  // no bounds checking
}

int main(int argc, char **argv)
{
    foo(argv[1]);
    return 0;
}

```



References

1) Wikipedia: Stack buffer overflow, link

- Security Design Principles
- Princple of Least Privilege

- Access Control Lists
- SSL