Popa and Weaver
Fall 2021

CS 161
Computer Security

Discussion 1

Note: **Feel free to come by office hours held by any of the staff.** Don't hesitate to ask for help! Our office hours exist to help you. Please visit us if you have any questions or doubts about the material.

Stack Diagram Practice

Consider the following simple function, and its corresponding assembly code

```
1  void swap(int* num1, int* num2, int arr_local[]) {
2      int temp = *num1;
3      *num1 = *num2;
4      arr_local[0] = *num1;
5      *num2 = temp;
6      arr_local[1] = *num2;
7  }
8
9  int main(void)
10 {
11     int x = 61;
12     int y = 1;
13     int arr[2];
14     swap(&x , &y, arr);
15 }
```

1. Complete the diagram of the stack if the code were executed until a breakpoint set on line 3. Assume normal (non-malicious) program execution. You do not need to write the values on the stack, only the names. There are no extraneous boxes, and each box represents 4 bytes in memory. The bottom of the page represents the lower addresses.

2. Now, draw arrows on the stack diagram denoting where the ESP and EBP point if the code were executed until a breakpoint set on line 3.

main's sfp
x
y
arr
arr
int* arr_local
int* num2
int* num1
swap's rip
swap's sfp
temp

Security Principles

We discussed the following security principles in lecture (*or in the textbook*, which you are responsible for reading):

A. *Know your threat model:* Know your attacker and their resources; the security assumptions originally made may no longer be valid

B. *Consider human factors:* Security systems must be usable by ordinary people

C. *Security is economics:* Security is a cost-benefit analysis, since adding security usually costs more money

D. *Detect if you can't prevent:* If one cannot prevent an attack, one should be able to at least detect when an attack happens

E. *Defense in depth:* Layer multiple defenses together

F. *Least privilege:* Minimize how much privilege you give each program and system component

G. *Separation of responsibility:* Split up privilege, so no one person or program has complete power

H. *Ensure complete mediation:* Make sure to check *every* access to *every* object

I. *Consider Shannon's Maxim:* Do not rely on security through obscurity

J. *Use fail-safe defaults:* If security mechanisms fail or crash, they should default to secure behavior

K. *Design in security from the start:* Retrofitting security to an existing application after it has been developed is a difficult proposition

Identify the principle(s) relevant to each of the following scenarios:

1. New cars often come with a valet key. This key is intended to be used by valet drivers

who park your car for you. The key opens the door and turns on the ignition, but it does not open the trunk or the glove compartment.

2. Many home owners leave a house key under the floor mat in front of their door.

3. It is not worth it to use a $400,000 bike lock to protect a $100 bike.

4. Warranties on cell phones do not cover accidental damage, which includes liquid damage. Unfortunately for cell phone companies, many consumers who accidentally damage their phones with liquid will wait for it to dry, then take it in to the store, claiming that "it broke by itself". To combat this threat, many companies have begun to include on the product a small sticker that turns red (and stays red) when it gets wet.

5. Social security numbers were not originally designed as a secret identifier. Nowadays, they are often easily obtainable or guessable.

6. Even if you use a password on your laptop lockscreen, there is software which lets a skilled attacker with specialized equipment to bypass it.

7. Shamir's secret sharing scheme allows us to split a "secret" between multiple people, so that all of them have to collaborate in order to recover the secret.

8. DRM encryption is often effective, until someone can reverse-engineer the decryption algorithm.

9. Banks often make you answer your security questions over the phone. Answers to these questions are "low entropy", meaning that they are easy to guess. Some security conscious people instead use a random password as the answer to the security question.[1] However attackers can sometimes convince the phone representative by claiming "I just put in some nonsense for that question".

[1] Q: "What is your dog's maiden name?". A: "60ba6b1c881c6b87"

10. Often times at bars, an employee will wait outside the only entrance to the bar, enforcing that people who want to enter the bar form a single-file line. Then, the employee checks each individual's ID to verify if they are 21 before allowing them entry into the bar.

11. Tesla vehicles come equipped with ”Sentry Mode” which records footage of any break ins to the vehicle and alerts the vehicle owner of the incident.

12. When a traffic light detects that it may be giving conflicting signals, it enters a state of error and displays a flashing red light in all directions.

Solution: (Note that there may be principles that apply other than those listed below.)

1. Principle of least privilege. They do not need to access your trunk or your glove box, so you don't give them the access to do so.
2. Shannon's Maxim. The security of your home depends on the belief that most criminals don't know where your key is. With a modicum of effort, criminals could find your key and open the lock.
3. Security is economics. It is more expensive to buy $400 bike lock than to simply buy a new bike to replace it.
4. There are probably two most relevant factors. “Consider human factors”: people will always try to lie and you must account for that when creating a system. More importantly, “Detect if you can't prevent”: it's prudent to try to add ways to detect something when creating the phone, since something like water damage is impossible to prevent.
5. Design security in from the start. Social security numbers were not designed to be authenticators, so security was not designed in from the start. The number is based on geographic region, a sequential group number, and a sequential serial number. They have since been repurposed as authenticators.
6. Know your threat model: most petty thieves do not have access to this software. (The software referenced is pcileech. The corresponding hardware is on my wishlist. -Keyhan Vakil)
7. Separation of responsibility: require everyone to come together to produce the secret, preventing one person from using the secret alone.

8. Shannon's Maxim. You must assume the attacker knows the system, so DRM encryption is not effective.

9. Consider human factors. The phone rep is inclined to believe the attacker is not malicious (social engineering).

10. Ensure complete mediation. There is a single access point through which everyone who wishes to enter the bar must be verified to be 21 before obtaining access.

11. Detect if you can't prevent. The vehicle owner learns about the intrusion to their vehicle even if they were not able to prevent it.

12. Use fail-safe defaults. The traffic light fails into a safe state because it functions as a stop sign for cars in all directions rather than continuing to operate with conflicting signals.