Popa
Spring 2018

CS 161
Computer Security

Discussion 2

Week of January 29, 2018

Question 1 ***Software Vulnerabilities*** **(20 min)**

For the following code, assume an attacker can control the value of `basket` passed into `eval_basket`. The value of `n` is constrained to correctly reflect the number of elements in `basket`.

The code includes several security vulnerabilities. **Circle *three* such vulnerabilities** in the code and **briefly explain** each of the three.

```
1  struct food {
2          char name[1024];
3          int calories;
4  };
5
6  /* Evaluate a shopping basket with at most 32 food items.
7     Returns the number of low-calorie items, or -1 on a problem. */
8  int eval_basket(struct food basket[], size_t n) {
9          struct food good[32];
10         char bad[1024], cmd[1024];
11         int i, total = 0, ngood = 0, size_bad = 0;
12
13         if (n > 32) return -1;
14
15         for (i = 0; i <= n; ++i) {
16                 if (basket[i].calories < 100)
17                         good[ngood++] = basket[i];
18                 else if (basket[i].calories > 500) {
19                         size_t len = strlen(basket[i].name);
20                         snprintf(bad + size_bad, len, "%s ", basket[i].name);
21                         size_bad += len;
22                 }
23
24                 total += basket[i].calories;
25         }
26
27         if (total > 2500) {
28                 const char *fmt = "health-factor --calories %d --bad-items %s";
29                 fprintf(stderr, "lots of calories!");
30                 snprintf(cmd, sizeof cmd, fmt, total, bad);
31                 system(cmd);
32         }
33
34         return ngood;
35 }
```

Reminders:

- **snprintf(buf, len, fmt, ...)** works like **printf**, but instead writes to **buf**, and won't write more than **len - 1** characters. It terminates the characters written with a '\0'.
- **system** runs the shell command given by its first argument.

Question 2 ***Security Principles*** **(15 min)**

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

A. Security is economics
B. Least privilege
C. Know your threat model
D. Defense in depth
E. Consider human factors
F. Design in security from the start
G. Ensure complete mediation
H. Division of trust
I. Consider Shannon's Maxim

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 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 doesn't work, but they don't know why. 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. If you use a random password as the answer to a security question, an attacker can often convince the phone representative by claiming "I just put in some nonsense for that question".

Question 3 ***TCB (Trusted Computing Base)*** **(10 min)**

In lecture, we discussed the importance of a TCB and the thought that goes into designing it. Answer these following questions about the TCB:

1. What is a TCB?

2. What can we do to reduce the size of the TCB?

3. What components are included in the (physical analog of) TCB for the following security goals:

   (a) Preventing break-ins to your apartment

   (b) Locking up your bike

   (c) Preventing people from riding BART for free

   (d) Making sure no explosives are present on an airplane