ITIS 6200/8200 Principles of Information Security and Privacy

Homework 1

Questions 1. We discussed the following security principles in lecture: (50 points)

A. Know your threat model: Know your attacker and their resources; the security assumptions originally made may no longer be valid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 costbenefit 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 principle(s) relevant to each of the following scenarios. Note that there may be more than one principle that applies in some of these scenarios. Give **one** answer that you believe is most relevant.

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

1. TAs of our class are allowed to edit assignments and upload grades in Canvas. Their credentials don't give them access to submitting final grades of students to the associate dean of the CCI.

Ans: Principle of least privilege. They do not need to decide and submit the final grades, so don't give them the access.

2. The garage doors of some residential houses use the years of the houses' construction as default passcode. Many home owners just keep it that way.

Ans: Shannon's Maxim. The security of your home depends on the belief that most criminals don't know what year your houses were built. They are in fact public information.

Know your threat model is also correct here.

3. It is not worth it to use a $500 lock to protect a $100 bike.

Ans: Security is economics. It is more expensive to buy $500 bike lock than to simply buy a new bike to replace it.

4. Social security numbers were not originally designed as a secret identifier. Nowadays, they are often easy to guess and obtain.

Ans: 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.

5. 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.

Ans: Separation of responsibility: require everyone to come together to produce the secret, preventing one person from using the secret alone.

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

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

7. 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. However, attackers can sometimes convince the phone representative by claiming "I just put in some nonsense for that question".

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

8. 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.

Ans: 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.

9. 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.

Ans: 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.

10. 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.

Ans: 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.

Question 2. Please describe one example in computer security to show that cryptography cannot solve all problems in security. (20 points)

Ans: There could be many different answers. Some examples below:

1. Cryptography can't protect you against human errors
    a. Social engineering is one of the easy one, e.g., steal your passcode by making friends with you.
    b. If you leave your computer unlocked when you go to the bathroom or to get a cup of coffee, somebody can use your computer and do things with your private keys.
2. Cryptography can't protect against most denial-of-service attacks
    a. Cryptography cannot provide availability in general.
3. Cryptography can't protect against stolen encryption keys
    a. The problem of information flow control: cryptography cannot prevent a party authorized to view information from improperly disclosing that information.

Question 3. Encryption usually needs a feature called "Avalanche Effect", which means a small change in the input will cause large changes in the output. In this task we will do some experiments. You will need: (1) a plaintext file you create (not need to be large, 1k byte or so should be fine); (2) an encryption software (e.g., AEScrypt); and (3) a binary editor/viewer (e.g., Hex Fiend for MacOS, Free Hex Editor Neo for Windows). (30 points)

Use the encryption software to encrypt your text file. Then change 1 byte or 1 bit in the text file, encrypt it again. Now use the binary editor to compare the two cipher text files. Are the differences big or small? In your homework submission, you need to attach the screenshots of the text files, and two files opened with the binary editor.

Ans: make sure the screenshots of two files indicate the differences.

Extra question (No extra points): Use your binary editor to change 1 bit in the cipher text file. Then use the software to decrypt. What do you get? Do you get a decrypted file similar to the original text file? Or will the software refuse to decrypt? Why do you think this happens?