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A. Know your threat model: Know your attacker and their resources; the security assumptions originally made may no longer be valid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

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.

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.

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

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

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.

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

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".

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.

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.

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.

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

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). (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.

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?