Contents

Homework 1: Rational Paranoia

Scenario 1. Chez Betty

Assumptions

- $\mathcal{P} \neq \mathcal{NP}$, otherwise all the decryption against encryption are fast to compute.
- We assume people with a valid Mcard (faculty, students and staff) are self-disciplined enough so that they do not intentionally (including helping others) cause loss to Chez Betty.
- We also assume that if at least one people in Chez Betty store has a valid Mcard, then he/she can play a role as a monitor and detect any suspicious behaviors of others. Thus, invaders can only cause loss to Chez Betty when there is no other valid Mcard holders in the store.
- We assume valid Mcard holders will notice the loss of their Mcard shortly and report to the Mcard administration to remove it from the system, so that there is no enough time for those who happen to pick up the lost Mcards.
- The web-based countermeasures does not need to be more secure than `https://weblogin.umich.edu` with two-factor authentication, since otherwise, hackers will try to defeat it instead, and if they success, there is no way to distinguish them from the victims.

Assets

- commodities such as snacks and drinks
- electrical devices such as refrigerators, the check-out computer and the laser scanner
- furniture such as chairs, shelves, sofas, doors, lights, etc.
- the website `https://chezbetty.eecs.umich.edu/` and all its sub-directories
- the Github repository `https://github.com/um-cseg/chez-betty`

Threats

1. The section "Forgot Password?" on the website `https://chezbetty.eecs.umich.edu/login/submit` allow users to reset the password by providing uniqname and UMID. This pair of information is public, especially to those who worked at the university, so the attacker can reset the password for an arbitrary Mcard holder (or even create an account for those who have never visited Chez Betty). The new password will be sent to the corresponding user by email, but it is much weaker. It only contains 6 capital letters, so the total number of possible passwords is $26^6 = 308915776$, which is weak under brute-force trying. If attackers manage to log into the system, then they can see the balance of the account and other information which should have been kept confidential.
2. Currently, the check-out machine still read the user information from the magnetic strip on the MCard. However, magnetic strip is proven to be less secure than chips, since it is easier to clone. Anyone holding an Mcard is under the threat of cloning the Mcards, and it is hard to detect. If an Mcard's magnetic strip is cloned by the attackers, then they can purchase as many things as they want from Chez Betty, and put the victim in heavy debt and shame (the Wall of Shame).

3. The Github repository https://github.com/um-cseg/chez-betty of Chez Betty is public and anyone can clone and push some variations. Attackers can alter the code so that users' information is secretly recorded and sent back to them. Thus, the next time Chez Betty is build from the code on Github, it will not be secure.

4. Attackers can follow a valid Mcard holder to enter the Chez Betty store and wait until no other valid Mcard holders are in the store and steal the objects. Or they can modify the check-out computer so that it secretly records user information and sent back to the attackers.

Countermeasures

1. The reset password sent to the users who claim to have forgotten the password should be longer, and when such a request is received, the server should give only one time for this user to log in. If the user fails to log in, this account should be frozen, and an alert should be sent to the corresponding user, reminding him/her that some malicious user is trying to hack into his/her Chez Betty account. For the users who don't claim to have forgotten the password, a limited times of trying should be given, so that if a wrong combination of uniqname and password is entered too many times, an alert should also be sent to the corresponding user. Also, the administrator of Chez Betty website should also be alerted, so that the attacker's IP address can be traced.

   - Users of Chez Betty can be securely protected by this mechanism, and attackers might be caught and punished.
   - The cost of this countermeasure is very low, since only a counter is needed to add to the login requests. And the Pseudo-random generator of reset password can be enhanced easily.

2. Together with Mcards, the system can ask for uniqname and password through https://weblogin.umich.edu for authentication, just as the Wolverine Access and Canvas do. Then, even if the Mcard is cloned (or even stolen) by an attacker, the attacker cannot use it in Chez Betty. Furthermore, the two-factor authentication can be applied to enhance the security (currently optional for students), since the attacker needs a phone of the victim other than the password and the Mcard.

   - Asking for authentication when placing orders is as secure as https://weblogin.umich.edu, which can be considered as secure based on our assumption.
   - The cost of this countermeasure is also very low, since it rely on the system which is assumed to be secure.

3. The purpose of maintaining Chez Betty website on Github is for everyone to contribute to its construction. But not every part needs to be shown to others. The Chez Betty can be separated to two repositories, one public and one private. The private one contains the core implementation, especially the code related to security. In particular, in website development, JavaScript files which describes the events and actions should kept private. The public repository contains aesthetic part and linguistic part. Thus, contributors can still improve the appearance of Chez Betty's website and translate the contents into multiple languages (which is exactly it desires).

   - This can also be a secure improvement, and it is based on the security of Github.
   - It can be hard to separate, but it is a one-time labor. No further difficulty to the maintenance of Chey Betty website.

4. The university can perform an update of Mcards so that the Mcard also uses chips instead of magnetic strips, just like credit cards.

   - This can bring up all the Mcard holders the security level, which is equivalent to a credit card.
   - The current MCards will be wasted and new Mcards need to be manufactured. Many chip readers need to replace the strip readers. So the cost is very high, but it thoroughly remove the risk of Mcards being cloned.

5. At the door of Chez Betty, Mcard readers can be installed to authenticate users to enter and exit. For the convenience of valid Mcard holders, no uniqname and password pairs are needed. And the store should remind all the customers that they are followed by others to enter the store, then they should monitor the followers until they exit by presenting their own Mcards. If unauthorized users enter the store by following a valid Mcard holder, they will be under surveillance so that they cannot do malicious things to harm the store. Furthermore, cameras should be installed both inside and outside the store to record door. The people who enter and exit the store both by following others will be particularly suspicious when loss is detected.

    - This action turns the valid Mcard holders to security guards (which may be better than cameras), and provide useful information to the detectives when Chey Betty suffer from stealing.
    - Installing card readers and cameras cost some money, and the card reader brings some degree of inconvenience to the valid Mcard holders.

Scenario 2. Law firm document management system

Assumptions

- Some documents stored in the firm are about sensitive legal, financial, or political matters.
- The security level of countermeasures will not be higher than agencies such as CIA, NSA, Pentagon, White House and the Federal Reserve, since the information/property in this firm is less sensitive.
- Managers and employees of the firm are loyal to the firm, so the whistle-blowing of the insider is not considered here.

Assets

- Documents that record client information and case descriptions, and evidence, either in solid (paper) form or in electronic form.
- Human resources such as managers and other employees.
- Technical property such as the building, decorations and office products such as computers.

Threats

1. The employees are under the threat of murder for the revenge of them winning a sue, or being kidnapped in order to ask the law firm to quit a sue.
2. Attackers may pretend to be the clients to enter the firm. Or then even don't need to pretend, since then can actually do business with the law firm, and take a chance to get the information of other clients, which is their real target.
3. If the firm use paper shredder to deal with the paper document waste, the waste can be analyzed to recover the original document.

Countermeasures

1. Employees should get a safeguard or body guard. The higher the position, the more protection, especially for the key layers and managers.
    - This improves the security by some extent, there is no guarantee.
    - This is very expensive, and it also restricts the behavior of the employee.
2. Clients are subject to enforced security check by X-ray scanner and identification at the entrance, just as the passengers needs to board a plane at the airport.

- This reduces the risk of letting armed attackers enter the firm.
- The X-ray scanner are expensive, and it causes some inconvenience for the clients. Privacy issues may occur since the scanner can produce the naked image of human bodies.

3. After the paper documents are shredded, the remainder should also be collected and burnt/dissolved such that the paper is teared apart in the chemical process from the molecular perspective.
   - This can reduce the probability of reconstructing the paper to the original document to reveal the information to a neglectable value ($< 10^{-100}$).
   - This is a common practice, and many agencies use it. It does not cost much, yet improve the security by a lot.

Scenario 3. Pentagon

Assumptions

The Pentagon is under any kind of threat that human beings can make. Here we exclude the security problems caused by natural disasters, such as earthquake, hurricane or thunder.

Assets

- Human resources such as government officials, military commanders, technicians, researchers, and security guards, etc.
- Documents that records national defence projects and other classified information.
- Technical properties such as the building, decorations and office products such as computers.

Threats

1. Terrorists may conduct suicide attacks, such as crashing a plane to the building.
2. Attackers can cut off the power supply so that the defence and surveillance system cannot work properly, and thus they can take a chance to invade.

Countermeasures

1. Missile defence system should be installed around the Pentagon to guard the sky.
   - This is very secure. The Pentagon never suffers from such attacks after 9.11.
   - This cost very much and still can cause damage to surrounding buildings.
2. Backup power supply should be build against the power-off.
   - This is a common practice, but it should also be kept secret so that only very limited officials knows how to activate it.
   - Compare to the national defence budget, this is a cheap system.