Michael Lee

Security Properties and Principles

1. Non-repudiation is the idea that one can't deny their actions, and it falls under the security objective of accountability. It means we can track down a user's actions, possibly with a log file, and given a perfect history they will not be able to refute it.

2. Complete mediation means that there is protection on access to every object in a system. Each time a user needs access they must provide proof of their authority. Separation of privilege is where the authentication process is divided into multiple parts, like in bank deposit boxes: two keys are needed to open any box.

3. Sudo represents the security principle of least privilege, that every action or user should have the minimum access necessary for them to complete their job. This prevents the user from accidently executing commands which could have detrimental effects, unless they force it and provide a password with sudo.

4. Attack surface is the parts of a system that have the potential for attack like a network connection, while vulnerability is the actual weakness within the system that can allow malicious activity.

5. Classify each attack

    a. Shadow Brokers – Confidentiality, user's data was breached.
    b. WannaCry – Availability, the ransomware ruined public utilities
    c. Petya/NotPetya/… - Availability, disrupted public utilities in Ukraine
    d. Wikileaks CIA – Confidentiality, The CIA had the ability to spy on anyone
    e. Cloudbleed – Confidentiality, Cloudflare leaked sensitive customer data
    f. 198 million voter records – Confidentiality, misconfigured server led to data being exposed
    g. Macron Campaign – Confidentiality and Integrity, Macron's emails we're leaked and they claimed not everything was authentic.

User authentication and Passwords

1. Designing a password system
    a. T = N * P / G => (26 + 26 + 10) ^ 7 * .5 / 250000 = 7043229 minutes / (60*24*365) = 13.4 years
    b. Passwords need to be 7 characters long because 6 characters long would only take 78.9 days given the same character set.
    c. This can lower the time it takes for the attacker to correctly guess the user's password because the user needs to be able to remember their password and

common words are vulnerable to dictionary attacks and brute forcing common password.

2. Activating the fingerprint security system wouldn't increase the security of the phone as it would just add another possible vector of vulnerability that the hacker could break into. The hacker only needs the password or the fingerprint sensor and not both to break into the phone. Having a fingerprint doesn't make the password any more secure.

3. You could add more hash indices within the bloom filter to reduce the amount of false positives you receive.

4. The bloom filter will not have false negatives because it will not falsely report that an element is a member of the given set.

5. It's poor practice to store the user's password in clear text because if he knows the user's plaintext password he can use that information to compromise other accounts as they may reuse their password in multiple places.

6. A salt adds an extra layer of security as it's a random string which gets added onto the user's password and computed into the subsequent hash. This means that the hacker can't just use lookup hash tables to match common dictionary words and their hash values to guess a user's plaintext password.

7. The purpose of the salt is to make it harder for a potential hacker to perform dictionary attacks where they match possible passwords to the hashed information that they already know. If they know the salt they could compute their entire table again with the salt in place, but since you usually use a different salt for each password the hacker would have to compute a new table for each salt which would be extremely time consuming. So while the salt might as well be kept secret (there's no reason to bleed the information) it doesn't have to be a secret. Salts allow you to use passwords in several places without being vulnerable and initialization vectors serve a similar purpose with keys. They, IVs, let you use the same key to encrypt different messages without betraying your key. Salts and IVs both add an element of randomness which make things more complex and time consuming for hackers.

8. Empty

9. Multi-factor authentication requires the user to prove their identity multiple times while mutual authentication is when the user has multiple ways to prove who they are, but they system only needs one to let them pass. (don't need to answer/for later)

10. (don't need to answer/for later)