Roman Styrku

ITIS 3200

Assignment 2

Total Marks: 25

Due: 10/17/2018

1. What is password guessing vulnerability? (2 pts)
   - Password Guessing Vulnerability is how vulnerable a password is to being “Guessed” either by a brute force attack or just by someone who knows the account owner. This is the reason why passwords are suggested to have multiple types of characters in random orders instead of just a simple word.

2. Note down at least two issues with password-based authentication. (2 pts)
   - One Issue with Password-Based Authentication is that some users can chose bad passwords without even thinking about it which can result in passwords that are vulnerable to a guessing attack or an implemented brute force attack.
   - A second issue with Password-Based Authentication is that Error Logs can contain “Almost” Passwords. Since one small mistake in a letter will throw an error during a login, if an Attacker checks error logs and finds similar errors, they can use the small typos to figure out the actual password of the user.

3. Describe the steps of rainbow table attack? (2 pts)
   - The steps of a rainbow table attack are Pre-Compute tables of hash values for all salts, A mammoth table of hash values. The attack will then use the possible salts and combine it with possible passwords from the log to find what combination matches the hash of the user’s password that they are trying to crack.

4. What are the advantages of Electronic ID (eID) cards? Do you think privacy can be an issue with an eID card? (3 pts)
   - Some advantages of Electronic ID cards are that they require something the individual has in order to gain access, can use the same purpose as other national ID cards, can provide stronger proof of identity in a wider span of applications, Is a physical card that has been verified by the government.
   - I think that privacy wouldn’t really become an issue with eIDs. I believe that it would end up like a driver license today. You don’t really take it out unless your proving your identification or getting pulled over but its still there. In the same sense even if someone else takes your drivers license, it’s not going to help them much since they still can’t access your information since the picture proof doesn’t match.

5. Is it possible to omit ePass functionality of eID card? Can eSign functionality replace ePass anyway? (3 pts)
   - I don't believe it is possible to remove ePass and replace it all with eSign. If the point of it is to serve as an Identification card, removing the physical side of it would open up too much simpler identity theft and attacks. With the goal being Identity Verification, nothing verifies identity more than physical proof.

6. Note down the authentication security issues? (3 pts)
   - Eavesdropping, Host Attacks, Denial of Service, Trojan Horse, Replay, Client Attacks.

7. How do clearance level and classification level help? (2 pts)
   - Clearance level indicates the level of trust given to a person with a security clearance, or a computer that processes classified information. This helps because it can let you give admin people access to some systems while keeping others access limited from the higher systems.
   - Classification Level indicates the level of sensitivity associated with some information, like a document or computer file. Helps because it lets the admin know the degree of damage that can be caused if the file gets to an enemy, or someone who isn't supposed to see it.

8. Note down the limitations of discretionary access. (3 pts)
   - Global Policy, Information Flow, Malicious Software

9. Describe Bell-LaPadula security policy shortly. (2 pts)
   - Subject (A) is allowed to read object (O) only if class (O) <= class (A)
   - Subject (A) is allowed to write object (O) only if class (A) <= class (O)

10. Write briefly the motivation behind the Chinese wall model? Write about the model intuitively. (3 pts)
    - The motivation behind the Chinese wall model is to make sure that no conflicts of interest arise.
    - A subject S can read an object O if: O is in the same Dataset as an object already accessed by S, or O belongs to a Col class from which S has not yet accessed any information.
    - A subject S can write to an object O if: S can read O according to the read rule, and No object in a different company dataset can be read.