CS 458 A2

Name: Thomas Lim Jun Wei
ID: 20700973

Question 1

Assumptions

- FAR is at 4%
- FRR is at 8%
- Windows of 7 swipes
- 3 swipe if rejection counter hits 3
- Rejection counter reset at 7 swipes
- Tablet is being used by others 9% of the time

1a)

FAR = $\sum_{x=0}^{2} \binom{7}{x} p^x (1-p)^{7-x}$ where p is the possibility of a rejected swipe.

= $\sum_{x=0}^{2} \binom{7}{x} 0.96^x (0.04)^{7-x}$

= 0.000201% (3 d.p.)

FRR = $\sum_{x=3}^{7} \binom{x}{r} p^r (1-p)^{x-r}$

= $\sum_{x=3}^{7} \binom{x}{3} 0.08^3 (0.92)^{x-3}$

= 2.75%

1b) Using Bayes Theorem, P(S | L) denotes probability of stranger locking the tablet within the first 7 steps = 1-0.000201

$P(S|L) = \frac{P(L|S)\,P(S)}{P(L)}$

$= \frac{P(L|S)\,P(S)}{P(L|S)\,P(S) + P(L|A)\,P(A)}$

$= \frac{[(1-0.000201)*0.09]}{[(1-0.000201)*0.09]+(0.91*0.0275)}$

= 78.2%

Question 2

2a)

File 1: None
File 2: Read
File 3: None
File 4: Write
File 5: Both

2b)

i. Professor, {assignments, feedback, exams, marks}, record - (Professor, {feedback, exams, marks})

ii. -

iii. (Student, {feedback, assignments, exams, marks, evaluations}), record - (Student, {feedback, marks, evaluations})

iv. Bob - (Professor, {assignments, exams, marks}), Record - (Professor, {assignments, exams, marks, evaluations})

v. -

Note: - represent no changes.

Question 3

3i)

1) the number combination is only S^6, which is consider too short. Salt combination might let attacker create a rainbow table easily consisting of every possible salt appended to every likely password.

2) Salt should not be stored in the database as this allow attackers with access to database file easy access to decrypt the hashed password.

3) 'Separation of Privilege" can be prevented as the account isn't secure with one level of login authentication.

Solution: Use a longer bit salt and add another form of second level authentication such as letting user to enter a OTP login successfully.

Question 4

4a) Man-in-the-middle attacks where attacker can intercept a communication between two parties within UW network.

4b) This rule prevents denial-of-service attacks from attackers outside the UW network.

4c) From 4B, denial-of-service attacks still can happen if attackers inside of UW network's source address is in the form of 129.97.x.y.

Programming Question

Sploit1

The exploit utilizes the login/confirm.php by logging into another user account when enter the url with an empty hash and entering user 'mmsabri'. Checking onto the user privilege rights. I can use this account to perform a down vote on any articles.

The exploit demonstrated the principle of "Fail-safe Defaults" was violated as login with an empty hash should only return the content sharing portal back to guest account.

Sploit2

This exploit is uncovered when I use this url: http://ugster05.student.cs.uwaterloo.ca/tjwlim/docs/data.db to find the login and hashed password of the portal. By running the passwords against a rainbow table, I am able to recover the un-hashed password by performing a SHA1 decryption. For this exploit. I used the user 'nnasresf' and posted an article on site.

This exploit showed that 'Separation of Privilege" and "Economy of Mechanism" was violated as the database file is not well protected and easily accessed by manipulating the site pages and its caused by poor protection of access path. During the password login, this exploit can be prevented if a second form of login authentication is implemented.

Sploit3

This exploit is a simple SQL injection command inserted at login page using "'or'1'='1" and any random password to force the site to return true in login authentication and for this case, return the first user in the database which is 'fkerschbaum'.

This exploits shows that "Complete Mediation: was violated and user input such as the password wasn't check properly to grant access to login.

Sploit4

This exploit is roughly similar to exploit 2, by chancing onto an old password text file located on http://ugster05.student.cs.uwaterloo.ca/tjwlim/docs/old_passwords.txt . By performing a few tests by inspecting the readable text file, I can login as user 'sdnaksha' and post an article using his account.

This exploit demonstrated that "Economy of Mechanism" is violated as once again, unwanted path is left behind on the site and old password file should not be left behind and in the form of readable format for attacker to utilise.