CS 458 Information Security

Homework 5: User Authentication, SSL/TLS

1. Authentication

(a) iPhone includes a fingerprint scanner which the user can choose (not) to use. Do you think activating fingerprint scanning would increase the security of the cellphone?

Answers may vary. Consider the following points when answering:

- Biometrics has a false positive and false negative rate, especially finger prints.
- iPhone's fingerprint scanner is nowhere near industrially secure level.
- iPhone's fingerprint scanner must be used in conjunction with a password (each reboot requires the user to enter the password before they can use fingerprints again.)

(b) Bloom filter is an efficient way to preemptively reject bad passwords with high efficiency, but it has a false positive rate (incorrectly rejecting good passwords). What can you do to decrease the chance of a false positive?

Bloom filter's false positive rate is approximately $(1 - e^{-kB/N})^k$, so to reduce false positives, we can increase the number of bits used for the hash functions (make hash outputs longer).

Note that Bloom filter will never give a false negative (incorrectly accepting a bad password). Why?

(c) A hotel uses the S/key system to verify if a key card is valid. Alice checks into the hotel and obtains a key card with password $H^{99}(x)$ where H is a secure hash function and x is some constant value. She successfully gets into the room. At this point, Alice's room lock will accept key card(s) with what password(s)?

$H^{99}(x)$ and $H^{98}(x)$.

(d) **Bonus**: In the historical novel Ivanhoe by Sir Walter Scott, jester Wamba said "If anyone says anything to you, just say *Pax vobiscum*". What does *Pax vobiscum* mean?

Peace be with you.

2. Password Security

(a) It is common practice not to store user's password in clear text. However, if an attacker has seized control of the database, he is likely already capable of modifying any user data on the site as an administrator. Why bother hashing the passwords then?

To prevent attacks on password reuse. Many people use the same username and password across multiple sites (even their primary email address and bank account!), so it is important that the compromise of one site does not bring hell to the user

(b) It is common practice to salt the user's password in addition to hashing. What attack does this practice prevent?

To prevent rainbow attack. Without salt, the same password with always be hashed to the same value (with the same hash function), and attackers have made pre-calculated tables for reverse-lookup of common or short passwords. Play with a rainbow table here: https://crackstation.net/ (you can generate hashes here: http://www.fileformat.info/tool/hash.htm)

Caveat Lector! Do not type your real passwords into these websites (especially the latter one). Why?

3. SSL

(a) What is perfect forward secrecy? What's one way to achieve it, as websites today are using?

Perfect forward secrecy means if a session key is compromised, all messages that are encrypted before that message should still be safe.

Websites today usually generate new public/private key pairs for each new session.

(b) IPSec: Which mode includes the IP header inside the encryption, transport mode or tunnel mode?

Tunnel mode.