CSC 437/539 Computer Security

Instructor: Dr. Natarajan Meghanathan

Sample Questions for Module 3 - User Authentication

1) What are the two general steps of an authentication process? Briefly explain them.

2) What is the difference between user authentication and message authentication?

3) What are the four general means of authenticating user identity? Give an example for each.

4) What is a *rainbow table*? What role does it play in attacks on password-based authentication?

5) What are the two common vulnerabilities of password-based authentication? Explain.

6) Explain any three significant countermeasures to mitigate attacks on password-based authentication.

7) How does salting complicate dictionary attacks? Explain the underlying principle.

8) How is salting used in the UNIX-systems during password encryption (DES algorithm)?

9) (a) If a UNIX system publicly displays the 12-bit salt values of each of its 2^{10} users along with the hash values of the 8-character long passwords, compute the average number of attempts needed for an attacker to launch a dictionary attack. Assume the cardinality of the character set of the passwords is 64 and the size of the dictionary of common passwords is 2^{20}. Also, assume that there is a 25% chance that a user password is chosen from the dictionary.
(b) If the UNIX system, described in (a), does not publicly display the salt values, compute the compute the average number of attempts needed for an attacker to launch a dictionary attack.

(10) Describe the standard UNIX-password encryption algorithm (assume salting is used) and explain how the final 13-character encrypted version of the password is obtained. Also, explain the role played by the salt value in the encryption process.

(11) Explain the characteristics of the FreeBSD and OpenBSD systems with respect to their rigor towards password-based authentication.

(12) Determine the user ID, group ID and 12-bit salt value of the username *arlin* based on the following entry information for that user in the UNIX password file.

```
arlin:f8fk3j1OIf34.:182:100:Arlin Steinberg:/u/arlin:/bin/csh
```

(13) Mention two significant reasons for publicly displaying the contents of the *passwd* file in the /etc folder of UNIX systems?

(14) Explain the purpose of the contents of the /etc/passwd and /etc/shadow files in modern UNIX systems.

(15) What is the idea behind the useful of Bloom filters to mitigate dictionary attacks? Explain.

(16) Why is a Bloom filter guaranteed not to generate false negatives? Also, why there could be false positives? Explain.

(17) Explain the impact of the number of hash functions as well as the ratio of the Max. value in the hash table and the # dictionary size on the probability of false positives incurred with the use of a Bloom Filter.

(18) Explain the three forms of token-based authentication in the increasing order of complexity and sophistication.

(19) Explain the role of the three memory components of a smart card: ROM, EEPROM and RAM.

(20) Explain the following three authentication protocols for a smart token:
(i) Static; (ii) Dynamic password generator and (iii) Challenge-response

(21) What is the difference between identification vs. verification in the context of biometric systems? Explain what appropriate biometric traits would you use for each of them.

(22) Rank the following biometric traits in a two-dimensional grids with regards to increasing cost and increasing accuracy:

Face recognition; Hand geometry; Voice recognition; Signature; Iris structure; Fingerprint; Retinal scans

(23) Briefly explain how biometric validations are typically made? (Hint: Hamming Distance)

(24) Explain the choice of the values for the biometric decision threshold for: (i) High-security applications; (ii) Civilian applications and (iii) Forensic applications. Explain the selection of the threshold values with respect to the nature of the operating characteristic curves of the biometric systems as well as the relationship between the probability of false positives and false negatives.

(25) Draw the typical profile for the probability density function of the validation scores for an imposter and a genuine user for biometric systems, and indicate the threshold, false positives and false negatives.

(26) Briefly explain the protocols that were discussed for remote user authentication using each of the schemes:
(i) Password-based authentication
(ii) Smart token-based authentication
(iii) Static biometric system-based authentication
(iv) Dynamic biometric system-based authentication