CSC 438 Systems and Software Security
Module 2 - Systems Security
Instructor: Dr. Natarajan Meghanathan

2.1 Authentication

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

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

3) How does the complexity of successfully launching a dictionary attack increases with the use of salting? Also, how is this complexity impact if the salt values are stored or not stored in the password file along with hashed passwords?

4) Calculate the number of symbols that should be part of a password that is desired to have entropy of 32-bits and the password is randomly chosen from a symbol set of count 128 symbols.

5) Calculate the number of symbols that should be part of a password that is desired to have entropy of 64-bits and the number of entropy bits per symbol of the password is 3.5.

6) Calculate the entropy bits per symbol for a password that is of length 8 symbols and composed of symbols that are randomly chosen from a set of count 64 symbols.

7) (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.

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

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

10) 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.

11) Explain the underlying principle behind the Zero Knowledge Proof Protocol.

12) Under the Zero Knowledge Proof Protocol, if the probability of a user managing to successfully get authenticated, even without knowing the exact password, is ¾ per trial, what is the probability that the user will be detected of not knowing the password in any one of 5 trials?

13) What are the two categories of identifiers/traits used by biometric systems? Give at least two examples for each category.

14) What are the two modes of usage of biometric systems? Explain their underlying principle – pros and cons. Also, give at least two examples for each mode.

2.2 Access Control

1) Differentiate between authentication and access control?

2) Briefly explain about three major access control models that we discussed in the class? Which of these is more scalable and why?

3) Explain the Confused Deputy problem using an illustrative example. Also, justify why C-Lists are preferred over ACLs?

4) State the Bell-LaPadula confidentiality model and the Biba Integrity model.

5) Consider a system with N subjects and M objects. Analyze the time complexity for the following activities for the three access control mechanisms discussed in class: Access Control Lists and Capability Lists and Access Control Matrix.

(a) Ease of determining or changing authorized access during execution for a subject to an object
(b) Ease of adding access permissions for a new subject to the different objects
(c) Ease of creating a new object to which all subjects by default have access.

2.3 File Protection

1) 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.

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

3) 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
```

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

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

6) Explain the concept of SetUserID and SetGroupID in UNIX OS and in what context they are used?

7) What is the purpose of setting each of these bits for a directory: read bit, write bit, execute bit.

8) What is purpose of setting a "sticky" bit for a file and for a directory?

9) Consider a file M.txt. What would be the command and the corresponding options/parameters you would pass to have this file be readable by all users (including the owner and his group), writeable only by the owner, and executable by the owner and group?

10) Suppose there exists an executable file N.exe that is owned by a certain user A who belongs to a certain group. How would you setup the permissions for this file so that any regular user and any group of users can also respectively execute the file with the same privileges that user A and his group has?

11) Briefly discuss the file descriptor vulnerability associated when a parent process forks a child process? New!!

12) What is the purpose of using Symbolic links (in UNIX) and Shortcuts (in Windows)? What is the commonality and difference between them? New!!

2.4 Firewalls and Intrusion Detection Systems

1) Distinguish between three types of network firewalls with respect to their operating principle as well as the nature of attacks and attack packets they could detect and drop.

2) Differentiate between the white list and black list approach of firewalls? What is the tradeoff?

3) Differentiate between signature and anomaly-based IDS. What kind of attacks they could detect? What is the tradeoff?

4) Differentiate between the following terms:
   a) Egress and Ingress filtering of firewalls
   b) Network and Host-based IDS
   c) Active and Passive IDS

5) What is the difference between a proxy and reverse proxy application firewall? Explain with an example.

6) If you are given a sequence of network firewalls (packet filter, stateful and application firewall) and a personal firewall to place between a network to be protected and the Internet, in what sequence would you place them and why? Justify.