Practice Questions for Computer Security

CS370/ECE499

Security Properties and Principles

1. What is non-repudiation and what security property/objective covers non-repudiation?

2. What do the principles of “complete mediation” and “separation of privilege” mean?’

3. Describe the principle exemplified by the practice of using “sudo” instead of always running as a “super user”?

4. Compare and contrast “Attack Surface” and “Vulnerability”

Crypto

1. What is a cipher? What is it used for?

2. What is the difference between a substitution cipher and transposition cipher?

3. Classify the following two ciphers into the two types discussed above: i) rail-cipher, and ii) book cipher

4. Encrypt the following plaintext using Columnar Transposition.
   Plaintext: “COMPUTER SECURITY II PRINCIPLES AND PRACTICES”
   Use keyword “WORD” to determine the width of the transposition and the order of columns.

5. What is a One Time Pad? Encrypt the following plaintext using the provided key as one time pad.
   Plaintext: “COMPUTER SECURITY II PRINCIPLES AND PRACTICES”
   Key: “AXSDJWJHWPNEOIAKANERHQWEYUGASKQPOIASDFMK”

6. With examples give differences between mono and polyalphabetic ciphers. Which ones are easier to crack and Why?

7. Given plaintext NOWISTHEWINTEROF, which of the ciphertexts below result from a columnar transposition (mention all that apply)?
   i. NSWEOTIRWHNOIETF
   ii. NWSHWNEOOITEITRF

iii. NWOIWNITSETRHOEF
iv. MNVHRSGDVHMSDQNE

8. What the difference between a stream cipher and a block cipher?

9. Identify each of the following as: a stream cipher (S), or a block cipher (B).
   a) **[S / B]** One-time pad
   b) **[S / B]** Vigenere cipher
   c) **[S / B]** AES

7. What is the advantage of a stream cipher over a block cipher?

8. What is the advantage of a block cipher over a stream cipher?

9. A good block cipher exhibits *avalanche effect*: if we flip one bit in the plain text, half of the bits are flipped in the cipher text. Two messages of the same length, *m1* and *m2*, differ by 5 bits. With a good block cipher, how many bits differ in the two resulting cipher texts? Assume both cipher texts are *n* bits long.

10. If you are starting a new project that does not depend on other legacy programs, which cipher would you use, 3DES or AES? Justify your answer.

11. Why is DES no longer considered secure? Can we use Double DES (2DES) instead? Why or why not?

12. What is the bit strength of 3-DES when used in Encrypt-Encrypt-Encrypt mode? Explain Why. (Assume the keys are independent)

13. What is an encryption or cipher mode? Name one disadvantage of using ECB mode.

14. What are the advantages of Counter mode over OFB mode?

15. Is it feasible to convert a block cipher into a stream cipher? If yes, give an example.

********** **The following 3 questions may not be relevant for midterm**************

16. What are the three key properties of a cryptographic hash?
    [Bonus]Which of the three properties implies the others. Please explain.

17. What is a birthday attack? Consider a hash function that maps inputs to a 32-bit hash. If an attacker launches a birthday attack, approximately how many steps will it take the attacker to find a collision with a 50% probability of success?

18. What is the difference between a cryptographic checksum and a message

authentication code? What primitive should one use to integrity protect files being transferred on an open channel?

****

User Authentication and Passwords

1. You are designing a password system with randomly selected passwords. The alphabet for the passwords is the set of alphanumeric characters in English both upper and lower case and the integers 0-9. You are told that the attacker can make 250,000 guesses each minute.
    a. If the passwords are 7 characters long, how long until the attacker has a 50% probability of correctly guessing user's passwords in an offline attack.
    b. How long do the passwords need to be to ensure that the 50% success rate is not reached until after 2 years?
    c. If the users select their own passwords, does this affect the relevance of your calculations from parts (a) and (b)? Explain your answer.

2. iPhone 6 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? Why or why not?

3. 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?

4. Why will a bloom filter never give a false negative (accept a bad password)?

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

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

7. Does a "salt" used in password hashing need to be kept secret? Why or why not? Compare and contrast "salts" and "initialization vectors (IVs)" used in CBC encryption mode.

8. What is the difference between multi-factor authentication and mutual authentication?

9. Consider the hash function h(i) = (i + 5) mod 7, and suppose it is used in an implementation of the S/Key protocol. Let the seed be value 0, and suppose that the first password the user returns after the initialization step is 4. What password does the user return on the third login counting the first login password as 4.