CS4920 Final Exam Practice Questions

Dr. Durant – 9 May 2014

- Let M designate a message and T designate an arbitrary time. When followed by subscript numbers, these letters designate specific messages and the time at which each is transmitted.
- Assume everyone knows the correct time and cannot be deceived regarding the current time.
- Assume no 2 messages share the tuple (A,T); that is, no sender 'A' will ever produce more than 1 message having the same time stamp.
- Let | denote the concatenation operator with the item to the left being first and most significant. (This implies a big endian representation.)

Consider the following 4 protocols that specify the format of a message from B to C.

- Protocol 1: M_n | H(S)
- Protocol 2: M_n | T_n | H(T_n | S)
- Protocol 3: M_n | T_n | H(M_n | T_n | S)
- Protocol 4: M_n | T_n | H(S | T_n | M_n)

1. The system described above is only attempting to guarantee one of the CIA properties. Which one?
2. Protocol 1 can be compromised trivially. Briefly describe a scenario in which this happens.
3. Protocol 2 is insecure if an attacker can modify messages. Explain this insecurity in further detail.
4. Protocol 3 solves most (perhaps all) of the remaining problems. Explain why.
5. Protocol 4 can be compromised given the structure of most cryptographic hash functions, whereas protocol 3 cannot. Explain why.
6. Review the articles distributed in class. The final will include copies of these articles if it includes any questions on them. Find them on the website by searching for "[discussed"
7. Secrets & Lies
    a. Chapter 3, Attacks: List 2 differing motivations of attackers and discuss how their objectives, access, resources, expertise and risk differ.
    b. Chapter 5, Security Needs: Describe the concept of "safe harbor" provisions and how they specifically relate to the EU Data Protection Act of 1998 (superseded by the Data Protection Directive after the book was published, but this doesn't change the answer).
    c. Chapter 9, Identification and Authentication.
        i. Discuss the false positive/false negative tradeoff of biometric identification methods. Illustrate with an ROC (receiver operating characteristic) curve.
        ii. Discuss how changes in technology and carefully defining the "secure permitted" have taken fingerprint identification from a joke to a technology widely deployed in 2013 on the iPhone 5s. How do the concepts of rate limiting, live detection, and password fallback fit together into the secure system view?
    d. Chapter 22, Product Testing and Verification:

i. What are some reasons bug bounties fail to work?

ii. How can the principle that OSS is good for security because anybody including experts can inspect and test the code be reconciled with high-profile OSS vulnerabilities like Heartbleed?

e. Chapter 24, Security Processes.

i. Least privilege. Consider a Java program that is vulnerable to receiving unexpected input that causes it to write to an unintended system file and not the intended output file. Give an example of how this principle in particular could have been used to prevent this bug.

ii. Defense in depth. Explain why having 2 firewalls on a corporate network, one for the primary internet connection and one of the backup internet connection, is not an example of defense in depth.

f. Chapter 25, Conclusions. Explain the economic model by which legally enforcing penalties for software vulnerabilities on manufacturers would reduce vulnerabilities. The auto industry can be used as an analogy, and insurance and the principle of security as risk management are key.

8. What is a covert channel? (review the notes for some concepts not discussed in class)
9. What is a control zone?
10. What is a similarity of the 3 types of cryptographic functions (hashes, secret key, and public key)?
11. Briefly define the 3 types of attacks against encryption algorithms (classified by the information known by the attacker).
12. A one-time pad establishes a secret, pseudorandom sequence of bits between sender and receiver. The pad is then XORed with the message to generate the ciphertext. (RC4 is often used to generate one-time pads.)

    a. What is the decryption algorithm?

    b. Describe a ciphertext only attack against a misuse of the one-time pad where the same pad sequence is used for 2 separate messages.
13. Describe why substitution and permutation are useful operations in secret key algorithms.
14. Let H be a cryptographically secure hash function. List the 2 types of hash function attacks that H is not susceptible to.
15. What is an important difference in the behavior of cryptographic hash functions relative to instances of the other 2 types of cryptographic functions? (Noting that a hash has 0 keys is not sufficient.)
16. You receive information encrypted with my private key. You decrypt it with my public key. Anyone could have performed this decryption, though, because no secret was involved. Why, then, would someone encrypt a message using a private key?
17. For messages and keys of the same size, encrypting with a public key is generally much more compute intensive than encrypting with a secret key. Why?
18. What is a standard solution to the above problem?
19. What is the purpose of a mode of operation?
20. Explain how a hash chain can be used to repeatedly prove knowledge of a password in the clear (Lamport's One-Time Password Scheme).
21. What is the purpose of the Diffie-Hellman key exchange algorithm?

22. Hashing passwords: Why should hashes of passwords, not passwords, be stored in an authentication database? What sort of attacks does salting prevent? Assuming a secure channel is established, is it better for the user agent to transmit the password or the hash of the password when performing authentication? Why?
23. Explain how a public key algorithm can be used to authenticate a user. (There are many ways to do this.)
24. What property of finite fields allows RSA and Diffie-Hellman to be secure? (Hint: What mathematical problem cannot be solved more efficiently than with brute force?)
25. Define perfect forward secrecy and explain how it could be implemented in practice.

---

26. List all numbers that can be used when doing arithmetic mod 7.
27. Compute the following results mod 7: 2+3, 4+6, 4+3.
28. What is the additive inverse of 2 when doing arithmetic mod 7?
29. What is the multiplicative inverse of 5 when doing arithmetic mod 7?
30. How many numbers have a multiplicative inverse when working mod 7?
31. Define Euler's totient function, $\phi(n)$.
32. Calculate $\phi(2)$, $\phi(5)$, $\phi(6)$, and $\phi(14)$. Show your work.
33. How many numbers have a multiplicative inverse when working in mod 14?
34. When working mod 14, (at most) how often will the exponentiation table repeat (*i.e.*, what is (the upper bound on) smallest natural number, n, for which $a^b = a^{b+n}$ is always true)? ["at most" and "the upper bound on" are required to make this question technically accurate, but can be ignored in most instances]
35. How many generators (primitive roots) are there when working mod 14?
36. Find one of the generators (test various numbers until you find one that works – show work).
37. State the RSA encryption and decryption algorithms given an n = pq with the standard meaning.
38. State the relationship between e and d (the primary encrypting and decrypting quantities).
39. n is part of the public key. What critical quantity(ies) related to n are kept private?
40. Calculate 6^{3382} working in mod 14. For maximum credit, use all simplification methods covered in class. Show your work.