CS4920 Final Exam Practice Questions

Dr. Durant – 12 May 2010

- 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. When Schneier wrote about stopping internal hackers (WSJ, 2/16/2009), he argued that protecting against internal attacks is an old problem and the old solutions are still sufficient: limit # of trusted people, ensure those trusted are trustworthy (background checks, etc.), limit/compartmentalize trust, give overlapping spheres of trust, detect breaches after the fact/prosecute the guilty.
    a. Discuss these solutions in terms of detective, corrective, and preventative.
    b. Note that surveillance is notably missing from this list. Discuss why given Schneier's philosophy.
7. What is a covert channel?
8. What is a control zone?
9. What is a similarity of the 3 types of cryptographic functions (hashes, secret key, and public key)?
10. Let H be a cryptographically secure hash function. List the 2 types of hash function attacks that H is not susceptible to.
11. 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.)

12. 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?
13. 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?
14. What is a standard solution to the above problem?
15. What is the purpose of a mode of operation?
16. Diagram the generation and use of a Kerberos V4 ticket for establishing a shared secret between users Alice and Bob, with Kerberos server KDC. Alice is the initiating party.
17. What Kerberos construct removes the need for a workstation to remember a user's password for an entire session (or re-prompt for it whenever a new ticket is needed)?
18. Explain how a hash chain can be used to repeatedly prove knowledge of a password in the clear (Lamport's One-Time Password Scheme).
19. What is the purpose of the Diffie-Hellman key exchange algorithm?
20. The standard compilation approach of C/C++ programs allows a stack overrun attack to take place by storing various types of data nearby in the same address space. What are two types of data that are relevantly stored in the same address space, opening up the ability of a stack overrun attack?
21. What often changes between two versions of a compiler (or different optimization settings) that makes exploiting a stack overflow vulnerability difficult?
22. What is different about Java that makes a conforming JVM implementation immune to a stack overflow attack?

---

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