University Of Washington, CSE 590P – Computer Security - Final

Tadayoshi Kohno, John Manferdelli

Due: 6:30pm, March 15, 2007. There are a total of 97 points possible on this final, though you will be graded out of a total of 80 points. That is, there is a possibility of earning 17 points of extra credit. You can pick which problems you answer.

See the course website (http://www.cs.washington.edu/education/courses/csep590b/07wi/) for instructions on how to submit your final. For this assignment, you should submit a PDF file named 'YourLastName-YourFirstInitial-Final.pdf. Please type your name on the first page of your final.

1. (15 points total.) Suppose the State of Washington wishes to start using paperless electronic voting machines for all elections. For simplicity, assume that after manufacturing the voting machines, the maker of the voting machines ships the machines directly to the polling location at which they will be used. Your task is to conduct a risk and threat analysis of this use of paperless electronic voting machines
   - 1.1. (3 points.) Describe three assets for this paperless electronic voting scenario.
   - 1.2. (3 points.) Describe three potential vulnerabilities with this paperless electronic voting scenario.
   - 1.3. (3 points.) Describe three threats to this paperless electronic voting scenario.
   - 1.4. (3 points.) Compute the quantitative risks associated with the above assets, vulnerabilities, and threats. Then describe in English your interpretation of these risks. See page 10 of Gollmann for more information.
   - 1.5. (3 points.) Describe three potential risk mitigation strategies.
2. (12 points total.) There are several key aspects to computer security: prevention, detection, and reaction. (To elaborate on "reaction," recall that the possibility of certain reactions can deter some attacks.)
   - 2.1. (4 points.) Describe two example prevention mechanisms in computer security. Be sure to state at least one asset that each mechanisms is designed to protect and at least one limitation of each mechanism.
   - 2.2. (4 points.) Describe two example detection mechanisms in computer security. Be sure to state at least one asset that each mechanisms is designed to protect and at least one limitation of each mechanism.
   - 2.3. (4 points.) Describe two possible reactions to computer security attacks. Be sure to provide information about the assets/attacks that you are responding to, and at least one limitation of each mechanism.
3. (14 points total.) We have discussed numerous security goals in class. For each of the goals stated below, describe two example applications for which those goals are important.
   - 3.1. (2 points.) Confidentiality.
   - 3.2. (2 points.) Integrity.
   - 3.3. (2 points.) Availability.
   - 3.4. (2 points.) Accountability.
   - 3.5. (2 points.) Non-repudiation.
   - 3.6. (2 points.) Usability.
   - 3.7. (2 points.) Reliability.
4. (8 points.) Alice publishes an RSA public key with n=371011 and e=5. Encrypt the message m=732 to get back a ciphertext c. What is Alice's private key? Prove it by decrypting the ciphertext c to recover m.
5. (7 points.) Suppose p=613. Use El Gamal to encrypt the message m=143 and show how you would decrypt it too. Use 2 as the base for the system but pick your own random a. When you encrypt, you will of course need to pick a b too.
6. (8 points.) This problem revolves around the notion of symmetric "authenticated encryption."
   - 6.1. (4 points.) Explain why it is often very important to not just use a symmetric encryption scheme (which provides privacy alone), but to combine the symmetric encryption scheme with a symmetric message authentication code (which provides integrity). Give two concrete examples of where using traditional encryption alone might not satisfy a system's security goals.

6.2. (2 points.) Describe one *insecure* method for combining a symmetric encryption scheme with a message authentication code. Be sure to explain why this is insecure.

6.3. (2 points.) Describe one *secure* method for combining a symmetric encryption scheme with a message authentication code. Be sure to provide an *informal* description (no mathematical proof) of why this approach might be secure.

7. (4 points.) You are designing a cryptographic protocol for two parties, Alice and Bob, to communicate. Assume that Alice and Bob both share the same secret symmetric AES key K (where K is 128-bits long). And assume that Alice knows Bob's 256-bit RSA public key. If Alice wishes to send an encrypted message to Bob, which should she use: symmetric encryption with a 128-bit key or RSA encryption with a 256-bit key? Justify your recommendation. Your recommendation should be based *only* on security, and not on performance or any other metric.

8. (5 points.) In computer security we often desire random numbers. In class we showed that bad things can happen if the random number generator is *not cryptographically secure*; for example, an attacker could predict other players' cards in an online poker website. Assume that you are developing an application that requires secure pseudorandom numbers. How would you go about generating those pseudorandom numbers? When answering this question, you can choose to answer within the context of your favorite operating system, language, and development environment.

9. (6 points total.) One approach to protecting against buffer overflow attacks is to use a "canary."

   9.1. (3 points.) Describe how the "canary" works. Be sure to state one class of buffer overflow attacks that the canary protects against, and explain why this protection mechanism is successful.

   9.2. (3 points.) Describe one type of buffer overflow attack that the canary does not protect against.

10. (10 points total) Exploring the Access control model. Angela is a security architect designing the next generation access control system. Her requirements include the following: (a) some operations should only be performed by trusted programs, (b) user identity is important but so are groups and roles, (c) hardware is considered secure while users are present but not during repair.

    10.1. (5 points) Sketch an Access Control Mechanism identifying the subjects and objects that will be controlled. Identify how the subjects are authenticated and appointed as well as the default access on objects. Identify the isolation requirements, vulnerabilities and threats to such a system.

    10.2. (2 points) Suppose use time is a potential access control parameter. How would this affect your design?

    10.3. (3 points) Now suppose the Access control system needs to be distributed (i.e.- able to control action on machines that are intermittently connected and in different "trust domains"). Discuss how your system would change and expressly consider how you would "revoke" ore "delegate" permissions previously granted. Again identify the subjects, objects, isolation and authentication requirements.

11. (8 points total) DRM and distributed security

    11.1. (2 points.) Discuss why time-stamping may be a requirement in certificate evaluation and what requirements might be imposed on the integrity, safety and accuracy of the timestamps both in the certificate and at evaluation time. Remember, certificates are evaluated across trust boundaries so there must be some normative standard.

    11.2. (3 points.) Discuss the isolation requirements for DRM and a mechanism for achieving them. Carefully assess attacks, benefits and risk analysis for hardware attacks against an economic return model. Don't forget the role of public policy and enforcement.

    11.3. (3 points.) Suppose your boss is under a lot of business pressure to insure the safety of computer security but is also under a lot of pressure to cut costs. She frequently wants to modify existing systems to achieve a security result. How would you explain the need for simplicity and "whole system" analysis? Can you construct a "compartmentalization" mechanism that help you achieve the simple security promise and allows her to use existing systems?