

Computer Security

Midterm

Fall 2001

Question Sequence

- Chapter - 1 (1 Question 10 points)
 1. Please classify each of the following as a violation of confidentiality, of integrity, of availability or of some combination of those:
 - (a) John copies mary's homework
 - (b) Paul crashes Linda's system
 - (c) Carol changes the amount of Angelo's check from 100to1000
 - (d) Gina forges Roger's signature on a deed
 - (e) Rhonda registers the domain name *AddisonWesley.com* and refuses to let the publishing house buy or use the domain name
 - (f) Henry spoofs Julie's IP address to gain access to her computer
- Chapter - 9 (2 Questions 30 points)
 1. Please prove that DES key consisting of all 0 bits and the DES key consisting of all 1 bits are both weak keys. What are the other two weak keys?
 2. Please describe the following keywords (include diagrams if necessary)
 - (a) Confusion
 - (b) Diffusion
 - (c) Triple DES
 - (d) Meet-in-the-middle attack
 3. Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice's and Bob's public keys.
 - (a) How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either?

- (b) How might Alice and/or Bob detect Eve's subversion of the public keys?
- Chapter - 10 (2 Questions 20 points)
 1. Need questions
 - Chapter - 12 (1 Question 20 points)
 1. Explain how one-time password schemes work. Assuming a one-time password scheme uses Lamport's technique to generate passwords: comment on the following.
 - (a) Explain whether the scheme is compromised if an attacker sniffed a password?
 - (b) How should the attacker proceed to attack this scheme?
 - (c) Where does security of this scheme come from?
 2. On Unix systems why are textitsalts used for? Does using passwords with a salt make attacking a specific account more difficult than using passwords without a salt? Please explain why or why not?
 - Chapter - 13 (1 Question 10 points)
 1. A common technique to inhibit password guessing is to disable an account after three consecutive failed login attempts.
 - (a) Please discuss how this might cause a denial of service attack. Why is this action a violation of the principle of least common mechanism?
 - (b) One can argue that this is an example of fail-safe defaults, because by blocking access to an account under attack, the system is defaulting to a known, safe state. Do you agree or disagree with this argument? Please justify your answer.
 2. The PostScript language describes page layout for printers. Among its features is the ability to request that the interpreter execute commands on the host system.
 - (a) Please describe a danger that this feature presents when the language interpreter is running with administrative or textitroot privileges
 - (b) Please explain how the principle of the least privilege could be used to avoid this danger.
 - Chpter - 14 (1 Question 10 points)
 1. What is a *persona* certificate? Why would anyone use a persona certificate? Give an example.

Extra Questions

1. If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?
2. If one-time pads are provably secure, why are they so rarely used in practice?
3. Explain the principle of least privilege. Which of the following demonstrates violations of this principle? Please justify your answer.
 - (a) *root*, *administrator* accounts in Unix and Windows operating systems
 - (b) A web server running as user *nobody* with read access to the file system