

SOEN 321 MIDTERM FALL 01

1. One computer-system vulnerability that is almost a cliché is: security-critical OS code that does not detect buffer overflow, which occurs when externally-supplied input data overflow the buffer allocated to receive them. Without giving details of how the attack is performed, explain at an abstract level how buffer overflows lead to security compromises.
2. What is the main security risk when users download and install software from the Internet? What is the main security risk if a hacker downloads and installs software "on your behalf" without telling you? (The hacker introduces foreign code into your system).
3. How does the use of a shadow password file affect off-line password-guessing attacks? If you must leave the /etc/passwd file world readable, what are some techniques that make off-line password guessing more computationally expensive?
4. Alice is protecting the data integrity of the files she stores locally on disk. She stores both the files and the hash-function "fingerprint" of each file on disk. Why are there enormous differences in Alice's life if she uses keyed hash functions as opposed to unkeyed hash functions?
5. When hierarchical certificate authorities are used in a public-key infrastructure, the main function they perform is to ...
6. In the STS Protocol version of Diffie-Hellman key exchange, we add digital signatures to the original DH protocol. One version of STS is:
A ---> B: $\alpha^x \text{ mod } p$
B ---> A: $\alpha^y \text{ mod } p, E_k (S_B (\alpha^y, \alpha^x))$
A ---> B: $E_k (S_A (\alpha^x, \alpha^y))$
where E is a symmetric-key encryption function, k is the Diffie-hellman key, and S is a digital signature in some public-key cryptosystem.
Why have we defeated the man-in-the-middle attack on DH? Explain.
7. Why are hash functions typically used in digital signatures?
8. In Unix, system calls are often stored in suid-root files to temporarily give the requesting process more privilege to carry out some task. The Unix designers assumed that this was not dangerous because they assumed that ...