

Information Assurance: Homework 6

Due October 20, 2006

1. Consider attack #2 on RSA digital signatures discussed in section 10.6.2.1 of the text. If the CA enforced that all public key changes much change both the exponent and the modulus of the public key, would this attack be avoided? Why or why not.
2. Show that, under the Yaksha key escrow scheme that Alice can obtain the session key by computing $(C_{\text{Alice}})^{d_A} \bmod n_{\text{Alice}}$.
3. After the initial ESP proposal, reviewers complained that an encryption protocol without integrity verification was not useful. Why is this the case? What harm could a interceptor do in this case? Assume the interceptor has no knowledge of secrets between the IPSec peers.
4. A system allows the user to choose a password with a length of one to ten characters inclusive. Assume that 20,000 passwords can be tested per second. The system administrators want to expire passwords once they have a probability of 0.10 of having being guessed. Determine the expected time to meet this probability under each of the following conditions.
 - a. Password characters must be digits (“0” through “9”).
 - b. Password characters may be capital letters (“A” through “Z”) and numerics (“0” through “9”).
 - c. Passwords are entered using the Elbonian alphabet of 156 characters.
5. Try running the John the Ripper password cracking program <http://www.openwall.com/john/>. You should be able to install it local to your environment for an unprivileged account. Obtain a password file from <http://www.cs.uiuc.edu/class/fa06/cs498sh/hw6/hw6-passwd>. This file contains nine accounts with passwords from a linux system. Four passwords should be cracked very easily. If you have access to a private system, try running the program for a while longer to see if you get more passwords cracked. I will also be posting word lists to the newsgroup that you can use to try to improve the cracking. Submit the account names and passwords that you crack. As long as you get four of the passwords, you will get full credit.
6. A computer system uses biometrics to authenticate users. Discuss ways in which an attacker might try to spoof the system under each of the following conditions.
 - a. The biometric hardware is directly connected to the system, and the authentication software is loaded onto the system.
 - b. The biometric hardware is on a stand-alone computer connected to the system, and the authentication software on the stand-alone computer sends a “yes” or “no” to the system indicating whether or not the user has been authenticated.