Week Five

Assignments

Prior to the next class, be sure to complete the readings specified in Table 1-1.

Source	Reading
NIST [1]	Introduction to Public Key Technology and the Federal PKI Infrastructure NIST SP800-32 Ch 1 Introduction Ch 2 Background Ch 3 Public key infrastructures Ch 4 Issues and risks in CA system operation
Fundamentals of Secure Computer Systems	Ch 13 Intrusion Detection Systems
Cryptography Decrypted	Ch 16 Digital Certificates Ch 17 X.509 Public Key Infrastructure Ch 20 Secure Socket Layer and Transport Layer Security Ch 21 IPSec Overview

Table 1-1 Readings Week Five

In addition to textbook reading assignments, also read the National Institute of Standards and Technology's (NIST), Special Publication SP 800-32 "Introduction to Public Key Technology and the Federal PKI Infrastructure".[1]

While you are reading SP 800-32, please think about the problems that PKI can solve. From your reading, you should learn the major PKI components along with their specific functions. In addition, you should also pay close attention to related PKI trust models, architectures, and processes. When you complete you reading, you should be able to describe certificates, their creation, and their use.

For next week, please answer the following questions.

Questions

1. List and define the four basic security services specified in NIST SP 800-32.
2. What is a cyclic redundancy check (CRC)? Give an example of a CRC application.
3. What is the key management problem? Why is it so difficult?
4. What is a secure hash function?

5. NIST 800-32 defines three classes of security algorithms. It further explains that they are almost always used in concert. Name the algorithms. Explain why they are used in concert.
6. What is a Public Key Infrastructure (PKI)?
7. List and define the major PKI components.
8. List and define two PKI architectures.
9. What are the two basic data structures used by PKI? Explain them.
10. Define and explain X.500 and X.509.

For this class, you will produce a poster. The poster will illustrate how a particular cryptographic service can be applied to organizational process to enhance an organization's security posture. Most posters will have a problem/solution structure. For next week, select a problem that has the potential to make a good focus for your poster and create a problem statement.

Once you have selected a problem, you will create a problem statement. Your problem statement may be several paragraphs long. At a minimum, one paragraph should define that problem. You should also write, at least, one paragraph explaining how appropriate use of cryptography could mitigate that type of problem.

For your journal assignment, find and present several annotated links to references relevant to either the problem, the solution, or a related application. Better essays will include several references.

Be sure to review the NIST readings.

[1] `http://csrc.nist.gov/publications/PubsSPs.html`