Final Exam Preparation Guide

Exam date: Dec. 6, 2011    Time: 12:30~2:30pm

1. Final exam will be close book, close note, 2 hour examination. There will be about 10 problems that you need to answer. 2/3 of the problems aim to test your knowledge on the concepts, the scope of applicability, the security services provided, the security mechanisms used, as well as pros and cons of the security protocols we learned. The other 1/3 of the problem will be focus on the analysis of the protocols and you will be able to demonstrate your ability of applying the principles and techniques in different situation. Similar to the midterm exam, most of the questions need descriptive answers.

2. One page single-sided aid sheet is allowed. Calculators are not needed.

3. The Final exam will focus on the lecture notes after the midterm, namely, we will test mainly on the following topics. Although not explicitly tested, the fundamental concepts we learned before midterm might be required in solving the problems in the final exam.

- Kerberos V4:
  - The function of Kerberos and the security services it provides.
  - Basic configuration.
  - The authentication mechanisms used in Kerberos Authentication - the concepts of KDC, long-term authentication key, session key, ticket, ticket-granting ticket, authenticator, credential, etc. (You need to know the messages exchanged and the major content in the messages)
  - The scalability of Kerberos authentication, the inter-realm authentication mechanism (again, you need to know the messages involved)

- PKI:
  - Concepts of PKI, certificate, chain of trust.
  - Know the configuration of different PKI models, be able to verify a certificate in any of the PKI model.
  - Understand the revocation mechanisms – CRL, OLRS, OLRS certificate.

- IPSec
  - The three protocols in IPSec – AH, ESP, IKE. The security services each protocol provides and the relationship among them
o Concepts of Security Association (database), Security Policy (database), and SPI. How do they work?
o Two modes – Transport mode and Tunnel modes. The difference between the two modes and the suitable application scenarios.
o What process is applied to the packet by AH and ESP (You need to know the processing to the level of header structure)
o Concepts of cookie, stateless cookie, endpoint identity hiding.
o The functions of the two IKE phases, the differences of the two modes of IKE phase 1.
o Understand and be able to explain how the security objectives are achieved in all the 8 IKE protocols – mutual authentication, session key establishment, endpoint identity hiding, and crypto parameters negotiation.

• SSL:
o The security services SSL provides.
o Understand the different mechanisms used in server authentication and client authentication.
o Concept of session resumption
o Compare Kerberos, IPSec, and SSL, understand the different scopes of applicability and implementation locations in TCP/IP protocol stack.