Institut for Matematik og Datalogi
Syddansk Universitet

April 10, 2002
JFB

Computer Security – F02 – Lecture 9

Lecture, March 26

We finished chapter 8, starting with section 8.8 and began on chapter 10 in the textbook, covering up to and beginning the subsection on Kerberos.

Lecture, April 9

We will finish chapter 10 and begin on chapter 12 in the textbook.

Lecture, April 16

We will finish chapter 12 and begin on chapter 11 in the textbook.

Discussion section, April 18

- Do exercise 10.3. You can find a description of KryptoKnight at the following URL:
  ftp://coast.cs.purdue.edu/pub/doc/authentication/kknight.ps.Z
- Read the folowing article, concentrating on the following quesstions:
  ftp://coast.cs.purdue.edu/pub/doc/authentication/kerberos_limits.ps.Z
  - What is challenge/response authentication?
  - What is a one-time password scheme?
  - Suppse that a client wants to access a server in another domain. Are there additional concerns if the client's and server's realms are not directly connected (and must go through intermediate domains to communicate)?
  - What keys get sent in Kerberos protocols? Are they sent securely?
  - Why is the network address included in a ticket?

Announcement

Matalogifest

Information concerning the next Matalogifest, to be held on Saturday, May 4, can be found at

http://www.imada.sdu.dk/∼ jones/matalogi/