INFT 865/INFS 766
SPRING 2000, RAVI SANDHU
SAMPLE QUESTIONS PART 2

1. Explain the architecture of the SSL protocol and the relationship among its various sub-protocols. Very briefly explain whether or not SSL requires the use of a PKI.

2. Explain the trust model and security objectives of the Kerberos protocol.

3. In your opinion what are the three most important extensions in X.509v3 compared to X.509v1. Explain each of these three extensions and why you consider it to be important.

4. The SSL Record protocol applies the following transformations in order: Fragmentation, Compression, MAC, and Encryption. (Some of these may be null transformations.) Discuss why this precise sequence is followed. Is the sequence in IPSEC different? Discuss why.

5. Explain how the ticket-granting service of Kerberos works. In particular show how Kerberos remains a stateless service in spite of having session keys established with possibly hundreds of clients.