

Project Design Document

Introduction to Information Security (266-642)

Due Date: April 10, 2006 (Monday)

This document “the Stallings book” refers to [2] and “the Handbook” refers to [1] (I have linked the Handbook to the class homepage. You can download it for free.)

Reading assignment: Please read section 14.1 from [2]. This section describes the design of Kerberos, an authentication system. You will use section 14.1 as a “template” for your design document. Your design document will have the following sections.

Project grading: The design document is worth 40% of the entire project grade. The final code is worth 60% of the entire project grade. As you can see, we are putting a lot of emphasis on the design document.

Length: The design document should be no more than 6 pages long. Remember that the design document will be used as the basis for your implementation.

1 Describing the entities

This section should describe various entities in your system, such as bank, customer, and merchant, and assign them short names or identifiers, e.g., *B (Bank)*, *C (Customer)*, *M (Merchant)*. These identifiers will be used later in the protocol description.

Example: See Page 405 [2, Chapter 14].

2 Flow of messages in the protocol

Show the flow of messages in the protocol. Make sure the format of the messages and flow is clearly depicted.

Example: For showing the protocol follow the example shown on Page 409, Table 14.1 [2, Chapter 14]. Show the format of each message and the rationale for each message. Follow the example given on Page 410, Table 14.2 [2, Chapter 14].

3 Architecture Diagram

This diagram shows various components of the system and flow of messages between them. This diagram presents an overall view of the system.

Example: Follow the Kerberos overview given on Page 412, Figure 14.1 [2, Chapter 14].

4 Design Review

Each team will be assigned a mentor (usually a graduate student working in security). Make sure that your mentor reviews your document before you submit. Incorporate all the suggestions that you get from the mentor.

References

- [1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.
- [2] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2003.