Course Document for
Introduction to Information Security

Somesh Jha
Computer Sciences Department
University of Wisconsin
Madison, WI 53706.
email: jha@cs.wisc.edu

1 Course Overview

Shared resources, such as the Internet, have created a global-information infrastructure. On the other hand, shared resources also create risks due to intentional or unintentional malicious behavior. *Information security* is the area that deals with protection from and detection of malicious activity. In this course, we will study fundamentals of information security. After the course, a student will have a good understanding of several facets of information security.

2 Syllabus

2.1 Basic Cryptographic Primitives

This part of the course will focus on cryptographic primitives. We will cover the following topics in detail.

- **Symmetric-key encryption:**
  - **Stream ciphers:** Linear/non-linear feedback shift registers.
  - **Block ciphers:** DES and Modes of operations.
- **Public-Key encryption:** We will cover RSA and Elgamal public-key encryption.
- **Hash functions and Data integrity:**
  - Basic properties of hash functions.
  - **Unkeyed hash functions (MDC):** MD4, MD5, SHA-1.

- **Keyed hash functions (MACs):** MACs based on block and stream ciphers. MACs based on MDCs.

- **Digital signatures:**
  - Classification of digital signatures.
  - Digital signatures related to RSA.
  - The digital signature algorithm (DSA).

2.2 Protocols

This section of the course will focus on protocols for various purposes. These protocols use the cryptographic primitives that we discussed in the first part. The protocols that we will discuss are:

- **Key Establishment Protocols:** Kerberos and Diffie-Hellman secret sharing.
- **Web security:** Secure Sockets Layer (SSL).
- **Secure payment protocols:** 1KP and CyberCash.
- **Digital money:** DigiCash.

2.3 System Security

This part of the course will focus on system security.

- **Common system vulnerabilities and attacks:** We will focus on TCP SYN flooding and denial-of-service attacks. Relevant material will be provided at lecture time. A list of vulnerabilities is maintained by the CERT coordination center (their web-page is `www.cert.org`) located at the Software Engineering Institute, Carnegie Mellon University.
- **Firewalls:** We will discuss architecture for firewalls. Firewalls are discussed in [1] and [3]. However, these books are not required. Class notes will be sufficient.
- **Intrusion detection systems:** Various types of intrusion detection systems will be discussed. Intrusion detection systems are discussed in detail in [2]. This book is also not required. If time permits, we will discuss an open-source intrusion detection system *snort* in great detail. Information about snort can be found at `www.snort.org`.

2.4 Special Topics

If there is any time remaining, we will discuss advanced topics such as *elliptic-curve cryptography (ECC)* and *smartcards*.

2.5 Book

The required text for this class is given below.

> W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, Fourth edition, 2006.

I will hand out extra articles and reading material as the class progresses.

3 Grading criteria (Not Finalized)

- **Homeworks (35%):** Short homeworks will be assigned during the class.
- **Exams (40%):** We will have two exams: a mid-term and a final. The two exams will have equal weight.
- **Project (25%):** This will be a significant project related to security. Students will pick one of the three or four projects that we will provide.

References

[1] W.R. Cheswick, S.M. Bellovin, and A. D. Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison Wesley Publishing company, 2003.

[2] S. Northcutt. *Network Intrusion Detection: An Analyst's handbook*. New Riders Publishing, 1999.

[3] E.D. Zwicky, S. Cooper, D.B. Chapman, and D. Russell. *Building Internet Firewalls*. O'Reilly and Associates, 2000.