Course Document for Introduction to Information Security

Somesh Jha
Computer Science 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 creates 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, the student will have a good idea 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:** Modes of operations and DES.
- **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 [2] and [5]. However, these books are not required. Class notes will be sufficient. If time permits, we will discuss a Linux firewall *ipchains* in great detail. Extensive documentation on the firewall ipchains can be found at the following website:
  `http://netfilter.filewatcher.org/ipchains/`.
- **Intrusion detection systems:** Various classes of intrusion detection systems will be discussed. Intrusion detection systems are discussed in detail in [4]. 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 Smartcards

If there is any time remaining, we will discuss architecture and applications of *smartcards*. Java card technology [1] is an environment for building smart card applications.

3 Grading criteria (Not Finalized)

- **Homeworks and paper reviews (30%):** Short homeworks will be assigned during the class. I will also handout reading assignments. For each reading assignment a short report will have to be written. Structure of the report will be provided later.
- **Exams (40%):** We will have two exams: a mid-term and a final. The two exams will have equal weight.
- **Vulnerability analysis presentation and report (10%):** Students will pick a common system vulnerability and analyze it in depth. A short presentation on this material will be given in the class by the students. Students can pick the vulnerability or consult a known database of vulnerabilities (such as `www.cert.org`).
- **Project (20%):** This will be a significant project related to security. Ideally, students will pick something they are interested in. Otherwise, I can suggest some projects. A detailed report and presentation are required for the project. I will prefer that the projects have an implementation component.

References

[1] Z. Chen. *Java Card Technology for Smart Cards: Architecture and Programmer's Guide*. Addison Wesley Publishing Company, 2000.

[2] W.R. Cheswick and S.M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison Wesley Publishing company, 2001.

[3] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

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

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