University of Colorado at Colorado Springs

CS 509: Syllabus

Cryptography and Network Security

TR 12:15-1:30 p.m.

Objective:
Develop an understanding of the security problems that can occur on the Internet, particularly, in the context of electronic commerce performed on the World Wide Web. Understand solutions available: the algorithms and implementations, with particular emphasis on cryptographic techniques.

Instructor: Jugal Kalita (262-3432)
Office: Engineering 178
Hours: MW 9:00-10:00 a.m., F 3:00-4:00 p.m., or by appointment

Text Book & Recommended Books


I will direct you to various Web sites for certain topics, and you should surf the Web also to find relevant sites. If you find a site that is particularly useful, please let me know so I can learn from it as well as the rest of the class.

Here is a list of books that I think would be useful if you want to study on your own. You do not have to buy them.

- *Applied Cryptography*, Second Edition, Bruce Schneier, Wiley, 1996. It is one of the most widely used books on cryptography by computer professionals. It discusses many, many techniques. Does not have mathematical details, but good discussions.

- *Handbook of Applied Cryptography* by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, 1996, CRC Press. It is a dense, hard cover book of about 800 pages. It is reputed to be the “best” book on cryptography in the market today. It is accessible to a large audience, not just the number theory types.


- *Maximum Security* by Anonymous, 1998, SAMS. It is a professional book, but is a great introduction to all topics in security. Very easy to read. It also provides extensive pointers to where freeware, shareware and commercial security tools are available.
• *Web Commerce Technology Handbook* by Daniel Minoli and Emma Minoli, McGraw-Hill. It is also a professional book, and it discusses all aspects of e-commerce security.

• *Web Security and E-Commerce*, Simson Garfinkel, 1997, O'Reilly. It is also a professional book, but covers a lot of topics at a non-theoretical level.


• *Inside Internet Security: What Hackers Don't Want You To Know*, Jeff Crume, Addison-Wesley, 2000. It is a semi-technical book that is very readable.


• *Java 2 Network Security*, by Marco Pistoia, Duane Reller, Deepak Gupta, Milind Nagnur and Ashok Ramani, 1999, Prentice Hall. This covers the same material as the book immediately above.

If I find other books I like during the course of the semester, I will let you know.

**Schedule of Topics**

The following schedule is tentative. I will give out handouts when appropriate.

<table>
<thead>
<tr>
<th>Weeks</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Introduction to security on the Internet and the WWW</td>
</tr>
<tr>
<td>2</td>
<td>Classical cryptographic algorithms</td>
</tr>
<tr>
<td>2</td>
<td>Symmetric algorithms: DES and Variation</td>
</tr>
<tr>
<td>2</td>
<td>Public key cryptographic algorithms.</td>
</tr>
<tr>
<td>2</td>
<td>Hash functions.</td>
</tr>
<tr>
<td>2</td>
<td>Authentication applications, Electronic mail</td>
</tr>
<tr>
<td>2</td>
<td>IP Security and Web Security</td>
</tr>
<tr>
<td>2</td>
<td>Security issues in JavaScript, Perl, Java, etc.</td>
</tr>
</tbody>
</table>

**Grading Scheme:** Home work assignments will count for 30% of the final grade. All home works may not be equally weighted. You will program in Perl or Java, as asked. **It is extremely important that you do not miss any home work assignment.** Midterm will count 20% toward the final grade and final 30%. An individual semester project is worth 15% of the class grade. Class attendance and participation are worth 5% of the grade.

**Note:** If you have special reasons for not being able to hand in an assignment on time or take an examination on a scheduled date, please make prior arrangements with the instructor. You cannot take a missed exam later without prior permission.