Course Description

The goal of the course is to present and explain formal and technical aspects of computer security on examples of real world systems and thus enable the student to relate theoretical approaches and technical implementations to the security requirements of the problem domain.

The course provides an in-depth presentation of security issues in computer systems, networks, and applications. Formal security models are presented and illustrated on operating system security aspects, more specifically memory protection, access control and authentication, file system security, backup and recovery management, intrusion and virus protection mechanisms. Application level security focuses on language level security and various security policies; conventional and public keys encryption, authentication, message digest and digital signatures. Internet and intranet topics include security in IP, routers, proxy servers, and firewalls, application-level gateways, Web servers, file and mail servers. Discussion of remote access issues, such as dial-up servers, modems, VPN gateways and clients.

Prerequisites

Prior knowledge of computer programming, operating systems and communications networking is assumed. General experience in working with a computer system, its operating system and applications is necessary. Java, DCE, .NET, unix/linux experience useful.

Course Learning Objectives

Upon successful completion of this course you will be able to:
- Understand and be able to discuss the general concepts of information security governance and the importance of balancing the use of security policy, processes, technology and operations to mitigate organizational security risks.
- Develop detailed security requirements based on market/business needs, threat profiles, security policy obligations and asset vulnerabilities/exposure.
- Perform asset assessments, determine probable threats and risks that drive solution architectural alternatives, trade-off studies, modeling and design issues.
- Prepare service/product security architectures and designs that sufficiently comply with enterprise security requirements thereby minimizing risks to acceptable cost levels.
- Plan operational security procedures, ensure operations security activities comply with policy, along with conducting periodic security reviews and audits.
- Support product/service development, integration and procurement activities ensuring that selected components, when deployed, will comply with the organizational detailed security requirements.
Course Outline


Lecture 5 - PKI Continued, Computer Security Related Hardware, Processor States and Status, Memory and Address Protection, The Security Kernel and Rings of protection, Network Models, Data Link Layer complexity.

Lecture 6 – ARP, DHCP, MPLS, LANs, MANs, WANs, IP and the network Layer, Transport Protocols, Unix Type OS Security Capabilities.


Lecture 9 - Layer 2 Network Security mechanisms (802.1q, 802.1x, 802.1i), Layer 3 Network Security mechanisms (IPsec)

Lecture 10 - Layer 3 Network Security mechanisms (IPsec, Firewalls, Intrusion Protection), Layer 4 Network Security mechanisms (TLS, SSL, DTLS, SSH), Application Layer Network Security mechanisms (Email)


Lecture 12 - Security of Network Services (DNS, NTP, Active Directory), Penetration Testing, Network and Security management. NGOSS and eTOM.

Lecture 13 – Operational Security Compliance, Course Review

Lecture 14 - Final Examination
Schedule
The class schedule for Spring 2011 MET CS695 A1 is:

<table>
<thead>
<tr>
<th>Date</th>
<th>Class</th>
<th>Date</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/24/11 (Mon)</td>
<td>Class 1</td>
<td>3/21/11 (Mon)</td>
<td>Class 8</td>
</tr>
<tr>
<td>1/31/11 (Mon)</td>
<td>Class 2</td>
<td>3/28/11 (Mon)</td>
<td>Class 9</td>
</tr>
<tr>
<td>2/7/11 (Mon)</td>
<td>Class 3</td>
<td>4/4/11 (Mon)</td>
<td>Class 10</td>
</tr>
<tr>
<td>2/14/11 (Mon)</td>
<td>Class 4</td>
<td>4/11/11 (Mon)</td>
<td>Class 11</td>
</tr>
<tr>
<td>2/22/11 (Tue)</td>
<td>Class 5</td>
<td>4/21/11 (Thu)</td>
<td>Class 12</td>
</tr>
<tr>
<td>2/28/11 (Mon)</td>
<td>Class 6</td>
<td>4/25/11 (Mon)</td>
<td>Class 13</td>
</tr>
<tr>
<td>3/7/11 (Mon)</td>
<td>Class 7</td>
<td>5/2/11 (Fri)</td>
<td>Final Exam</td>
</tr>
</tbody>
</table>

Course Materials

Required Course Book
None

Methods of Instructions
The class sessions will be conducted in the lecture format once a week (see course schedule for possible exceptions). The mandatory components of the course work include class attendance, weekly on-line reading assignments, submitting homework assignments on time and taking the on-line midterm and proctored final exams.

Evaluation and Grading
You will have to do homework assignments to help you master the material. You will also have to read the textbooks and to be ready to discuss the issues related to the current class topics.

Grades will be based on:
- Weekly homework assignments (30%),
- Weekly in-class quizzes (30%),
- Weekly class participation (5%) and
- Final examination (35%).

Grading criteria for the homework assignments, 2 quizzes and the final exam include your ability to understand course concepts and their relationships.

Homework assignments and quizzes are mandatory. Their timely and satisfactory completion is an absolute requirement for receiving any credit for this course.
Grade ranges are as follows:
• A 94 - 100%
• A- 90 - 93%
• B+ 87 - 89%
• B 84 - 86%
• B- 80 - 83%
• C+ 77 - 79%
• C 74 - 76%
• C- 70 - 73%
• D 60 - 69%
• F < 60%

==============================================

**Homework Assignments**

Homework assignments are mandatory. Their timely and satisfactory completion is an absolute requirement for receiving any credit for this course. Homework assignments are required to be submitted via the “Student DropBox” under “Student Tools” within the Blackboard page for this course (CS695s B1 Enterprise Information Security (Fall 2010)) no later than mid-night of the evening prior to the next class.

Assignments should be typed, no more than 4 pages in length. Please use a type font no smaller than 12 point Times Roman, 1” margins on all sides. Also ensure that your name is included within the document and also part of the document file name. **Word 2003** is the required file format.

File names for assignment documents should be:

CS695-HW<number>-<student last name>-<student first name>.doc

where:

<number> = 1, 2, 3, 4, 5, 6, 7, 8, 9, or 10

An example assignment file name is:

CS695-HW5-Jacobs-Stuart.doc

All assignments will be identified on the last page of each week's lecture notes along with a due date. Assignments submitted after mid-night of the night that homework is due will have 3 points deducted for each 24 hours late.

==============================================

**Examinations**

There will be weekly in-class quizzes and an in-class proctored final exam.

The proctored final exam will be held in class on Tuesday 12/7/2009 and last 3 hours. This exam is open book/notes but no electronic resources allowed.
If the final will be missed it will be the responsibility of the student to arrange with the professor a mutually agreeable schedule for completion of work.

If any work is to be completed beyond the scheduled dates of this course the student must negotiate a Boston University "Contract for an Incomplete Grade" with the professor.

You will have to do homework assignments to help you master the material. You will also have to read the textbooks and to be ready to discuss the issues related to the current class topics.

=====================================================

**Academic Honesty**

The course is governed by the Academic Conduct Committee policies regarding plagiarism (any attempt to represent the work of another person as one’s own). This includes copying (even with modifications) of a program or segment of code. You can discuss general ideas with other people, but the work you submit must be your own. Collaboration is not permitted.

=====================================================

**Instructor Information**

Instructor: Stuart Jacobs, MSc, CISSP  
Office hours: By Appointment  
Office Address: 808 Commonwealth Ave., Room 250. Boston, MA 02215. E-mail: sjjacobs@bu.edu

=====================================================

**Instructor Biography**

Stuart Jacobs

Computer Science Department Metropolitan College Boston University 808 Commonwealth Ave, 2nd floor Boston, MA 02215

Email: sjjacobs@bu.edu

Mr. Jacobs obtained his MSc in Applied Statistics and Educational Research, Southern Connecticut State University, New Haven CT and BA in Computer Science, University of Wisconsin Madison. He has over 35 years of industry experience and was principal investigator for the design of an autonomous agent distributed vulnerability analysis system and a Mobile IP prototype using public key cryptography.

Mr. Jacobs served as the lead Security Architect at Verizon Corp. where his responsibilities include security architecture, requirements development and standardization activities, including serving as Verizon's security subject matter expert to ANSI-ATIS, ITU-T, TMF, OIF and IETF. Previously Mr. Jacobs served as a Systems Engineer and network architect at GTE Government Systems Inc. where he was responsible for research and development on numerous strategic and tactical US military communications systems ranging from submarine deployed high data rate satellite base stations to NORAD early warning communication systems. Mr. Jacobs also performed telecommunications engineering on network management architectures and developed course materials on security, networking and network management. Now, as an adjunct faculty member, he teaches courses in Computer and Communications Security.
Non-required textbooks and references good for further study

The following books are NOT required for this course. However you will find each to be valuable resources to anyone involved in the Information Security area.


**Firewalls and Internet Security**, Repelling the Wily Hacker, William R. Cheswick, and Steven M. Bellovin, Addison-Wesley, 1994 *This book is a classic for its very detailed treatment for statefull firewalls and DMZs and is still relevant today.*


**Computer Related Risks**, Peter G. Neumann, Addison-Wesley, 1995 *This book is one of the definitive texts on the basic concepts of what constitutes risks, especially information security risks.*

**Applied Cryptography**, Bruce Schneier, 2nd Edition, Wiley & Sons, 1996 *This book is an excellent source for details on most any encryption algorithm you are likely to encounter. Most any version, starting with the 2nd edition, will be invaluable.*

**Computer Security**, Dieter Gollmann, 2nd ed, John Wiley, 2006 *This book provides depth coverage of computer security and is highly recommended.*