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

Lecture 13 – Operational Security Compliance and 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>
</tr>
</thead>
<tbody>
<tr>
<td>9/10/12 (Mon)</td>
<td>Class 1</td>
</tr>
<tr>
<td>9/17/12 (Mon)</td>
<td>Class 2</td>
</tr>
<tr>
<td>9/24/12 (Mon)</td>
<td>Class 3</td>
</tr>
<tr>
<td>10/1/12 (Mon)</td>
<td>Class 4</td>
</tr>
<tr>
<td>10/9/12 (Tue)</td>
<td>Class 5</td>
</tr>
<tr>
<td>10/15/12 (Mon)</td>
<td>Class 6</td>
</tr>
<tr>
<td>10/22/12 (Mon)</td>
<td>Class 7</td>
</tr>
<tr>
<td>10/29/12 (Mon)</td>
<td>Class 8</td>
</tr>
<tr>
<td>11/5/12 (Mon)</td>
<td>Class 9</td>
</tr>
<tr>
<td>11/12/12 (Mon)</td>
<td>Class 10</td>
</tr>
<tr>
<td>11/26/12 (Mon)</td>
<td>Class 11</td>
</tr>
<tr>
<td>12/3/12 (Mon)</td>
<td>Class 12</td>
</tr>
<tr>
<td>12/10/12 (Mon)</td>
<td>Class 13</td>
</tr>
<tr>
<td>12/17/12 (Mon)</td>
<td>Final Exam</td>
</tr>
</tbody>
</table>

Dates in this color identify sessions where the A1 and EL sections both meet on campus (TBD at this time)

Course Materials

Required Course Book


Methods of Instructions

On-campus session will be held in MET CS dept. computer Lab 2 near the dept office in the Fuller Bldg. 808 Commonwealth Ave. Not in room 133 of the Fuller bldg. (808 Commonwealth Ave.

There will be Wimba classroom sessions for both sections to join

Both sections are expected to use Vista:

- for reading assignments beyond text book assigned reading,
- Submitting homework assignments
- Taking on-line quizzes,
- Participating in discussion threads
- Taking the on-line final examination and practice final exam
Both sections are expected to

- Complete joint on campus session exercises

Section A1 (on-campus)

There will be weekly face-to-face meeting sessions on campus in Computer Lab 2 (see course schedule for possible exceptions).

Section EL blended

There will be four face-to-face meeting sessions on campus in Computer Lab 2 (see course schedule for possible exceptions) The dates for these required EL sections are TBD at this time.

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

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:

- bi-weekly home work assignments (25%)
- bi-weekly quizzes (25%)
- combined session in-class exercises (10%)
- class and Vista discussion thread participation (5%)
- proctored final exam (35%)

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 Vista for this course no later that 
mid-night (12:00 AM) the day due.

• For each day after the date a homework assignment is due will result in a penalty of 3 
points.

• Homework passed in that is over 5 days late will receive a grade of zero (0).

• All assignments will be identified on the last page of each week's lecture notes and its 
due date.

• File names for assignment documents should be:

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

      An example assignment file name is:

      CS695-HW5-Jacobs.doc

• Assignments must be typed, no more than 4 pages in length, use 12 point Times Roman 
type font, 1” margins on all sides

• Include your name and assignment number in the header and a page number in the footer 
of your assignment submission document

• Title cover pages are not required

• Assignment submission documents MUST be in Word 2003 or Word 2007 file formats 
that are NOT encoded in XML.

• Quoted material and citations must follow the American Psychological Association 
(APA) format with a reference section at the end of each document that includes citations 
or quotations.

• Wikipedia is NOT an acceptable source.

Examinations

The proctored final exam will be held in class on Monday 6/7/2012 and last 3 hours. This exam 
is open book/notes but no electronic resources allowed.

A practice final exam will be available on Vista which can be taken as many times as a student 
wishes.

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**

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

**Email:** sjjacobs@bu.edu

Mr. Jacobs’ CV is available on Vista under Course Information
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.


This book is very useful should you decide to sit for the CISSP examination to prepare you for the style and level of detail of questions in the six hour exam.

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.


This book is a classic for its very detailed treatment of general networking security and hardening of unix typs operating systems and is still relevant today.


This book provides an interesting look into those involved in malware and some of the techniques used for breaching targeted systems.


This book is an interesting collection of discussions on security engineering and associated challenges.

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.


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.


This book provides depth coverage of computer security and is highly recommended.


This book provides depth coverage of network security and is highly recommended.