COURSE OUTLINE
Elec 567 – Advanced Network Security and Forensics
Spring 2014

Instructor:
Dr. Issa Traore
Phone: 250-721-8697
E-mail: itraore@ece.uvic.ca

Office Hours:
Days: Monday, Thursday
Time: 10:30am-12:00pm
Location: EOW 415

Lectures:
A-Section(s): A01 / CRN 21146
Days: Monday, Thursday
Time: 8:30-10:00am
Location: ECS 130

B-Section(s)

Labs: No lab
Location: ELW

Required Text:
Title: Computer Network Security
Author: Jie Wang
Publisher: Springer
Year: 2009

Optional Text:
Title:
Author:
Publisher:
Year:

References:
3. Lectures Notes available on Moodle

Assessment:
Assignments: 15%
Project: 45% (22.5-22.5%)
Mid-term Exam: 35%  Date: March 24/2014
Attendance and Participation: 5%
Final: no final exam

Note: Failure to complete all laboratory requirements will result in a grade of N being awarded for the course.

Due dates for assignments:
1. Assignment: due February 3/2014
2. Project Part I: due February 24/2014
3. Project Part II: due April 3/2014
4. Mid-term Exam: March 24/2014
The final grade obtained from the above marking scheme will be based on the following percentage-to-grade point conversion:

<table>
<thead>
<tr>
<th>Passing Grades</th>
<th>Grade Point Value</th>
<th>Percentage for Instructor Use Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>9</td>
<td>90 – 100</td>
</tr>
<tr>
<td>A</td>
<td>8</td>
<td>85 – 89</td>
</tr>
<tr>
<td>A-</td>
<td>7</td>
<td>80 – 84</td>
</tr>
<tr>
<td>B+</td>
<td>6</td>
<td>77 – 79</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
<td>73 – 76</td>
</tr>
<tr>
<td>B-</td>
<td>4</td>
<td>70 – 72</td>
</tr>
<tr>
<td>C+</td>
<td>3</td>
<td>65 – 69</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>60 – 64</td>
</tr>
<tr>
<td>D</td>
<td>1</td>
<td>50 – 59</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Failing Grades</th>
<th>Grade Point Value</th>
<th>Percentage for Instructor Use Only</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>0</td>
<td>35 - 49</td>
<td>Fail, conditional supplemental exam. (For undergraduate courses only)</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>0 – 49</td>
<td>Fail, no supplemental.</td>
</tr>
<tr>
<td>N</td>
<td>0</td>
<td>0 – 49</td>
<td>Did not write examination, Lab or otherwise complete course requirements by the end of term or session; no supplemental exam.</td>
</tr>
</tbody>
</table>

The rules for supplemental examinations are found on page 80 of the current 2013/14 Undergraduate Calendar.

<table>
<thead>
<tr>
<th>Term in which E Grade Was Obtained</th>
<th>Application Deadline for Supplemental Exam</th>
<th>Supplemental Exam Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>First term of Winter Session</td>
<td>February 28 in the following term</td>
<td>First week of following May</td>
</tr>
<tr>
<td>Second term of Winter Session</td>
<td>June 30 in the following term</td>
<td>First week of following September</td>
</tr>
<tr>
<td>Summer Session</td>
<td>October 31 in the following term</td>
<td>First week of following January</td>
</tr>
</tbody>
</table>

Deferred exams will normally be written at the start of the student’s next academic term; i.e., approximately 4 months following the deferral of the exam.

**Course Description**

**Course Objectives**

The purpose of the course is to introduce fundamental concepts and techniques underlying the science and art of computer security, with a particular emphasis on network security vulnerability assessment and forensics investigation techniques. Examples of attack techniques and tools are introduced, as well as adequate countermeasures against these attacks.

**Learning Outcomes**

By the end of this course, students should have a good grasp of network vulnerability assessment and...
forensics investigation techniques, as well as secure architecture design and related technologies.

**Syllabus**

**Unit 1: An Overview of Computer Security**
- Ethical issues.
- Introduction of fundamental security principles and concepts.

**Unit 2: Network Attacks and Penetration Testing**
- Review of attack methods and tools
- Generic penetration testing methodology
- Port scanning, denial of service, attack on authentication system, and input validation attacks, web application vulnerabilities (e.g. SQL injection, Cross-Site Scripting, Directory traversal) etc.

**Unit 3: Malicious Logic**
- Trojan horses
- Rootkits
- Viruses
- Worms
- Botnets

**Unit 4: Security Policies**
- Notions and examples of security policies and models: Bell-LaPadulla, Biba, Chinese Wall etc.
- Basic access control model, reference monitor concept, security kernel.
- Role-based access control model.

**Unit 5: Firewall Systems**
- Classes of firewall
- Firewall configurations and architectures
- Network Address Translation (NAT)
- Linux IP Tables

**Unit 6: Intrusion Detection Systems (IDS)**
- IDS models, architectures, and tools
- IDS performances

**Unit 7: Network Forensics**
- Forensics Logs
- Investigation of hacking incidents

**Unit 8: Computer Forensics**
- Investigative Techniques
- Linux-based Forensics Analysis
- Windows-based Forensics Analysis

**Unit 9: Mobile Devices and E-mail Forensics**
- E-mail artifacts identification and conversion
- E-mail forensics analysis
- Mobile device evidence
- Analysis of mobile devices evidence

**Unit 10: Virtual Private Network (VPN)**
- Network Layer Security
- IPSec protocol
- VPN Technology
- Secure Network Architecture

**Note to Students:**
Students who have issues with the conduct of the course should discuss them with the instructor first. If these discussions do not resolve the issue, then students should feel free to contact the ECE Chair by email or the ECE Chair's secretary to set up an appointment.
Accommodation of Religious Observance
See http://web.uvic.ca/calendar2013/GI/GUPo.html

Policy on Inclusivity and Diversity
See http://web.uvic.ca/calendar2013/GI/GUPo.html

Standards of Professional Behaviour
You are advised to read the Faculty of Engineering document Standards for Professional Behaviour at http://www.uvic.ca/engineering/current/undergrad/index.php#section0-25 which contains important information regarding conduct in courses, labs, and in the general use of facilities.

Cheating, plagiarism and other forms of academic fraud are taken very seriously by both the University and the Department. You should consult http://web.uvic.ca/calendar2013/FACS/UnIn/UARe/PoAcI.html for the UVic policy on academic integrity.

**Plagiarism detection software may be used to aid the instructor and/or TA's in the review and grading of some or all of the work you submit.**