ICS 121 Course Syllabus
Computer Security
Information and Computer Sciences
Windward Community College
Spring 2017

Instructor: Dave Stevens
Email: david.stevens@hawaii.edu
(Student should expect a response to their email within 24 hours, excluding weekends and holidays)

Classroom: WW
Meeting Time: by arrangement
CRN: 64437

Supplemental Materials:
- Currently registered University of Hawai‘i – WinCC students are eligible for a free subscription to MS Office 365 University for Windows, Mac, iOS, and Android.
- MS Office 365 University includes: Word, Excel, PowerPoint, OneNote, OneDrive, and more!
- Licensed users may install and run Office on up to 5 devices (virtual machines count as a device).
- Click here to register for MS Office 365 University using your “hawaii.edu” email account.

Dreamspark:
- You should have received an email from the WinCC IT team for membership on the Microsoft Imaging website.
- This website is where you can obtain free software for your WinCC experience.
- Please, follow the instructions to sign up asap.
- If you have not received this email, please let me know immediately!

Office Hours:

<table>
<thead>
<tr>
<th>Mon / Wed.</th>
<th>3 – 4pm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tues / Thurs</td>
<td>4:30 – 5:30pm</td>
</tr>
<tr>
<td>Fri</td>
<td>By appointment only</td>
</tr>
</tbody>
</table>

Office: Kapi‘olani Community College – Kōpiko 116
Office Phone: 734-9843
Office Fax: 734-9147
This is a shared fax machine:
- Please include your name and mine on any transmitted documents.
- Please do NOT include personally identifiable information (PII)

Required textbook:
Mark Ciampa
Course Description: ITS 122 introduces fundamental cyber security concepts. This course covers the fundamentals of risk management, cryptography, incident response and recovery, access control, authentication, types of attackers and attacks, and countermeasures. Students sometimes choose to take the CompTIA Security+ certification test following completion of this class because of the large overlap between this course and the Security+ exam objectives.

Course Objectives: Upon successful completion of ITS 122, the student should be able to:

- List the first principles of security and describe why each principle is important to security and its relationship to the development of security mechanisms and security policies.
- Describe why good human machine interfaces are important to system use, the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.
- Analyze common security failures and identify specific design principles that have been violated, and the needed design principle, when given a specific scenario.
- List the fundamental concepts of the Information Assurance/Cyber Defense discipline and describe how they can be used to provide system security.
- Identify the elements of a cryptographic system and describe the differences between symmetric and asymmetric algorithms, which cryptographic protocols, tools and techniques are appropriate for a given situation, and implementation issues.

Grading:

<table>
<thead>
<tr>
<th>Graded Item</th>
<th>Points Per Item</th>
<th>Total Points</th>
<th>Range</th>
<th>Class Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projects (x15)</td>
<td>1</td>
<td>15</td>
<td>90 – 100</td>
<td>A</td>
</tr>
<tr>
<td>Netlabs (x20)</td>
<td>1</td>
<td>20</td>
<td>80 – 89</td>
<td>B</td>
</tr>
<tr>
<td>Quizzes (x4)</td>
<td>5</td>
<td>20</td>
<td>70 – 79</td>
<td>C</td>
</tr>
<tr>
<td>Mid-Term</td>
<td>20</td>
<td>20</td>
<td>60 – 69</td>
<td>D</td>
</tr>
<tr>
<td>Final</td>
<td>20</td>
<td>20</td>
<td>below 60</td>
<td>F</td>
</tr>
<tr>
<td>eCafe survey</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Lecture videos:

Lecture videos, from the books author, are available at this website: [http://community.cengage.com/Infosec2/w/lecture-videos](http://community.cengage.com/Infosec2/w/lecture-videos)

The videos are hosted on a private Youtube.com channel. So, you’ll have to sign up for the Cengage Infosec website to watch the videos.

Individual lecture video links (note: You must be signed into the website for these links to work!)

- [Chapter 1 - Introduction to Security](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 2 - Malware and Social Engineering Attacks](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 3 - Application and Networking Based Attacks](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 4 - Application, Data, and Host Security](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 5 - Basic Cryptography](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 6 - Advanced Cryptography](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 7 - Network Security Fundamentals](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 8 - Administering a Secure Network](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 9 - Wireless Network Security](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 10 - Mobile Device Security](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 11 - Access Control Fundamentals](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 12 - Authentication and Account Management](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 13 - Business Continuity](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 14 - Risk Mitigation](http://community.cengage.com/Infosec2/w/lecture-videos)
- [Chapter 15 - Vulnerability Assessment](http://community.cengage.com/Infosec2/w/lecture-videos)

Class Schedule:
<table>
<thead>
<tr>
<th>Week #</th>
<th>Objectives</th>
</tr>
</thead>
</table>
| Week 1      | **Topic(s):**  
  - Challenges of Securing Information  
  - What is Information Security?  
  - Who are the Attackers?  
  - Attacks and Defenses  
  **Reading:**  
  - Chpt 1 – Introduction to Security  
  **Homework:**  
  - Log into MS Office 365  
  - Log into Netlab / Change Password  
  - Log into MS Imagine / Change Password  
  - Netlab – Lab 13: Mitigation and Deterrent Techniques – Password Cracking  
  - Project 1-3: Create a Windows Virtual Machine, for Security Testing Part 1  
    - Pgs. 37 – 39  
    - Uses Windows 10, from MS Imagine, instead of Windows 8.1  
  - Project 1-4: Create a Windows Virtual Machine, for Security Testing Part 2  
    - Pgs. 39 – 40 |
| Jan. 23rd – Jan. 29th |                                                                                                                                 |
| Week 2      | **Topic(s):**  
  - Attacks Using Malware  
  - Social Engineering Attacks  
  **Reading:**  
  - Chpt 2 – Malware and Social Engineering Attacks  
  **Homework:**  
  - Netlab – Lab 9: Analyze and Differentiate Types of Malware  
  - Project 2-1: Write Protecting and Disabling a USB Flash Drive  
    - Pgs. 81 – 83 |
| Jan. 30th – Feb. 5th |                                                                                                                                 |
| Week 3      | **Topic(s):**  
  - Application Attacks  
  - Network Based Attacks  
  **Reading:**  
  - Chpt 3 – Application and Network Based Attacks  
  **Homework:**  
  - Netlab – Lab 10: Analyze and Differentiate Types of Attacks Using Windows Commands  
  - Netlab – Lab 11: Analyze and Differentiate Types of Application Attacks  
  - Project 3-1: Scan Web Browser Plug-ins  
    - Pgs. 125 – 126 |
<p>| Feb. 6th – Feb. 12th |                                                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Week 4</th>
<th>Topic(s):</th>
</tr>
</thead>
</table>
| Feb. 13th—Feb. 19th | - Securing the Host  
- Securing the Static Environments  
- Application Security  
- Securing Data |
| Reading: | - Chpt 4 – Host, Application, and Data Security |
| Homework: | - Netlab – Lab 15: Importance of Data Security – Data Theft  
- Project 4-2: Setting Windows Local Security Policy  
  ○ Pgs. 173 – 174 |

<table>
<thead>
<tr>
<th>Week 5</th>
<th>Topic(s):</th>
</tr>
</thead>
</table>
| Feb. 20th—Feb. 26th | - Defining Cryptography  
- Cryptographic Algorithms  
- Using Cryptography |
| Reading: | - Chpt 5 – Basic Cryptography |
| Homework: | - Netlab – Lab 19: General Cryptography Concepts  
- Project 5-1: Using OpenPuff Steganography  
  ○ Pgs. 216 – 218 |

<table>
<thead>
<tr>
<th>Week 6</th>
<th>Topic(s):</th>
</tr>
</thead>
</table>
| Feb. 27th—Mar. 5th | - Digital Certificates  
- Public Key Infrastructure (PKI)  
- Key Management  
- Cryptographic Transport Protocols |
| Reading: | - Chpt 6 – Advanced Cryptography |
| Homework: | - Netlab – Lab 8: Configuring Backups  
- Netlab – Lab 20: Cryptography  
- Project 6-1: SSL Server and Client Tests  
  ○ Pgs. 258 – 260 |

<table>
<thead>
<tr>
<th>Week 7</th>
<th>Mid-Term available online – Mar. 9th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar. 6th—Mar. 12th</td>
<td>Topic(s):</td>
</tr>
</tbody>
</table>
| | - Security Through Network Devices  
- Security Through Network Technologies  
- Security Through Network Design Elements |
| Reading: | - Chpt 7 – Network Security Fundamentals |
- Netlab – Lab 4: Protocols and Default Network Ports – Connecting to the Remote System  
- Project 7-1: Configuring the Windows Firewall  
  ○ Pgs. 304 – 305 |
<table>
<thead>
<tr>
<th>Week</th>
<th>Dates</th>
<th>Topic(s):</th>
<th>Reading:</th>
<th>Homework:</th>
</tr>
</thead>
</table>
| Week 8   | Mar. 13th – Mar. 19th | - Common Network Protocols  
- Network Administration Principles  
- Securing Network Applications and Platforms | - Chpt 8 – Administering a Secure Network | - Netlab – Lab 2: Secure Network Administration Principles, Log Analysis  
- Netlab – Lab 12: Mitigation and Deterrent Techniques – Anti-Forensic  
- Project 8-2, 8-3: Create / Load a Virtual Machine from a Physical Computer  
○ Pgs. 348 – 349 |
| Week 9   | Mar. 20th – Mar. 26th | - Wireless Attacks  
- Vulnerabilities of IEEE Wireless Security  
- Netlab – Lab 5: Secure Implementation of Wireless Networking  
- Project 9-3: Use Windows Netsh Commands  
○ Pgs. 396 – 397 |
| Mar. 27th – Apr. 2nd | Spring Break Holiday no class this week | | | |
| Week 10  | Apr. 3rd – Apr. 9th | - Types of Mobile Devices  
- Mobile Device Risks  
- Securing Mobile Devices  
- Project 10-1: Creating and Using QR Codes  
○ Pgs. 430 – 432 |
| Week 11  | Apr. 10th – Apr. 16th | - What is Access Control?  
- Implementing Access Control  
- Authentication Services | - Chpt 11 – Access Control Fundamentals | - Netlab – Lab 18: Access Control / Audit  
- Project 11: Using Windows Local Group Policy Editor  
○ Pgs. 469 – 471 |
### Week 12
**Apr. 17th – Apr. 23rd**

**Topic(s):**
- Authentication Credentials
- Single Sign-On
- Account Management

**Reading:**
- Chpt 12 – Authentication and Account Management

**Homework:**
- Netlab – Lab 17: Authentication, Authorization, and Access Control
- Project 12-1: Use an Online Rainbow Table Cracker
  - Pgs. 511 – 512

---

### Week 13
**Apr. 24th – Apr. 30th**

**Topic(s):**
- Disaster Recovery
- Environmental Controls
- Incident Response
- Controlling Risk
- Reducing Risk Through Policies
- Awareness and Training

**Reading:**
- Chpt 13 – Business Continuity
- Chpt 14 – Risk Mitigation

**Homework:**
- Netlab – Lab 6: Incident Response Procedures
- Project 13-1, 13-2: Creating / Restoring a Disk Image Backup
- Project 14-3: Training Through a Gaming Format
  - Pgs. 599 – 601

---

### Week 14
**May 1st – May 7th**

**May 3rd – Last Day of Instruction**
**May 4th – May 5th – Finals Study Period**
**May 8th – May 12th – Finals Week**

**eCafe due – May 4th**

**Final available online – May 8th**

**Topic(s):**
- Assessing Vulnerabilities
- Vulnerability Scanning vs. Penetration Testing
- Third Party Integration
- Mitigating and Deterring Attacks

**Reading:**
- Chpt 15 – Vulnerability Assessment

**Homework:**
- Netlab – Lab 14: Discovering Security Threats and Vulnerabilities
- Project 15-2: Using HoneyDocs
  - Pgs. 636 – 637

---

### Additional Information
Regular attendance in class is strongly encouraged. Students who attend class regularly are more likely to earn higher grades. For distance learning sections, attendance is checking into Laulima at
least once a week and completing the required work for the week. Students, who are ill or have other reasons for missing class, should email the instructor for an excused absence. The student is responsible the material covered in class and any in-class work missed. In-class work for excused absences may be turned in within one week of the class missed. Any assignments due at the beginning of class should be turned in online or at the start of the next class.

**Disabilities Accommodation Statement**

If you have a physical, sensory, health, cognitive, or mental health disability that could limit your ability to fully participate in this class, you are encouraged to contact the Disability Specialist Counselor to discuss reasonable accommodations that will help you succeed in this class. Ann Lemke can be reached at 235-7448, lemke@hawaii.edu, or you may stop by Hale ‘Akoakoa 213 for more information.