Credits: 3  
Class Meetings: None. This is a Video Streaming (V) course with exams on campus.

Instructor:  
Michael McAlpin  
Email: michael.mcalpin@ucf.edu  
Office: HEC – Adjunct Office (HEC-348)  
Phone: 407-459-4623  
(Google Phone – leave a message or text & please identify yourself)  
Office Hours: W-F 2:30 to 4:30 p.m.

Teaching Assistants (with office hours in HEC-328):  
TBD – will be announced upon confirmation via Webcourses

Course Objective:  
This course is designed to provide a basic understanding of security theory and practice for modern computing environments. Students will acquire proficiency in a number of classic and modern symmetric and public key cryptographic methods. Students will explore important topics in key exchange mechanisms; modes of operation; malware attacks, vulnerabilities, and defenses; network, web, and email security; digital rights management; and legal and ethical issues.

Course outcomes:  
1) Outcome 1: Apply knowledge of computing and mathematics appropriate to the discipline; specifically to include the application of mathematics, science and engineering to solve and reason about computational problems.

2) Outcome 2: Demonstrate an understanding of professional, ethical, legal, security, and social issues and responsibilities.

3) Outcome 3: Apply mathematical foundations and computer science theory, in particular principles of algorithmic design and complexity analysis, in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices.

4) Outcome 4: Demonstrate their knowledge and understanding of, and their ability to apply the concepts and design principles relating to: data structures, computer architecture and organization, programming languages, operating systems, and networks.
Course Topics:

- Number systems
- Modular arithmetic
- Classic cryptography
- Modern techniques
- Modes of operation
- DES and AES
- Public key cryptography
- RSA algorithm
- Operating systems security
- Malware and botnets
- Integrity checking
- Antivirus defense techniques
- Internet architecture
- Internet protocol and TCP
- Application layer and DNS
- Firewalls, tunneling and intrusion detection
- Wireless network security
- Web security
- Email security
- Pretty Good Privacy
- Digital rights management
- Legal and ethical issues
- Operating systems security
- Malware and botnets
- Integrity checking
- Antivirus defense techniques
- Internet architecture
- Internet protocol and TCP
- Application layer and DNS
- Firewalls, tunneling and intrusion detection
- Wireless network security
- Web security
- Email security
- Pretty Good Privacy
- Digital rights management
- Legal and ethical issues

Prerequisites:
COP 3223, Introduction to Programming with C, or EGN 3211, Engineering Analysis and Computation, or CET 2364, Systems Applications in C.

Required Textbook:

Other recommended sources:

Grading Policy:
(20%) Programming assignments – your own original code in C, C++, or Java
(25%) Exam #1 – closed book, closed notes exam given on campus.
(25%) Exam #2 – closed book, closed notes exam given on campus.
(30%) Final Exam – closed book, closed notes exam given on campus.
( 5%) Bonus Assignment – optional, up to 5 points added to final grade.
TOTAL: 100% (not including bonus)

Letter Grades:
A = 85 or better
B = 70 to 84.999
C = 60 to 69.999
D = 50 to 59.999
F = 49.999 or less

Course Policies:

- Programming Assignments: Due dates and times will be announced in Webcourses when the programming assignment is published. You should submit programs well before the deadline to avoid last-minute problems. If you submit both before and after the deadline, only what is submitted before the deadline will be graded. Only the last timely submission will be graded. If there is no submission prior to the deadline but there is a submission after the deadline, then only the first submission after the deadline will be graded. Late submissions will have one point deducted for every minute past the deadline.

- Webcourses: the instructor will use Webcourses to post Tegrity video lectures, lecture slides, announcements, assignments, grades, and other information related to this course. Please make sure to check Webcourses regularly (at least once per day) for any important information about the course.

- Email: email is the best way to contact me.

- Academic Activity: As of this term, Fall 2014, all faculty members are required to document students' academic activity at the beginning of each course. In order to document that you began this course,
please complete the following academic activity by the end of the first week of classes, or as soon as possible after adding the course, but no later than August 27. Failure to do so will result in a delay in the disbursement of your financial aid.

• **Exams:** You are expected to take exams at your assigned dates and times. Exam sessions are assigned based on the first letter of your last name (surname), as listed in the schedule. Please note that the alphabetical order for exam sessions alternates for each exam.

• **Makeup Exams:** The make-up exam sessions are for extenuating circumstances only, as determined at the sole discretion of the instructor. One example of an extenuating circumstance is a conflicting exam in another course. Being scheduled for work is not generally sufficient; particularly since the exam dates and times are known on the first day of classes. If you do not take an exam at your assigned session and you do not have prior permission to attend another session, 5 points will be deducted from your grade.

• **Make-up Programming Assignments:** No make-up programming assignments will be given.

• **Academic Integrity:** Plagiarism or cheating of any kind on an examination, quiz or assignment will not be tolerated. It may result in an “F” for that assignment (and may, depending on the severity of the case, lead to an “F” for the entire course) and may be subject to appropriate referral to the Office of Student Conduct for further action. Please refer to The Golden Rule (http://www.goldenrule.sdes.ucf.edu/) of the University of Central Florida's Student Handbook for further information.

I will assume for this course that you will adhere to the academic creed of this University and will maintain the highest standards of academic integrity. In other words, don't cheat by giving answers to others or taking them from anyone else, and don't share program code for programming assignments. I will also adhere to the highest standards of academic integrity, so please do not ask me to change (or expect me to change) your grade illegitimately or to bend or break rules for one person that will not apply to everyone.

**Important Dates:**
- **Classes begin:** August 24.
- **Withdrawal deadline:** Monday, November 2.
- **Classes end:** Monday, December 7.
- **Final exam:** December 11 or December 12 (depending on the scheduling), as specified in the schedule (Exam’s time and location will be announced in Webcourses’ Announcements Section).

  - **Fall 2015 Holidays are:**
    Labor Day: September 7.
    Veteran’s Day: November 11.
    Thanksgiving: November 26 and 27.

**Students with Disabilities:**
Students with disabilities who have special testing or other needs are required to contact the Student Disability Services (SDS) office at the beginning of the semester in order to make special arrangements before requesting accommodations from the instructor. SDS is located in the Student Resource Center, Room 132, and can be reached at (407) 823-2371, TTY/TDD only phone (407) 823-2116.

**Schedule:**

<table>
<thead>
<tr>
<th>Week/Dates</th>
<th>Topics Covered</th>
<th>Readings/Assignments</th>
</tr>
</thead>
</table>
| Week 1 (08/24 - 08/28) | Course Overview  
|                  | Introduction to Computer Security  
<p>|                  | Number Systems                              | Chapter 1               |</p>
<table>
<thead>
<tr>
<th>Week</th>
<th>Dates</th>
<th>Topics</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 2</td>
<td>(08/31 - 09/04)</td>
<td>Modular Arithmetic, Classic Cryptography</td>
<td>8.2.1, 8.1.1, 8.1.2, 8.1.3, 8.1.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Classic Crypto: Playfair, Hill, and Transposition Ciphers</td>
<td>8.1.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modern Crypto: DES</td>
<td></td>
</tr>
<tr>
<td>Week 3</td>
<td>(09/07 - 09/11)</td>
<td>Classic Crypto: Playfair, Hill, and Transposition Ciphers</td>
<td>8.1.1, 8.1.2, 8.1.3, 8.1.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modern Crypto: AES and Modes of Operation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review for Exam 1</td>
<td>8.1.6, 8.1.7, 8.5.1</td>
</tr>
<tr>
<td>Week 4</td>
<td>(09/14 - 09/18)</td>
<td>Modular Crypto: AES and Modes of Operation</td>
<td>Study for exam !!!</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EXAM #1 Cryptographic Hash Functions and Integrity Checking</td>
<td>8.3</td>
</tr>
<tr>
<td>Week 5</td>
<td>(09/21 - 09/25)</td>
<td>Cryptographic Hash Functions and Integrity Checking</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Key Cryptography, Digital Signatures, and RSA</td>
<td>8.2, 8.4.1, 8.5.2</td>
</tr>
<tr>
<td>Week 6</td>
<td>(09/28 - 10/02)</td>
<td>Operating Systems Security</td>
<td>Chapter 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EXAM #1 Cryptographic Hash Functions and Integrity Checking</td>
<td>Program 1 due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malicious Attacks and Botnets</td>
<td></td>
</tr>
<tr>
<td>Week 7</td>
<td>(10/05 - 10/09)</td>
<td>Operating Systems Security</td>
<td>Chapter 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Layer &amp; DNS Firewalls, Tunneling, and Intrusion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wireless Networking</td>
<td>Study for exam !!!</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet Protocol &amp; TCP</td>
<td>5.1</td>
</tr>
<tr>
<td>Week 8</td>
<td>(10/12 - 10/16)</td>
<td>Malware Malicious Attacks and Botnets</td>
<td>Chapter 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EXAM #2 ARP-Spoofing and Denial-of-Service</td>
<td></td>
</tr>
<tr>
<td>Week 9</td>
<td>(10/19 - 10/23)</td>
<td>Network Security Concepts, Internet Protocol &amp; TCP</td>
<td>Study for exam !!!</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Layer &amp; DNS Firewalls, Tunneling, and Intrusion</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wireless Networking</td>
<td></td>
</tr>
<tr>
<td>Week 10</td>
<td>(10/26 - 10/30)</td>
<td>Web Security Attacks on Clients and Servers</td>
<td>Chapter 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EXAM #2 ARP-Spoofing and Denial-of-Service</td>
<td>Program 2 due</td>
</tr>
<tr>
<td>Week 11</td>
<td>(11/02 - 11/06)</td>
<td>Email Security and PGP</td>
<td>10.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Legal and Ethical Issues Digital Rights Management</td>
<td></td>
</tr>
<tr>
<td>Week 12</td>
<td>(11/09 - 11/13)</td>
<td>The “Cloud” Internet of Things</td>
<td>Bonus Assignment due</td>
</tr>
<tr>
<td>Week 13</td>
<td>(11/16 - 11/20)</td>
<td>Email Security and PGP</td>
<td>10.4</td>
</tr>
<tr>
<td>Week 15</td>
<td>(11/30 - 12/04)</td>
<td>The “Cloud” Internet of Things</td>
<td></td>
</tr>
<tr>
<td>Week 16</td>
<td>(12/07 - 12/11)</td>
<td>Email Security and PGP</td>
<td>Study for Final Exam !!!</td>
</tr>
<tr>
<td>Week 17</td>
<td>(12/14 - 12/18)</td>
<td>Finals - 12/9 -&gt; 12/14</td>
<td></td>
</tr>
</tbody>
</table>