

# School of Computer Science University of Central Florida

## CAP 6133: Advanced Topics in Computer Security and Computer Forensics

### Tentative Syllabus

---

**Instructors** : **Joohan Lee**  
Office : CSB 234 Phone : 823-6095 E-mail : jlee@cs.ucf.edu  
**Sheau-Dong Lang**  
Office : CSB 203 Phone : 823-2474 E-mail : lang@cs.ucf.edu

**TA** : **TBA**  
Office : TBA E-mail : TBA@cs.ucf.edu  
Phone : TBA

**Course Homepage:** <http://www.cs.ucf.edu/~jlee/cap6133>

**Meeting Times and Location** : TTH 12:00-1:15pm (CSB 221)  
**Office Hours** : TTH 1:30 pm – 3:30 pm (Dr. Lee),  
or by appointment (both Drs. Lee and Lang)  
**TA Office Hours** : TBA

#### Objectives

The purpose of this advanced topics course is to provide an in-depth study of the fundamental issues related to computer security and forensic analysis, by building upon the knowledge from coursework in operating systems, networking, and the previous two Computer Forensics courses (I and II). The state-of-the-art technology, both in software and hardware, will be addressed. Commercial tools for setting up firewalls, intrusion detection, event monitoring and logging, forensic analysis, will be used in the teaching labs to provide the hands-on experience. Further, computer related crimes using documented trial cases will be discussed. We will also use expert speakers from the relevant domains including security system administrators, law enforcement officers, attorneys and lawyers in cyber laws, to provide guest lectures. The class will be divided into small groups to work on team projects from a selected list of topics. Time permitting, we will discuss more advanced topics.

#### Prerequisites:

- COP 5611, COT 5405, CDA 5501; or consent of instructor
- Proficiency in C and JAVA programming language and familiarity with the UNIX operating system

#### Textbook:

*Computer Security: Art and Science* by Matt Bishop, Addison Wesley, 2003.  
Other reading materials will be used as well.

#### References:

*Security in Computing* by Charles P. Pfleeger and Shari Pfleeger, 3<sup>rd</sup> Edition, Prentice Hall, 2003.  
*Investigative Data Mining for Security and Criminal Detection* by Jesus Mena, Butterworth-Heinemann, 2002.

**Grading Policy:**

- (20%) Mid Exam – closed book, closed notes exam given in class.
- (20%) Final Exam – closed book, closed notes given during the final exam week.
- (25%) Projects – Written mostly in C and JAVA on UNIX or Windows systems
- (25%) Homework assignments.
- (10%) Class and Lab participation

**Letter grades:** 90 – 100: A, 87–89:A-, 84 – 86: B+, 80–83:B, 77–79:B-, 74–76:C+, 70–74: C, 65–69:C-, 60–64:D+, 50 – 60: D, Below 50: F

**The Semester Plan:**

Week 1: Introduction (Chap 1 from Bishop's book)

Week 2: Access Control Matrix (Chap 2 from Bishop's book)

Week 3: Foundational Results (Chap 3 from Bishop's book)

Week 4: Policy Models (Chap 4 and 5 from Bishop's book)

Week 5: Network Intrusion Detection (Chap 25 from Bishop's book)

Week 6: Network Intrusion Detection (Statistical Approach)

Week 7: Network Intrusion Detection (Data Mining Approach)

Week 8: Network Security (Chap 26 from Bishop's book) and Firewall Lab I and II

Week 9: Guest Lectures

- Reverse Code Engineering by Terry Gillette, President, SI Government Solutions
- Malicious Code Detection by Muazzam Siddiqui, IST

Week 10: Operating System Security (Chap 4 and 5 from Pfleeger's book)

Week 11: Malicious Logic and Program Security (Chap 22 from Bishop's book and Chap 3 from Pfleeger's book)

Week 12: Malicious Code Detection

Week 13: Vulnerability Analysis (Chap 23 from Bishop's book) and Auditing (Chap 24 from Bishop's book)

Week 14: Student Presentation

Week 15: Student Presentation