

B649: Introduction to Computer Security
Spring, 2004

Instructor: Kay Connelly,
connelly@indiana.edu
LH 301E

AI: Nick Edmonds
ngedmonds@indian.edu
LH 305

Office Hours: Mon, Tue 2:30-3:30 pm, LH301E

Lecture: Tue, Thu, 1-2:15 pm, LH102

Lab: 1:00 – 2:15 pm, MW

Credits: 3 credits

2:30 – 3:45 pm, TR

Web Page: www.cs.indiana.edu/~connelly/b649_Spring04.html

Overview

This is a graduate course on computer security. The primary course objectives are to

1. provide an introduction to security principles and concepts,
2. give hands on experience with security concepts and tools,
3. explain the interdisciplinary nature of computer security.

Topics include security terminology, policies, protocols, cryptography, design principles, identity, information flow, assurance, malicious logic, and vulnerability analysis.

This course has a lecture and laboratory component. The lecture provides the theoretical foundation of computer security while the laboratory provides hands-on experience.

Grading

Grades are assigned on a straight 90%, 80%, etc... scale. Grades are weighted as follows:

- **Homework: 25%**
- **Laboratory: 25%**
- **Midterm: 20%**
- **Final Exam: 30%**

Homework

There are seven homework assignments. You must email your answers to the AI by noon of the due date (see schedule). Late homework will be docked 10% per day, up to 2 days late. Your lowest homework grade will be dropped.

Laboratory

Lab will begin with an overview of the topic by the AI. Unless otherwise directed, you must perform the labs by yourself. You may leave the lab once you have completed the assignment. It is possible that you may finish during the first lab of the week, in which case, you do not need to attend the second lab. There are no makeup labs. The lowest lab grade will be dropped.

Exams

Exams are closed books and closed notes. The final is cumulative, but will emphasize the material since the midterm. The exam format will be approximately 1/3 short answer, 1/3 algorithmic, 1/3 essay/design. Except for extreme circumstances, you must schedule make-ups in advance with an appropriate documented excuse. "I overslept" will not be acceptable. Likewise, forgetting to schedule a makeup when you are presenting a paper at a conference will not be acceptable.

Ethics

You may learn some skills in this course that are not legal for you to use outside of the lab. You *will* be subject to University, State and Federal law if you use these skills outside of the scope of this course. If you are unsure, *do not do it!* Ask.

Text

Matt Bishop's *Computer Security: Art and Science*

Supplementary handouts will be provided in class or from the web page.

Cheating Policy

It is expected that you will abide by The Indiana University Code of Student Rights, Responsibilities, and Conduct (http://campuslife.indiana.edu/Code/Part_4B.html) and its application to programming courses (<http://www.cs.indiana.edu/dept/integrity.html>). Acts of academic dishonesty undermine the effectiveness of the class and the learning experience for all, and will be dealt with in strict accordance to the Code of Student Rights.

Schedule

Date	Topic	Lab Topic	Readings	Due
1/13	Overview	Protecting email	Chapter 1	
1/15	Access Control		Chapters 2, 15	
1/20	Policies	Buffer Overflow	Chapter 4	Homework #1
1/22	Confidentiality Policies		Chapter 5	
1/27	Integrity Policies	Tripwire, file corrupt	Chapter 6	
1/29	Hybrid Policies		Chapter 7	
2/3	Cryptography I	data recov/destruction	Chapter 9	Homework #2
2/5	Cryptography II		Chapter 9	
2/10	Keys	Suid Exploits	Chapter 10	
2/12	Ciphers		Chapter 11	
2/17	Authentication I	Password attacks/	Chapter 12	Homework #3
2/19	Authentication II	Tcp/ip primer	Chapter 12	
2/24	Review			
2/26	MIDTERM			
3/2	Design Principles	Sniffers	Chapter 13	
3/4	Identity		Chapter 14	
3/9	Information Flow	Spoofing	Chapter 16	Homework #4
3/11	Confinement		Chapter 17	
3/16	SPRING BREAK			
3/18	SPRING BREAK			
3/23	Assurance	DoS	Chapter 18	
3/25	Assurance Systems		Chapter 19	
3/30	Malicious Logic I	Worms/Viruses	Chapter 22	Homework #5
4/1	Malicious Logic II		Chapter 22	
4/6	Vulnerability Analysis I	Firewalls	Chapter 23	
4/8	Vulnerability Analysis II		Chapter 23	
4/13	Auditing	Logging tools	Chapter 24	Homework #6
4/15	Intrusion Detection Systems		Chapter 25	
4/20	Physical Tampering	IDS	Anderson #14 handout	
4/22	Information Warfare		Anderson #16 handout	
4/27	Privacy		Database Nation handout	Homework #7
4/29	Review			
5/?	FINAL			