

CS442/542 Computer Security Concepts (Fall 2004)*

Dr. Jim Alves-Foss

Course Overview

Course Objectives: Cryptographic systems, coding and decoding of messages; network, database, and operating system security issues, capability and access control mechanisms; current trends and research in mandatory and discretionary security policies. (Prerequisites: Operating Systems (CS 341) and Probability Theory (Stat 3001)).

Goals: Introduce principles, mechanisms and implementations of computer security; learn how attacks work, how to defend against them, and how to design systems to withstand such attacks.

- What is computer security: notion of an informal policy, formalization of policy governmental vs. commercial, etc.; ethics and law
- Encryption: classical, public-key; implementation, problems; the UNIX file encryption mechanism and its cryptanalysis; the DES and RSA
- Authentication: model of authentication systems, traditional passwords, challenge/response, one-time passwords; cryptographic protocols, simple cryptosystems; the standard UNIX authentication system, its limits and alternate forms; implementations of other mechanisms
- Access control: controlling access to resources, access matrix model, undecidability result, access control lists and capability lists; mandatory controls, originator controls; variants; UNIX scheme and augmentations
- Integrity: cryptographic checksums, malicious logic, viruses, Trojan horses; defenses, prevention; UNIX integrity checking tools and how they work; malicious logic and UNIX
- Security-oriented programming: design principles, focusing on common problems; gates vs. privileged servers; environment, exception handling; writing secure servers and secure setuid/setgid programs in the UNIX environment
- Networks and security: Internet Security Architecture, analysis of Internet protocols, design and implementation considerations; firewalls; UNIX networking and security
- Penetration analysis: common types of flaws, examples, flaw hypothesis methodology, analysis of programs and systems; UNIX instances of problems, flaws, and how to fix them
- Secure systems: types, models, design, changes to non-secure systems; comparative analysis

This Course ...

- is an intensive course focusing on fundamentals of computer security
- requires time, dedication, and willingness to think outside the box

*Copyright © 2004, Dr. Jim Alves-Foss, all rights reserved.

Organizing Theme: *Game: Planning for the unexpected*

- Polices – what are the end goals of the game?
- Encryption and Access Control – what are the pieces?
- Analysis – what are the rules and how can we win?

Administrative Matters

Instructor

- Jim Alves-Foss, 225 JEB, (208) 885-5196
- Email: jimaf@cs.uidaho.edu
- Office Hrs: W 9-11am (or by appt.)

Communication

- Home page: <http://webct.uidaho.edu>
 - Class handouts
 - Homeworks and corrections
 - Grades
 - Links to other relevant course resources

Prerequisites

- CS 341 (or equivalent) - Operating Systems
- Stat 301 (or equivalent) - Probability Theory
- Good understanding of basic concepts of computing
- Drop course if you do not have the pre-requisite

Grading

Quizzes (100 pts)

- There will be a quiz every Tuesday at the beginning of class, except on exam week. The quizzes will cover the lecture material and assigned readings of the previous week. Each quiz is worth 10 pts, the best 10 quiz grades will count.

Homeworks (400 pts; more pts for CS 542 students)

- Written assignments, primarily from the text.

Exams (150 pts Each) : video students add two weeks to each of these dates.

- Exam I – Sept 28
- Exam II – Nov 4
- Exam III – Dec 16 (8am)

Paper (150 pts) – for CS 542 Students ONLY

- This will be discussed in detail at the end of the first week

Letter Grades

- Each class is different, so there is no absolute grading scheme. However I will honor the following guarantees:

> 90% = you earn an A	> 80% = at least a B
> 70% = at least a C	< 50% = you earn an F
- Significant difference between homework scores and exam scores \Rightarrow alternate grading scheme.
For instance, 90% on homeworks + fail both midterm and final \Rightarrow fail course

Textbook

- Bishop, "Computer Security: Art and Science",

Course Policies

- Be considerate (this is a video class class, be quiet, don't dwell on little things, don't take up too much space, don't chain smoke, don't put on too much perfume/cologne, please bathe and don't snore.)
- Written Homeworks due in-class on due date. **NO DELAYS/NO EXCEPTIONS; NO LATE ASSIGNMENTS; NO EXTRA CREDIT**
- Re-grades within **one week** of receiving returned graded assignments. After one week, I will not regrade your work. So do not come for regrades just before your final.
- Attendance is not mandatory. However, **YOU** are responsible for all material to get a good grade
- **NO MAKEUP EXAMS;** So make your plans around exams accordingly. Family trips, and early airplane reservations are NOT a valid excuse.
- **Student Conduct:**
 1. Do your own work. May discuss general approach, but develop your own solutions.
 2. Solutions from other sources prohibited.
 3. Any instance of suspected cheating will result in a zero on that assignment and referral to University Officials.

Disability Support Services Reasonable Accommodations Statement:

Reasonable accommodations are available for students who have a documented disability. Please notify the instructor during the first week of class of any accommodation(s) needed for the course. Late notification may mean that requested accommodations might not be available. All accommodations must be approved through Disability Support Services located in the Idaho Commons Building, Room 333.

- 885-7200
- email at jdss@uidaho.edu
- website at www.access.uidaho.edu or www.webs.uidaho.edu/aap

Lectures, Readings and Due-Date Schedule

The following is a *tentative* schedule. Major topics are in italics. Dates and topics are subject to change. Changes will be provided in class or with specific assignments on the web or through e-mail. **VIDEO STUDENTS: Add 2 weeks to each of these dates**

Week	Dates	Topic	Readings	Quizzes	Assignments Due
1	Aug 24 Aug 26	<i>Introduction Overview</i>	Ch 1	1 (Prerequisites)	
2	Aug 31 Sep 2	<i>Foundations</i>	Ch 2 & 3	2	Written HW 1 (Overview)
3	Sep 7 Sep 9	<i>Security Policies</i>	Ch 4 & 5	3	<i>Paper Topic Due</i>
4	Sep 14 Sep 16	<i>More Policies</i>	Ch 6 & 7	4	
5	Sep 21 Sep 23	<i>More Policies</i>	Ch 8	5	Written HW 2 (Policies)
6	Sep 28 Sep 30	Exam 1 9:30 – 10:45			
		<i>Cryptography</i>	Ch 9 & 10		
7	Oct 5 Oct 7	<i>Cryptography</i>	Ch 10 & 11	6	
8	Oct 12 Oct 14	<i>More Crypto</i>	Ch 12	7	Written HW 3 (Crypto)
9	Oct 19 Oct 21	<i>Design Principles</i>	Ch 13 & 14	8	
10	Oct 26 Oct 28	<i>More Design</i>	Ch 15 & 16	9	
11	Nov 2 Nov 4	<i>More Design</i>	Ch 17		Written HW 4 (Design) <i>Paper Draft Due</i>
		Exam II 9:30 – 10:45			
12	Nov 9 Nov 11	<i>Assurance</i>	Ch 18 & 19	10	
13	Nov 16 Nov 18	<i>More Assurance</i>	Ch 20 & 21	11	<i>Paper Reviews Due</i> Written HW 5 (Assurance)
	Nov 22-26	Thanksgiving Holiday			
14	Nov 30 Dec 2	<i>Catch-up & Other Topics</i>		12	
15	Dec 7 Dec 9	<i>More Catch-up Review</i>		13	<i>Final Paper Due</i> Written HW 6 (??)
16	Dec 16	Exam III – 8:00-9:15 AM			

Textbook: Matt Bishop, *Computer Security: Art and Science*, Pearson Education, Boston, 2003.
ISBN 0-201-44099-7.

Homework #1: (Due 9:30 am Tuesday August 31)

- Chapter 1 (pages 25–28) #1,2,3,8,9,11,15,18,19,21

Quiz #1: (Due by 10pm Friday August 27th) Taken on-line through WebCT.