

**CS 336 Introduction to Information Assurance
Fall 2008 Syllabus**

Catalog Description: Introduces the confidentiality, availability and integrity goals of information systems; resistance, recognition and response categories of assurance. Focus on computer security and survivability, including cryptography, network security, general purpose operating system security and dependability and special purpose systems for high assurance security and dependability.

Class Meetings: TuTh 2:00 – 3:15 in TLC 31
Course Credits: 3 cr.
Prerequisites: CS 240
Textbook: W. Stallings, *Cryptography and Network Security*, 4th Edition, 2006
Instructor: Dr. Paul W. Oman, Professor of Computer Science
Office: McClure 409; Phone 885-6899; Email oman@uidaho.edu

Course Goals:

1. Familiarize students with the principles of Information Assurance (IA).
2. Explore and understand cryptographic systems.
3. Differentiate between obsolete and state-of-the-art security practices.
4. Recognize computing system vulnerabilities and corresponding mitigations.
5. Adopt an ethical perspective on the use and misuse of these technologies.

Course Grading: A point system will be used for grading. Your semester grade will be based on the cumulative number of points you have earned by the last day of finals week. Grades will be assigned as follows:

A	325 – 400 points	D	175 – 224 points
B	275 – 324 points	F	< 175 points
C	225 – 274 points		

There will be two exams and projects or labs, for a maximum total points of 400, assigned as follows:

Midsemester exam	100 points	Projects	50 points each
Final exam	200 points	RADICL Labs	10 points each, 50 points total

A project is defined to be an in-class presentation or a typed research paper. Each project is worth 50 points. A lab exercise is a proctored RADICL Lab exercise and report summary. Each lab exercise is worth 10 points and there will be 5 lab exercises. Unfortunately, off-campus students do not have access to RADICL at this time and, hence, are limited to research papers and/or presentations (live via a campus visit or remote via PowerPoint with accompanying audio- or videotape).

In any given month you may turn in only one project or two labs. At most you can turn in either (a) two projects in two different months or (b) one project and five RADICL labs spread out across four months. **THE LAST DAY TO TURN IN PROJECTS OR LABS IS TUESDAY, DECEMBER 9.** All projects **require instructor approval and scheduling prior to beginning** the project. Approval will be granted on a first-come, first-served basis with only one student approved for each topic. All labs require RADICL proctor approval and validation. This will be discussed in class.

CS 336 Guidelines and Rules

1. In all projects you need to cite your sources using formal bibliographic references.
2. In-class presentations are limited to 30 minutes and should include PowerPoint slides for the in-class computer and handouts for the class participants. Equipment other than the in-class computer and overhead projector needs to be arranged in advance. Material covered in the in-class presentations will be included on the exams. Presentation dates will be arranged individually. Presentation topics will be discussed in class.
3. Research papers are expected to be 5-10 typed pages (12 point fonts), including references and graphics. They must contain, in order: Title, Author contact info, Abstract, Introduction, Body, Conclusions, and References. Research papers will only be accepted on the last school day of each month except for December when they are due on Dec. 9. Research paper topics will be discussed in class.
4. RADICL lab exercises must be contained within the RADICL lab, proctored by the RADICL SysAdmin, and cannot stray from the lab exercise description. The labs will be progressive in detail and difficulty, so you cannot miss the first ones and expect to do the later ones.
5. **Unauthorized probing and hacking on any system are not tolerated.** Anyone caught attempting to probe, hack, or crack computer systems or accounts outside of their immediate ownership without the express written approval of the instructor, will be disenrolled or failed from the course and remanded to the appropriate university, state, and federal authorities. All offensive activities, like hacking, cracking, probing, sniffing, snorting, etc., should only be done in isolated or controlled environments with the instructor's prior approval.
6. **Cheating and plagiarism are not tolerated.** Anyone caught copying or stealing another person's work will receive a zero for that entire work task, whether it is a test, project, or lab exercise. Anyone caught plagiarizing another person's work, from printed or electronic sources, will receive a zero for that project or lab exercise. Anyone caught sharing work with other classmates, unless they are working on an approved team project and the sharing is restricted to teammates, will receive a zero for that project. Note that plagiarism is not just copying other people's writings, it includes all instances of passing off someone else's work as if it is your own. If you use other people's work, cite that work in a footnote or reference list.

**CS 336 Introduction to Information Assurance
Fall 2008 Tentative Schedule**

Week	Dates	Topic	Readings
1	Aug. 26, 28	Introduction & Vocabulary	Ch. 1, 18, & 19
2	Sept. 02, 04	Ethics: Uses & Misuses of Security	"
3	Sept. 09, 11	Classic Ciphers	Ch. 2
4	Sept. 16, 18	Block Ciphers, DES, & 3-DES	Ch. 3, 6.1, & 6.2
	Sept. 19	Last day to drop without getting a "W."	
5	Sept. 23, 25	Modular Arithmetic & Euclid's Algorithm	Ch. 4
6	Sep.30, Oct.2	AES	Ch. 5
7	Oct. 07, 09	Other Topics in Symmetric Cryptography; Review	Ch. 6 & 7
8	Oct. 14, 16	Midsemester Exam & Review	Date TBD
9	Oct. 21, 23	Using Number Theory in Public-Key Cryptosystems	Ch. 8
10	Oct. 28, 30	Public (aka, Asymmetric) Key Cryptography	Ch. 9
11	Nov. 04, 06	Key Exchanges and Key Management	Ch. 10
12	Nov. 11, 13	Message Authentication and Digital Signatures	Ch. 11, 12, & 13
13	Nov. 18, 20	Other topics in Asymmetric Cryptography; Review	Ch. 14
14	Nov. 24-28	Thanksgiving Break	
15	Dec. 02, 04	Email, TCP/IP and Web Security	Ch. 15, 16, & 17
16	Dec. 09, 11	Viruses and Firewalls	Ch. 19 & 20
	Dec. 09	Last day for presentations, papers, and labs.	
17	Dec. 15-19	Final Exam (Wednesday, Dec. 17, 12:30 – 2:30, TLC 31)	Comprehensive

CS 336 – Introduction to Information Assurance
Possible Topics for Fall 2008 Projects

ALL PROJECTS REQUIRE PRIOR APPROVAL.
ONLY ONE PERSON PER TOPIC; FIRST-COME, FIRST-SELECTION.

RADICL (Reconfigurable Attack-Defend Instructional Computing Lab) Exercises (JEB 6):

- There are 7 total RADICL lab exercises
- The first two labs are during class time (Sept. 25 & 30) and are mandatory
- The first two labs will show you how to use RADICL
- The remaining five labs will be conducted in the evenings; they are optional and worth 10 points each, for a total of 50 points
- The labs will show various offensive and defensive security tools and techniques
- The lab exercises are progressive, so you cannot skip one and expect to do the next

Papers:

- Voice Over IP (VOIP) Security (assigned Sands)
- Multimedia Over IP (MOIP) Security
- Quantum Cryptography
- Beyond 802.11: Next Generation Wireless Network Protocols
- Is GSM the Final Word in Telephony?
- Terrorist Uses of Steganography (assigned Weingart)
- Recent Attempts to Crack AES
- Can Emergency Services Rely on the Internet?
- How Electronic Fund Transfers are Secured
- Computer Virus Dissection (assigned Grzebielski: Melissa)

In-Class Presentations:

- Any of the paper topics listed above are also suitable for in-class presentations
- The AES Competition Criteria and Entries
- Promises and Problems in Public Key Cryptography
- Cracking WEP and WPA (a demonstration) (assigned Blaker)
- Internet and Network Traffic Analysis (a demonstration)
- Computer Worm Dissection (e.g., Nimda, Slammer, MyDoom, CodeRed)
- Cracking DES and 3DES (assigned Daly)
- Very Small Crypto Algorithms (e.g., TEA, RC4)