

GRADUATE PROGRAMS IN SOFTWARE
University of St. Thomas
St. Paul, MN

SYLLABUS SPRING 2011
SEIS721

Course Title

Advanced Computer Security

Meeting Time/Place

Tuesdays, 5:45PM – 9:00 PM, OSS-329

Credit Value

3 semester credits

Prerequisites

SEIS635: Software Analysis and Design (Required)

SEIS645: Computer and Network Communication (Required)

SEIS720: Computer Security (Required)

SEIS640: Operating Systems Design (Recommended)

Instructor

Bradley S. Rubin, Ph.D. (Brad)

E-Mail Address

bsrubin@stthomas.edu

Office Address

OSS-312

Office Hours

Tuesdays and Thursdays, 3:30 – 5:30 PM

(Email and phone calls welcome too)

Lab

OSS-334

Course Description

This course is the next step beyond the prerequisite course, Computer Security. Given the security concepts and building blocks developed in the former course, this course both explores these previous topics in greater depth and covers additional topics. Topics will include advanced cryptography, single sign on using directories, wireless network security, firewalls, VPNs, and intrusion detection and prevention systems, and other security technologies. There is special emphasis on application security issues as well. In

addition, this course utilizes a computer security lab for hands-on exercises that reinforce the material and covers weekly current events in computer security.

Course Objectives

- Gather factual knowledge (terminology, classifications, methods, trends) in computer security
- Learn to apply course material (to improve thinking, problem solving, and decisions)
- Develop specific skills, competencies, and points of view needed by professionals in the field most closely related to computer security

Required Texts

- Anderson, Ross, "Security Engineering", 2nd edition, 2008 [ROSS08]
- Howard, Michael et. al. "24 Deadly Sins of Software Security", 2010 [HOWA10]
- Supplementary Papers

Grading Policy

Weekly homework and labs (50%)

- Textbook and other written exercises
Typical assignments include: mathematical problems in cryptography (including use of Mathematica), ethical/legal case studies in areas like privacy and digital rights management requiring research of appropriate laws, Perl programming, network trace identification using Ethereal, network attack identification using Snort, system vulnerability assessment using Nessus, and TCP/IP protocol analysis using Internet RFCs.
- Current security events
- Lab exercises (4-5, no late penalty for labs)
- 10% of the possible points off for each day late (max 1 week late)
- Assigned Tuesday, due following Tuesday at midnight, returned on the 2nd Tuesday (turned in on paper during class (preferred) or emailed to me)

Midterm (25%)

- Multiple choice

Final (25%)

- Multiple choice

Blackboard

- Lecture notes (pdf format), papers, homework assignments/answers, and grades will be available on Blackboard each week (usually 24 hours in advance of class)

Weekly Class Schedule

90 min Lecture

15 min Break

15 min Security Current Events

75 min Lecture, Homework Assignment

Course Outline

Week 1

- Course Introduction
- RSA Attacks
- ElGamal
- Mathematica Intro
- Lab Tour/Sign-in

Week 2

- Elliptic Curve Cryptography
- Lattice-based Cryptography
- LAB 1: Generate a PGP Certificate and Sign/Encrypt Email with PGP

Week 3

- Digital Rights Management
- Watermarking
- Steganography

Week 4

- SSL
- STS (Strict Transport Security)
- LDAP and Active Directory
- Perl 101
- LAB 2: Active Directory/LDAP Exploration

Week 5

- Distributed System Security
- Cloud Computing Security
- Wireless Network Insecurity/Tools/Solutions

Week 6

- Privacy and Anonymity
- Election/Game/Web App Security
- Email-Based Identification and Authentication
- Midterm Q&A
- LAB 3: Creating a Certificate for ISS 6.0 on Windows 2008 Server

Week 7

- Quantum Computing
- Midterm Exam

Week 8

- Midterm Results
- Firewalls
- Intrusion Detection Systems
- Vulnerability Assessment Tools
- LAB 4: Blocking a Port on the Firewall

Week 9

- Honeypots
- Multilevel and Multilateral Security
- Economics of Security
- Managing Security Development
- Systems Evaluation and Assurance

Week 10

- SQL Injection
- Web Server-Related Vulnerabilities
- Web Client-Related Vulnerabilities
- Use of Magic URLs, Predictable Cookies, and Hidden Form Fields
- Buffer Overruns
- Format String Problems

Week 11

- Integer Overflows
- C++ Catastrophes
- Catching Exceptions
- Command Injection
- Failing to Handle Errors
- Information Leakage

Week 12

- Race Conditions
- Poor Usability
- Not Updating Easily
- Executing Code with Too Much Privilege
- Failure to Protect Stored Data
- The Sins of Mobile Code
-

Week 13

- Use of Weak Password-Based Systems
- Weak Random Numbers
- Using Cryptography Incorrectly
- Failing to Protect Network Traffic
- Improper Use of PKI, Especially SSL
- Trusting Network Name Resolution

Week 14
- Final Exam

Attendance Policy

- Attendance sheet must be initialed each week
- A maximum of two absences expected

Academic Integrity

Academic integrity is defined as not cheating and not plagiarizing; honesty and trust among students and between students and faculty are essential for a strong, functioning academic community. Consequently, students are expected to do their own work on all academic assignments, tests, projects and research/term papers. Academic dishonesty, whether cheating, plagiarism or some other form of dishonest conduct related to academic coursework and listed in the Student Policy Book under "Discipline: Rules of Conduct" will automatically result in failure for the work involved. But academic dishonesty could also result in failure for the course and, in the event of a second incident of academic dishonesty, suspension from the University.

Here are the common ways to violate the academic integrity code:

Cheating - Intentionally using or attempting to use unauthorized materials, information, or study aids in any academic exercise. The term academic exercise includes all forms of work submitted for credit.

Fabrication - Intentional and unauthorized falsification or invention of any information or citation in an academic exercise.

Facilitating Academic Dishonesty - Intentionally or knowingly helping or attempting to help another to violate a provision of the institutional code of academic integrity.

Plagiarism - The deliberate adoption or reproduction of ideas or words or statements of another person as one's own without acknowledgment. You commit plagiarism whenever you use a source in any way without indicating that you have used it.

Cheating

In cases of cheating, the instructor will impose a minimum sanction of failure of work involved. The instructor will inform the student and the program director in writing of:

1. the nature of the offense,
2. the penalty imposed within the course;
3. the recommendation of the instructor as to whether further disciplinary action by the director is warranted.

If the instructor or the director of the program determines that further disciplinary action is warranted, a disciplinary hearing shall be commenced at the request of either the instructor or the director. (If there is a previous offense of this nature on the student's record, a hearing is mandatory.)

Here are examples of various kinds of plagiarism. In each instance, the source is a passage from p. 102 of E.R. Dodd's *The Greek and the Irrational* (Berkeley, 1971; reprinted: Boston: Beacon, 1957). First here is the original note, copied accurately from the book *Functions*, Dodds 12, p. 102: "If the waking world has certain advantages of solidity and continuity its social opportunities are terribly restricted. In it we need as a rule, only the neighbors whereas the dream world offers the chance of intercourse, however fugitive, with our distant friends, our dead and gods. For normal men it is the sole experience in which they escape the offensive and incomprehensible bondage of time and space."

Here are five ways of plagiarizing this source: (If you have any questions about plagiarism ask the instructor)

1. Word-for-word continuous copying without quotation marks or mention of the author's name.

Dreams help us satisfy another important psychic need - our need to vary our social life. This need is regularly thwarted in our waking moments. If the waking world has certain advantages of solidity and continuity, its social opportunities are terribly restricted. In it we need, as a rule, only the neighbors, whereas the dream world offers the change of intercourse, however fugitive, with our distant friends, our dead, and our gods. We awaken from such encounters feeling refreshed, the dream having liberated us from the here and now...

2. Copying many words and phrases without quotation marks or mention of the author's name.

Dreams help us satisfy another important psychic need - our need to vary our social life. In the waking world our social opportunities, for example, are terribly restricted. As a rule, we usually encounter only the neighbors. In the dream world, on the other hand, we have the chance of meeting our distant friends. For most of us it is the sole experience in which we escape the bondage of time and space....

3. Copying an occasional key word or phrase without quotation marks or mention of the author's name.

Dreams help us satisfy another important psychic need - our need to vary our social life. During our waking hours our social opportunities are terribly restricted. We see only the people next door and our business associates. In contrast, whenever we dream, we can see our distant friends. Even though the encounter is brief, we awaken refreshed, having freed ourselves from the bondage of the here and now...

4. Paraphrasing without mention of the author's name.

Dreams help us satisfy another important psychic need - our need to vary our social life. When awake, we are creatures of this time and this place. Those we meet are usually those we live near and work with. When dreaming, on the other hand, we can meet far-off friends. We awaken refreshed by our flight from the here and now.

5. Taking the author's idea without acknowledging the source.

Dreams help us to satisfy another important psychic need - the need for a change. They liberate us from the here and now, taking us out of the world we normally live in....

If you quote anything at all, even a phrase, you must put quotation marks around it, or set it off from your text; if you summarize or paraphrase an author's words, you must clearly indicate where the summary or paraphrase begins and ends; if you use an author's idea, you must say that you are doing so. In every instance, you also must formally acknowledge the written source from which you took the material. **(This includes material taken from the World Wide Web and other Internet sources.)** Reprinted from "Writing: A College Handbook" by James A.W. Herrerman and John E. Lincoln. By Permission W.W. Norton & Co. Inc., Copyright 1982 by W.W. Norton & Co. Inc. Students are encouraged to report incidents of academic dishonesty to course instructors.

When academic dishonesty occurs, the following procedures will be followed.

A. The instructor will impose a minimum sanction of failure for the work involved. The instructor will notify the student and the appropriate academic dean/director in writing of the nature of the offense and that the minimum sanction has been imposed. The instructor may recommend to the dean that further penalties should be imposed. If further penalties are imposed, the dean/director will notify the student immediately and the student will have five working days to respond to the intention to impose additional penalties. The student has the right to respond to the charge of academic dishonesty and may request in writing that the dean review the charge of academic dishonesty as fully as possible. If the dean/director determines that no further sanctions will be applied, the instructor's sanction will stand and the instructor's letter to the dean/director and student will be placed in the student's file. If no further charges of academic dishonesty involving the student occur during the student's tenure at St. Thomas, the materials will be removed from the file upon graduation.

B. If the student has been involved in a previous incident of academic dishonesty, the dean will convene a hearing, following guidelines listed under “Hearings and Procedures” in the Student Policy Book. During the hearing, all violations of academic integrity will be reviewed. The student and the faculty member charging the most recent incident will be present at the hearing.

C. In either situation, A or B, if the dean/director determines that further sanctions are warranted, the student will be informed in writing. Among the sanctions considered by the dean/director will be the following: failure for the course in which the incident occurred; suspension from the university for the following semester; expulsion from the university; community service; a written assignment in which the student explores the principles of honesty and trust; other appropriate action or sanctions listed under “Sanctions” in the Student Policy Book. The materials relating to the incident including the instructor’s original letter to the student and dean and the dean’s decision following the hearing, will become part of the student’s file.

Students with Disabilities

In compliance with the University of St. Thomas policy and disability laws, I am available to discuss academic accommodations that you may require as a student with a disability. Students are encouraged to register with the Enhancement Program-Disability Services office for disability verification and for determination of academic accommodations. Please do so within the first two weeks of the term. Appointments can be made by calling 651-962-6315 or 800-328-6819, extension 6315. Telephone appointments are available as needed. You may also make an appointment in O’Shaughnessy Educational Center, room 119. For further information, you can locate the Enhancement Program on the web at <http://www.stthomas.edu/enhancementprog/>.

Recording of Classroom Activities

All recordings of class sessions using any device is expressly prohibited without the written permission of the instructor. (See **Class Session Recording Permission Form**.)