Syllabus for

IT-S448, ITMS448-02, ITMS548-02
System and Network Security Autumn 2014

Faculty Information

Instructor: Bill Lidinsky
Address: 201 E Loop Rd., Wheaton, IL 60419
Telephone: 630-682-6028
Fax: 630-682-6010
Office: Room 225 at IIT's Rice campus
Other times by appointment
Email: lidinsky@iit.edu

Course Catalog Description

Prepares students for a role as a network security administrator and analyst. Topics include viruses, worms, other attack mechanisms, vulnerabilities and countermeasures, network security protocols, encryption, identity and authentication, scanning, firewalls, security tools, and organizations addressing security. A component of this course is a self-contained team project that, if the student wishes, can be extended into a fully operational security system in follow-on courses (ITMS539 or ITMS549). Prerequisite: ITMO 440 or ITMO 540 (2-2-3) (**C**)

Homework and Exams

Homework assignments will be made on a week-by-week basis. All assignments will be submitted via Blackboard in Microsoft Word 2000. Unless otherwise specified, assignments will be due on or before 11:55 pm on the 2nd Monday following the date that it was assigned. This should accommodate most extenuating circumstances that students may encounter. Late homework will not be accepted.

There will be two exams: a midterm and a final.

Team Project

This course will have a significant team research/implementation project. Each team will normally consist of 2 or 3 students. The student teams with consent of the instructors will select projects from a project description document. The deliverables for each project are discussed in this document. We encourage a project that extends into IT-S549, ITMS 539 or ITMS549 during the spring 2015 semester. Two-semester projects can be much more rewarding to the student and are valuable when seeking employment.

Plagiarism will result in an automatic grade of E. This result can be avoided as follows:

Paper and Presentation:

- Your paper & presentation must contain your own words; not the words of others.
- If you wish to use the words of others, you may do so provided you do all three of the following:
    1. *Separate the words of others from your words.*
        - Either quote or indent the words & use different font styles.
    2. *Properly reference the words of others.*
    3. *Restrict words of others to <30% of your work.*
        - *i.e., >=70% must be your own work and words*

  You must be scrupulous about the above 3 items.

Team Project Implementation

In contrast to the paper and presentation, the implementation itself can consist of components gleaned from others. Today's systems are often comprised of smaller already developed subsystems "glued" together to achieve the overall system goals. In general your team project systems for this course should:

1. Use freeware or shareware whenever possible.
2. Be low in IIT.cost.
3. Have some custom software or scripts that integrate the shareware together into a single working system.
4. NOT be the installation and use of a single acquired system.

Prerequisites

- IT-O440, ITMO440, ITMO540 or consent of instructor
- A working knowledge or the use and internals of Windows or Linux or both.
- Programming or scripting ability

Credits

ITMS-enrolled students will receive, upon successful completion of the course, 3 semester hours of credit.
IT-enrolled students will receive 4.2 CEUs (Continuing Education Units).

Lecture Day, Time, and Place

Mondays from 1:50 - 5:20pm. Room 250 (ForSec Lab) at IIT's Rice campus in Wheaton IL.

Laboratory Day, Time, and Place

The laboratories will be integrated with the lectures during the lecture day, time and place.

Course Objective and Outcome

The goal of this course is to give the student an in-depth understanding of network and computer security. This in-depth understanding will include detailed working knowledge of all the important security topics.

A student successfully completing this course will have an excellent in-depth knowledge of network and computer security. A student with the knowledge gained in this course should be able to function in an entry or intermediate level security position. Also upon completion of this course, a student should be able to, with modest test preparation, acquire a Security+, SSCP, or other similar certification.

In addition, because of the team project, the student will become an expert in the specific facet of security associated with the team project. He/she should also have very practical experience in the development of a security system.

Book for This Course

W. Stallings, L. Brown, ***Computer Security: Principles and Practice Second Edition***, Prentice Hall, ISBN-10: 0-13-277506-9, ISBN-13: 978-0-13-277506-9.

Course Requirements

Requirements include attendance at class meetings or sessions (Lectures, labs and project work), homework, midterm and final exams, team project implementation, presentation and documents. Project can end at the end of the fall 2014 semester, but we will strongly encourage doing at 2-semester project.

Team project activities and deliverables are indicated in the Course Schedule. So are the dates of the two exams: midterm and final. Students will take the exams during the times and dates shown in the Course Schedule.

Grading

Grade weights will be as follows:

Midterm	20%
Final	25%
Homework	20%
Team project interim submissions	15%
Team project final submissions	20%

At the end of the class, the letter grades assigned will be based on the class average numerical grades (i.e., letter grades will be "curved").

Project Presentations

During the second class, each project team must make a brief PowerPoint presentation on their project. This presentation must include the following:

- One or two slides describing the project
- One or two slides presenting the problem or problems that your project is trying to address
- One to four slides showing your general approach.
- One slide showing your project plan on a Gantt chart. Include major milestones and who is doing what and when. Do not include too much detail. Show the entire Gantt chart on one slide.

After your presentation, post your PPT slides on Blackboard to the Discussion Board Forum for your project.
A second project presentation will be required approximately half way through the semester.

Three Key Documents

Before the fourth class, each team must submit to the course Blackboard Discussion Board forum for your project 3 key documents that have been significant to your research to date. These documents can be papers, chapters from books, etc. Do not just provide URLs. You must submit the entire documents. Do not submit documents that were listed in the *Project Description* document.

Technical Document (TecDoc)

The technical document for your team's project should have the following properties:

- Identify the problem that your project is trying to solve and describe how your project solves it.
- Describe in detail your implementation. There should be enough detail so that a knowledgeable person, after reading you paper, could re-implement your system.

First Draft of Technical Document (Due midway through the semester)

This draft will help you solidify your thoughts about what is to included in your team's work and get all members of the team coordinated and thinking in the same way. It will expose differing perspectives and help resolve them.

It total length should be 4 to 8 pages single-spaced. It must include title page, abstract page, body, and bibliography to date. Omit the acknowledgements and reference page for this submission only. The description is to be formatted according to the paper format information (except it's shorter). The submission should include your current ideas about how your paper will be organized including major sections and first level subsections. In each section and subsection include (1) a word description discussing **your vision of the contents** of the section and subsection, and (2) maybe some technical content. The last page will contain a bibliography to date. (Omit the Reference section for this submission.) This submission should include sections and subsections covering both relevant technical information and your project. Each subsection **must** have a statement in it regarding its expected page length (e.g., 1/4 page, 1.5 pages) in the final paper.

I want to emphasize that for this draft you do not need to have technical content for every section or subsection. But you do need to have technical content in some of the sections. But each section, whether it has technical content or not, must contain at the beginning your **vision** of what will likely be in that section. As an example, if you were writing a paper on the effects of full spectrum artificial lighting on worker efficiency, you might have the following section as sort of background information:

> **2. SEASONAL AFFECTED DISORDERS**
>
> In this section we will briefly review SAD research to date and the possible ways of treating it using lighting. Included will be both statistical and anecdotal studies. Since this is information preliminary to our actual work, we will keep the section brief. It should be, in the final paper, about 1 page in length.
>
> *< The above is then followed by the actual technical content for this section. >*

Include in an appendix for this 1st draft a Gantt chart for your work. It should include the following: all major tasks, the person or persons responsible for each major task, the elapsed time allotted to do the task and the time when the task needs to be done in order to complete the project. For type II teams, include your entire project continuing through May 2009, but show major deliverables by the end of this semester.

Penultimate Technical Document (Due week 12 of the semester)

This is the next to final technical document. It should be close to being finished. It must follow the technical document format that has been defined. There must be no empty or nearly empty sections or subsections.

Final Technical Document (Due week 14 of the semester)
The finished technical document.

User Manual (UsrMan)
Your user manual must be such that a knowledgeable person that is not familiar with your project can use your system. There should be step-by-step instructions, possibly with screen shots or complete command lines telling the reader how to proceed.

UsrMan submissions will be at the same times as the TecDocs.

Demonstrations and Accompanying Presentations
The demonstrations and their accompanying PowerPoint presentations are to show off your work and to show the reviewers and me that what you built works. They also can be used by you to show your work to potential employers. This will give you a competitive edge in employment interviews.

Initial Class Presentation (class session 4)
This presentation will be done in the ForSec Lab. You will have 15 minutes total to make your presentation. **Rehearse!** The PowerPoint presentation and must do the following:

1. Briefly define the problem. (1 slide)
2. Briefly discuss how your system solves the problem. (1-2 slides)
3. Briefly describe how your system works. (2-3 slides)
4. Provide a Gantt chart showing your project plan. (1 slide)

The number of slides excluding a title slide must be ≤ 7 slides.

Second Class Presentation and First Demonstration (class session 12)

This presentation and demo will be done in the ForSec Lab. Your project will not be finished at this point, so you may be able to demonstrate only part of your system. You will have 20 minutes total to make your presentation and do your demo. **Rehearse!** The PowerPoint presentation will precede the demo and must do the following:

5. Briefly define the problem. (1 slide)
6. Briefly discuss how your system solves the problem. (1-2 slides)
7. Briefly describe how your system works. (2-4 slides)
8. Tell and show with screen shots what we will see in your demonstration that will follow your presentation. (3-4 slides)

The maximum number of slides excluding a title slide must be ≤ 10 slides.

Final Class Presentation and Demo (class session 14)
This presentation and demonstration may or may not be done in the ForSec Lab. People outside our class will be invited to attend. You will have 30 minutes total for both your presentation and demo. Rehearse your combined presentation and demo. **Make it smooth!**

Your presentation will again precede your demo and must do the items identified above. In this presentation you must describe in more detail how your system works. You may have up to 12 slides this time.

For **T1** teams, your demo must show your entire system. For **T2** teams you must show a partially working system and explain your project plans for the following semester.
(Note: To do all the projects during a single session may be difficult. We may need to rearrange the schedule to present and demo projects on two evenings.)

ForenSecure15
T2 teams are required to present and demonstrate their project at the ForenSecure15 conference in April 2015 at IIT's Rice campus. **T1** teams are encouraged to do the same. This is a conference that has technical presentations by working professionals, exhibits by corporations and other organizations and to which the public is invited. In the past student exposure at this conference has frequently yielded job offers, once or twice on the spot.

Presentations by themselves will be about 20-30 minutes each and will be in the Rice auditorium. Demonstrations will follow all the presentations.

Class Schedule

Session	Topics
#01 Mon 25aug14	CourseIntro. FollowOnCourses. ForSecLabX48. Steganography. Project Descriptions *On Monday 25 August, we must do the following: (1) Determine team members,* *(2) Decide if your team is type T1 or T2, (3) Choose team projects*
Mon 01sep14	**Labor Day Holiday.**
#02 Mon 08sep14	SecurityIntroduction *In class each team presents their project and their initial plan.* *Class will **not** be held in room 250 on this date only.*
#03 Mon 15sep14	Virus lecture. Virus lab
#04 Mon 22sep14	Attacks. Attack mechanisms. *1st Interim Submission: Teams make 10 min. PowerPoint presentations in class on projects* *Submit PowerPoint files to Bb.* *Each team will receive feedback on their project immediately after each presentation.* *Teams submit 3 documents of significance to Bb (the documents themselves) plus references.*
#05 Mon 29sep14	Secret Writing 1 *Reviewers defined.* *Technical format for project documentation. 1st team mtgs individually with Instructor*
#06 Mon 06oct14	Secret Writing 2. PGP
13oct14	**Fall Break**
#07 Mon 20oct14	Review for midterm. Review homework assignments *2nd Interim submission:* *1st Drafts: Teams submit 1st TecDoc, UsrMan & PPT to Bb.* *2nd meeting with individual teams to discuss projects. Same drill as on 29 Sept.*
#08 Mon 27oct14	**MIDTERM EXAM**
#09 Mon 03nov14	Midterm review. VNC lecture & lab
#10 Mon 10nov14	Authentication, identification, access control Part 1 Crack passwords lab
#11 Mon 17nov14	Authentication, identification, access control Parts 2 & 3 Internet security protocols Firewalls. VPNs
#12 Mon 24nov14	*This class session will be devoted entirely to team project presentations and demonstrations.* *Teams must have their demonstrations working and very close to completion.* *3rd meeting with individual teams to discuss projects. Teams demo their projects.* *2nd Penultimate Drafts: Teams submit 2nd TecDoc & UsrMan to Bb to their project Discussion board.*
#13 Mon 01dec14	***Final Project Demos & Presentations:*** ***Each team makes final Pres followed by final Demo of their project*** *FinalSubmission: Teams submit their final Pres, TecDoc and UsrMan to Bb.*
Mon 08dec14	**FINAL EXAM (see note)** *Note: The final exam may be on line, in which case there will be no meetings during final week.*

Legend *Blue sans serif italic font refers to the project activities & deliverables.*
Black serif font refers to lectures & labs.

NOTES 1. On Monday 08sep 2014 we will meet in a lecture room at Rice that is not the ForSec Lab. The room number is to be determined.