ITMS 448/548 Cyber Security Technologies
Fall 2014 Syllabus - Section 01
V3 - Updated 9/18/2014

Instructor: Shawn Davis
Contact Email: sdavis17@iit.edu
Rice Campus Office Hours: By appointment via email

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 one of two follow-on courses (ITMS549 or ITMS539).

Prerequisites: ITMO 540 or Consent of Instructor

Credit: 2-2-3 Semester Hours

Course Day/Time: Wednesday Evenings from 5:30 PM – 9:05 PM
Course Location: IIT Rice Campus in Wheaton, IL - Room 250

Lectures/Labs, Projects:
Each class will typically be broken up into two sessions:
-Session A: Lecture/Lab
-10 Minute Break
-Session B: Team Project Time

Required Textbook:
Computer Security: Principles and Practice, 2nd ed
By: W. Stallings, L. Brown
Publisher: Prentice Hall
ISBN-10: 0132775069

Course Objective/Outcome:
Each successful student will gain an in-depth understanding of various important network and computer security concepts and practices. Additionally, each student will become an expert in the specific facet of security associated with her/her team project. Students, through their course exams and team project presentations, will demonstrate the ability to apply information assurance and security concepts, specifically on the topics of malware analysis, attack vectors, mitigation/deterrents, cryptography, Stego basics, firewalls, IDS/IPS, internet security protocols, authentication, and wireless network security.

Lecture Notes:
Copies of the course lecture notes in the form of a PDF of the PowerPoint presentation accompanying each lecture will be provided for each student on Blackboard. No video lectures will be provided.
# ITMS 448/548 Cyber Security Technologies
## Fall 2014 Syllabus - Section 01

**Schedule of Topics/Readings:**

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic/Lab (Assigned Reading)</th>
<th>Activities (Project Activities)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Aug 27</td>
<td>Course Intro, Follow-on Courses, RADISH, Security Overview (<a href="#">Read Ch. 1</a>)</td>
<td>Initial team meeting to gather infrastructure and start setting up project workspaces. Ensure remote access to project. Elect Team leader.</td>
</tr>
<tr>
<td>2</td>
<td>Sep 3</td>
<td>Malware Overview, Exploit Kits (<a href="#">Read Ch. 6</a>)</td>
<td>Team project time. Create GANTT chart.</td>
</tr>
<tr>
<td>3</td>
<td>Sep 10</td>
<td>Malware Analysis (No Reading)</td>
<td>Team project time. (GANTT chart due to Blackboard (Bb) before class.)</td>
</tr>
<tr>
<td>4</td>
<td>Sep 17</td>
<td>Attack Vectors &amp; Mitigation Techniques (<a href="#">Read Ch. 7</a>)</td>
<td>Team project time. Create 1 page progress report.</td>
</tr>
<tr>
<td>5</td>
<td>Sep 24</td>
<td>Attack Vectors II &amp; Mitigation Techniques (No Reading)</td>
<td>Team project time. (1 page progress report due to Bb before class.)</td>
</tr>
<tr>
<td>6</td>
<td>Oct 1</td>
<td>Cryptography (<a href="#">Read Ch. 2 &amp; 20</a>)</td>
<td>Team project time. Create 1\textsuperscript{st} draft of TechDoc.</td>
</tr>
<tr>
<td>7</td>
<td>Oct 8</td>
<td>Crypto (Cont.), Stego Basics, Midterm Review (<a href="#">Read Ch. 21</a>)</td>
<td>Team project time. (1\textsuperscript{st} draft of TechDoc and GANTT due to Bb before class)</td>
</tr>
<tr>
<td>8</td>
<td>Oct 15</td>
<td>Midterm Exam (No Reading)</td>
<td>Teams work on 10 min interim PowerPoint with status and initial working demo of project.</td>
</tr>
<tr>
<td>9</td>
<td>Oct 22</td>
<td>Firewalls (<a href="#">Read Ch. 9 [except 9.6]</a>)</td>
<td>Teams present interim PowerPoint and demos to class (submit PowerPoint to Bb before class.)</td>
</tr>
<tr>
<td>10</td>
<td>Oct 29</td>
<td>IDS/IPS (<a href="#">Read Ch. 8 &amp; 9.6</a>)</td>
<td>Team project time. Create 2\textsuperscript{nd} draft of TechDoc.</td>
</tr>
<tr>
<td>11</td>
<td>Nov 5</td>
<td>Internet Security Protocols, Internet Authentication Applications (<a href="#">Read Ch. 22 &amp; 23</a>)</td>
<td>Team project time. (2\textsuperscript{nd} draft of TechDoc and GANTT due to Bb before class.)</td>
</tr>
<tr>
<td>12</td>
<td>Nov 12</td>
<td>Wireless Network Security &amp; Attacks (<a href="#">Read Ch. 24</a>)</td>
<td>Team project time.</td>
</tr>
<tr>
<td>13</td>
<td>Nov 19</td>
<td>User Authentication, Access Control (<a href="#">Read Ch. 3 &amp; 4</a>)</td>
<td>(Final version of TechDoc due to Bb before class.) Each student assigned one team’s TechDoc to evaluate.</td>
</tr>
<tr>
<td>14</td>
<td>Nov 26</td>
<td>Thanksgiving Break - No Class</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Dec 3</td>
<td>Final Presentations &amp; Demos of Projects, Brief Final Review (No Reading)</td>
<td>Teams present final version of PowerPoint and working demo to class (submit to Bb before class.) Students will evaluate all presentations via Bb survey during class.</td>
</tr>
<tr>
<td>16</td>
<td>Dec 10</td>
<td>Final Exam (No Reading)</td>
<td>Evaluation of other team’s TechDoc due to Bb before class.</td>
</tr>
</tbody>
</table>
ITMS 448/548 Cyber Security Technologies
Fall 2014 Syllabus - Section 01

Attendance:
This course focuses heavily on group project work and therefore attendance is required. Absences may affect your final grade.

Readings:
Readings for the class will be assigned from the textbooks; there may be additional reading assigned in the form of online reading.

Homework:
Homework may be assigned in the form of labs or questions/problems from the textbook or other sources and will be published and submitted on Blackboard. Most homework will be due prior to the 5:30 PM start time of the second class following the assignment. Two weeks are given to complete each homework assignment to accommodate most extenuating circumstances that students may encounter. Late homework will therefore not be accepted. All homework answers must be completely in the student’s own words. No direct quotes are allowed. Paraphrasing is allowed if a source is cited.

Examination:
The midterm and final examination will consist of multiple choice, fill-in-the-blank, short answer, and short essay questions. Questions will be based on the course materials for each topic. Both exams are closed-book/closed-notes. Students need to be present for exams as make-ups are not permitted.

Grading: Grading criteria for ITMS x48 students will be as follows:
A Outstanding work reflecting substantial effort ................................................................. 90-100%
B Undergraduate/IT Students: Excellent work reflecting good effort .................. 80-89.99%
B Graduate Students: Satisfactory work fully meeting expectations .................... 80-89.99%
C Undergraduate/IT Students: Satisfactory work meeting minimum expectations ...... 70-79.99%
C Graduate Students: Substandard work not meeting expectations .................... 65-79.99%
D Undergraduate/IT Students: Substandard work not meeting expectations ...... 60-69.99%
D Graduate Students: Graduate students may not be assigned a D grade ............. N/A
E Undergraduate/IT Students: Unsatisfactory work ............................................. 0-59.99%
E Graduate Students: Unsatisfactory work ............................................................. 0-64.99%

The final grade for the class will be weighted as follows:
Homework .................................................................................................................. 20%
Team Project Interim Submissions ........................................................................ 15%
(1st and 2nd drafts of Technical Reports, Interim PowerPoint, Progress Report, Demo)
Team Project Final Submission/Presentation ...................................................... 20%
(Final version of Report and PowerPoint, Final Demo)
Evaluation of all Team Presentations and of a Single Other Team’s Paper ............. 10%
Midterm Exam ......................................................................................................... 15%
Final Exam .............................................................................................................. 20%
Plagiarism:
All work submitted by students must be their own. Plagiarism will normally result in an automatic grade of zero for the assignment and an Academic Dishonesty Report filed.

IIT Code of Academic Honesty:
Please review and be familiar with the Code of Academic Honesty which can be found at the below URL: http://www.iit.edu/student_affairs/handbook/information_and_regulations/code_of_academic_honesty.shtml

Documentation Style:
The selected documentation style for reports and technical documents for this class is APA.

Other Class Resources:
Online readings and other class resources are on http://blackboard.iit.edu.

Computer Use Policies:
Please ensure that you have read and understand the IIT and ITM Network and Computer Use Policies found at http://www.itm.iit.edu/data/ITMComputerUsePolicies.pdf.

Americans with Disabilities Act (ADA) Policy Statement:
Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone: 312.567.5744 or disabilities@iit.edu.

Project Deliverables for Each Team:
One member of each team must upload their project deliverables to their team’s folder under the Blackboard (Bb) “Groups” menu prior to the indicated due date. Late project deliverables will not be accepted past their indicated due dates on this syllabus.

1. **GANTT Chart** (Due to Bb before class on Sep. 10th)
   a. First, determine all of the tasks necessary to complete the project.
   b. This chart should show the following:
      i. List of tasks and subtasks.
      ii. Bar chart of when tasks and subtasks will be started and estimated date of completion.
      iii. What group members will be working on which tasks.
      iv. Percentage of completion in list and bar chart of tasks.
   c. Example of one task and subtasks (you will have many and the bar chart will cover the entire semester (or two if you have a two semester project):
d. GANTT will be updated throughout the semester.

2. **Progress Report** (Due to Bb before class on Sep. 24th)
   a. 1 page report providing me an update as to how things are progressing and any issues that may be occurring.

3. **1st Draft of TechDoc and Updated GANTT Chart** (Due to Bb before class on Oct. 8th)
   a. The TechDoc is a technical report you will be starting now and adding to over the semester (or year for 2 semester projects.) This first draft will help you solidify your thoughts about what is to be involved in your team's work and to get all members of the team coordinated and thinking in the same way. It will expose differing perspectives and help resolve them.
   b. Total length should be 4 to 8 pages single-spaced. It must include title page, abstract page, body, bibliography to date, references, and 2 appendixes. The first appendix will include your team’s updated GANTT chart. The second appendix will include a user manual. (Over the course of the semester, be sure to document all steps taken in getting your project from an idea to a working demo.)
   c. The submission should include how your paper will be organized and include major sections and first level subsections in the body. In each section and subsection include (1) a brief description discussing your vision of the contents of the section and subsection, and (2) maybe some technical content. Update your bibliography and references page. Remember, a bibliography is a list of sources that you used in researching the project whether cited or not. The references page should only contain sources cited within the report. For this first draft you may not have any content in your references page which is okay. The GANTT appendix should be updated and your User Manual appendix should have at least the initial steps you have taken.
   d. Each subsection must also have a statement in it regarding its expected page length (e.g., 1/4 page, 1.5 pages) in the final paper.
   e. 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 each section.
4. **Interim PowerPoint and Project Demo** (Presented in class on Oct. 22\textsuperscript{nd}. PowerPoint due to Bb before class starts that day. If a software project, current version of software due to Bb before class as well)
   a. 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. Your team will have 20 minutes total to make your presentation and do your demo. **Rehearse**! The PowerPoint presentation will precede the demo and must include the following:
      • Briefly define the problem your project is attempting to solve. (1 slide)
      • Briefly discuss how your system solves the problem. (1-2 slides)
      • Briefly describe how your system works. (2-4 slides)
      • Tell and show with screen shots what we will see in your demonstration that will follow your presentation. (3-4 slides)
   b. The maximum number of slides excluding a title slide must be \leq 10 slides.
   c. Execute a live or recorded demonstration.

5. **2\textsuperscript{nd} Draft of TechDoc and Updated GANTT Chart** (Due to Bb before class on Nov. 5\textsuperscript{th})
   a. The 2\textsuperscript{nd} draft of the technical report must follow the format that I defined for the 1\textsuperscript{st} draft. This draft should contain full content and be close to the level of completion that your final draft will have. There must be no empty or nearly empty sections or subsections.
   b. Your GANTT chart should be updated with percentages of task completion.
   c. I may provide feedback on your 1\textsuperscript{st} draft that you should take into account for this draft.

6. **Final Version of TechDoc** (Due to Bb before class on Nov. 19\textsuperscript{th})
   a. This is the completed technical report.
   b. I may provide feedback on your 2\textsuperscript{nd} draft that you should take into account for this draft.
   c. The final technical report should not include a GANTT chart.

7. **Final PowerPoint and Project Demo** (Presented in class on Dec. 3\textsuperscript{rd}. Final PowerPoint due to Bb before class starts that day. If a software project, final version of software due to Bb before class as well)
   a. This presentation and demonstration may or may not occur in the ForSec Lab. People outside our class may be invited to attend. You will have 30 minutes total for both your presentation and demo. **Rehearse** your combined presentation and demo. **Practice and make it smooth!**
   b. Your presentation will again precede your demo and must include the type of items identified in the Interim presentation above. In this presentation you must describe in more detail how your system works. You may have up to 14 slides this time.
c. For one semester project teams, your demo must show your entire system. For two semester project teams you must show a partially working system and explain your plans for your follow-on course during the spring 2014.

d. (Note: We will try to have all project presentations on Dec 3rd. If necessary, we may need to have 1 or 2 groups present after the final exam on Dec. 10th.)

8. Project Presentation & Demo Evaluations
   a. On Dec. 3rd, as teams are presenting, every student will evaluate each presentation and demo via a Blackboard survey. The survey must be submitted before the end of class. Teams do not need to self-evaluate their own presentation/demo.

   a. On Nov. 19th, each student will be assigned to evaluate one team’s TechDoc and provide their responses via a separate Blackboard survey. These evaluations are due before the Final Exam on Dec. 10th.

ForenSecure15:
Two semester project teams are required to present and demonstrate their project at the ForenSecure15 conference in April 2015 at IIT’s Rice campus. One semester project teams that have successful projects will be asked 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 of the presentations and will take place outside the ForSec Lab.