Preliminary Syllabus for INFO I533/CSCI B547
The Design and Analysis of Secure Protocols and Systems & Information Assurance
Spring 2017

Instructor: Steven Myers
AI: Omkar Bhide
Email: samyers@indiana.edu
Email: okbhide@umail.iu.edu
Office Phone: (812) 856-1860
Twitter: @Cryptolicious (Links to an external site.)
Office hours: By appointment in person, via telephone, or videoconference

Communication

Please use Canvas Inbox email to contact me about course issues. I am in the course at least once a day Monday-Friday. I will normally check in at least once over the weekend.

If you email me at the @indiana email address, please ensure that 'I533' or 'B547' appears in the topic. If it does not, there is no guarantee that your email gets past my spam filter, gets read in a timely manner, or gets read at all. If you email asking a question that is covered in the syllabus, I will not reply. For more than the simplest of questions, please schedule a time to meet with me or your AI. Writing long monologues via email is too time consuming, and I’ll probably redirect you to office hours with me or Omkar (in person or remote) anyway. Further, I get a better sense of the actual problems when we are working in real-time.

This course is entirely in Canvas. All announcements, grade notifications, discussion activity, etc. will reach you via Canvas notifications. Please make sure you are set up to receive emails and notifications from Canvas at an address/phone number you will actually check.

Motivation

With the increasing number of people, businesses, governments and organizations using the Internet, the Cloud, the IoT and information technology for a growing number of their operations, the need to ensure that these systems are secure is becoming more and more essential. While understanding the specific security aspects of different technologies such as firewalls, operating systems, cryptography, secure development, etc. are essential to designing secure systems, it is not sufficient. In particular, a systems designer must be able to integrate these technologies in appropriate ways to ensure the resulting system is secure. Many people improperly believe that if they include enough security technology the resulting system will magically be secure, without giving thought to what problems these technologies both solve and create.

In this course, we will cover the design and analysis of secure systems including identifying security goals and risks, risk management, risk analysis and treat modeling, defense in depth, integrating different
technologies to achieve security goals, developing security protocols & policies, implementing security protocols and secure coding. In short, how does one take all of the security technologies, secure development practices and protocols and integrate them into a functioning whole? To do this, we also need to understand how most of the modern attacks function, including writing zero-day attacks. For it is difficult to understand how to protect a system, if you don’t understand the major attacks that are currently being deployed.

In this course, we will consider some real world scenarios that have many security requirements. We will require the use of many security technologies and protocols, determine the requirements necessary to solve the security requirements, and then consider how to design systems and protocols to achieve these requirements. In particular, we will start with defining some vague security requirements for a system to be implemented, and then consider the development process from the highest levels of planning hardware and software requirements, staff security policy, etc., to the lowest level of writing secure code, and then finally the testing process.

Prerequisites

A reasonable programming background is necessary. A course in operating systems, networking and computer architecture are helpful but not necessary. You are not required to know any particular language, but rather it is assumed you can pick up new languages if needed for the course. In particular, you will be programming in C, x86 AMD64 assembly language, shell scripts and potentially other languages, as well as using related tools during this course. Basic knowledge on cryptographic primitives such as what symmetric-key and public-key encryption, digital signatures, and cryptographic hashes is also assumed.

Textbooks

The course textbooks are:

*Threat Modeling: Designing for Security*

by Adam Shostack, Wiley
Computer Security, Principles and Practice Third Edition
by William Stallings and Lawrie Brown, Prentice Hall

Even though the above are the course texts and readings will be assigned from them, they are far from perfect resources. Therefore, there will be readings and other resources given throughout the term from other sources. Further, since we can only delve in to the many different security topics at a fairly low depth, the following texts go in to some of the topics of this course in significantly more detail. Thus, students interested in further reading may find the following texts interesting.

- Introduction to Computer Security, by Math Bishop, Addison Wesley
- Security Engineering (Second Edition), by Ross Anderson (Links to an external site.), available free online
- Secure Programming with Static Analysis, Brian Chess and Jacob West, Addison
- The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, John Sammons, No Starch

Other Requirements

In addition to the course texts you need to have access to a

High-level Syllabus
No battle plan ever survives contact with the enemy.

– Helmuth von Moltke

Below is a rough syllabus of the topics I intend to cover. However, this is only a guideline, and we will most likely deviate from it. I will make updates to this section as we go along, so please check the course home page and keep up with all course announcements for a more specific timeline and future readings.

1. Security & privacy: goals, principles & excuses; costs of security & insecurity; risk management
2. Risk analysis: threat & adversary modeling (high-level)
3.
4. Access control in operating and data management systems
5. OS memory protection, stack call frames, link library tables
6. Buffer overflows, shell code, and related attacks
7. Penetration testing
8. Logging and auditing
9. Secure coding practices
10. Software Security, OS hardening, patching, CVEs and other strategies.
11. Passwords & authentication mechanisms
12. Forensics
13. Privacy technologies

Assignments

There will be several assignments (3-5) that allow students to show mastery of technical parts of the course. These assignments will have portions that need to be completed individually and may have portions that need to be completed in small groups.

Lab Assignments

Most weeks your lab will have an assignment where students will need to demonstrate their ability to perform certain tasks in the lab, or commenced in lab and finished on the student’s own time. Unless specifically stated otherwise, each individual assignment will have the same weighting. Lab assignments are due at the next regularly scheduled lab session, unless otherwise stated.

Readings

Every week there will be readings assigned, based on our expected progress. These readings will be announced in class, and on Canvas. **The expectation is that students will arrive to class having done the assigned readings, and students will be called upon in class to lead the discussion of reading.** There may also be quizzes given to assess students on readings. These quizzes will be given with no prior warning (other than this one).
Just-in-time (JIT) Quizzes

I may use just-in-time quizzes to ensure that students are reading material before class, and following material discussed in class. In this case, you will be notified of an online quiz to be performed through Canvas before the next class. All JIT quizzes will have the same value.

Final Exam

There will be a final exam for this course. It will be at the registrar scheduled time for this course. **While the final exam is only worth 30% of your grade, you must achieve a grade of 45% on it to pass the course.**

Grading

- Final Exam 30%
- Weekly Labs 20%
- Assignments 30%
- Reading, Just-in-time quizzes, and class participation 20%

Important Dates

- Martin Luther King Jr. Day: January 16th
- Spring Break: March 12 - 20
- Final Exam: TDB

For more information, please see the [IUB Registrar's Academic Calendar](https://www.indiana.edu/~registrar/academic/). For more information, please see the [IUB Registrar's Academic Calendar](https://www.indiana.edu/~registrar/academic/).

Plagiarism

I may encourage, if not expect, you to work in groups to solve the assignments. However, each student must write up their own set of solutions to assignments (unless specified otherwise) and these write-ups must be done individually and without the aid of any notes that resulted from such group work. Finally, you should not write up any solutions within three hours of a group meeting or discussions with your classmates. I advise that students read the [Code of Student Rights, Responsibilities, & Conduct](https://www.indiana.edu/~registrar/codeofconduct/). to understand issues of plagiarism. **No assignments will be marked until you affirm in your first assignment that you have read the IU student code.** Working in groups does not mean that you cannot plagiarize. There is a [small online resource here that goes over issues of plagiarism](https://www.indiana.edu/~registrar/codeofconduct/)., if you have any doubts.

Accommodations for Students with Disabilities

Every attempt will be made to accommodate qualified students with disabilities (e.g. mental health, learning, chronic health, physical, hearing, vision, neurological, etc.) You must have established your
eligibility for support services through the appropriate office that services students with disabilities. Note that services are confidential, may take time to put into place, and are not retroactive. Captions and alternate media for print materials may take three or more weeks to get produced. Please contact your campus office (Links to an external site.)Links to an external site, as soon as possible if accommodations are needed. For accessibility information for persons using adaptive technology with Canvas, please visit Canvas Product AccessibilityLinks to an external site.

Technology Support

For Canvas questions please see the "Help" link at the top right of the page and check the UITS Knowledge BaseLinks to an external site, for more information (type “Canvas” in the search box for a full list of Canvas-related topics).

If you have any other questions about or issues with any of the technology used in this course please contact the University Information Technology Services (UITs) support team. At IUPUI you can contact the support team by the following ways:

- Call 812-855-6789
- Email ithelp@iu.edu
- Live Chat at http://ithelplive.iu.edu/Links to an external site.
- Walk in at Learning Commons, Herman B Wells Library

Course Summary:

<table>
<thead>
<tr>
<th>Date</th>
<th>Details</th>
</tr>
</thead>
</table>
| Fri Jan 15, 2016 | Lab #1 Assignment  | due by 12pm
|                | Assignment #3      | due by 12:01pm
|                | Lab #2 Assignment  | due by 11:59pm
|                | Lab #3 Assignment  | due by 11:59pm
<p>|                | Lab #6 Assignment  | due by 11:59pm |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Details</th>
<th>Due By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Jan 18, 2016</td>
<td>Assignment #2 (Static Analysis and Secure Coding)</td>
<td>9am</td>
</tr>
<tr>
<td></td>
<td>Final Exam</td>
<td>11:59pm</td>
</tr>
<tr>
<td></td>
<td>Lab #4 Assignment</td>
<td>11:59pm</td>
</tr>
<tr>
<td>Fri Jan 20, 2017</td>
<td>Elevation of Privilege Game</td>
<td>11:59pm</td>
</tr>
<tr>
<td></td>
<td>Assignment #1 (Buffer Overflows in Assembly)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Final Exam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Midterm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Participation: Day 1 - Midterm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Participation: Midterm - End of Course</td>
<td></td>
</tr>
</tbody>
</table>