Important Information

Instructor: Dr. Mike Rosulek  
<rosulekm@eecs.oregonstate.edu>

Teaching assistant: Zhangxiang Hu  
<huz@eecs.oregonstate.edu>

Meeting time: MWF 10

Classroom: KEC 1003

Website: http://eecs.oregonstate.edu/~rosulekm/netsec  
Please check often for links, announcements, homeworks, etc.

Office hours: To be announced.

How to Succeed in this Course

• There are some “easy points” available: attendance quizzes, and the early deliverables of the final project. Make sure you max out on these easy points! Note: those are the only easy points. All other points will be hard-earned.

• Don’t be caught off guard that homeworks are worth so much of your final grade! Take homeworks seriously, start them early, and submit solutions that you are proud to put your name on. If you start getting discouraged at the homeworks, realize that there are no exams (and if the homeworks are hard, just imagine what kind of exams I would write).

• This is a 400-level course for mature students. The lectures are not meant to be complete recipes for completing the homeworks. Even if you understand 100% of the lectures, be willing to do additional reading/learning on your own when you encounter new twists.

• Don’t think of office hours as “remedial instruction.” They are an additional resource available to you, just like a textbook or the internet. Take advantage of this effective resource! It’s quite useful to have availability of someone who knows and enjoys talking about the course material.
**Rough Schedule**

- week 1: Web application security: cross-site scripting attacks
- week 2: Web application security: SQL injection attacks etc
- week 3: Applied cryptography: data privacy
- week 4: Applied cryptography: data integrity
- week 5: User authentication & session management
- week 6: Advanced protocols: some subset of {DNSsec, IPsec, TLS, SSH, Tor}
- week 7: Large-scale attacks: bot-nets, denial of service
- weeks 8-10: Student projects

**Homeworks**

There will be several (6 ± 1) homeworks throughout the quarter. They are meant to assess but also expand your understanding of the material.

You may ... work in groups to understand the questions, study ideas, and develop answers

... consult external resources

You must ... write & submit your own solution

... type your solution (this is a great excuse to teach yourself \LaTeX)

... include the following “disclaimer” in your submission:

> This submission reflects my own understanding of the homework and solutions. All of the ideas are my own, unless I explicitly acknowledge otherwise.

... explicitly acknowledge all resources & assistance (other than lecture / office hours) that influenced your solution.

You may not ... share solution writeups with others, or accept solution writeups from others

... implicitly or explicitly take credit for the work/ideas of others (this is plagiarism)

**Final Project**

Students will work in teams of 2 on final projects. In weeks 8–10 of the course, teams will also give a presentation of their findings.
**Topic:** Your project should address either a **vulnerability** (a property of a system whose exploitation has the potential to cause harm) or a **countermeasure** (actions taken to mitigate a vulnerability). You should stay within the realm of network security, although I interpret “network” quite loosely.

Here are some topic ideas that I came up with, but you are welcome (encouraged) to choose others, with approval.

- Certificate framework of the web, 2-factor authentication, cross-site request forgery attacks, buffer overflow attacks, integer overflow attacks, format string attacks, side-channel attacks (length, timing, etc), securing internet routes (BGP), man in the middle attacks on SSL, intrusion detection, alternative approaches to authentication like OpenID, CBC padding-oracle attacks, spam mitigation proposals, digital currency, VPNs, attacks on WEP/WPA wifi protocols, perfect forward secrecy (off-the-record messaging)

**Writeup:** Your team will make a written document, on the order of 5-10 pages, describing the topic. This writeup can be a simple document, though it could also be in the form of a website and could even be interactive.

I strongly encourage you (though this is not required, and will not factor into grading) to make a highly polished, **publicly available** website that will benefit the wider community. Think something with the scope/quality of http://excess-xss.com/.

**Presentation:** Your team will have 25 minutes (half of one lecture) to present your findings. In fairness of all teams, the time limits will be **strictly enforced**. There are 8 lectures$^1$ × 2 slots per lecture = 16 slots available. If the number of enrolled students differs from 32, I will adjust team sizes or number of presentations appropriately.

Make your presentations as engaging/interactive as possible! Don’t just talk about attacks, **show** attacks in action! Give live demonstrations, similar to those presented in lecture. If possible, teach the audience how an attack works, and get them to actually carry out simple versions of the attack. In general, be creative in how you make your presentation engaging.

Even if you are discussing a countermeasure, you can motivate why the countermeasure is necessary by describing an attack that is possible without the countermeasure.

**Deadlines:**

Apr 25: **Proposal:** Submit for approval (1) the members of your team, (2) a few sentences describing your proposed project topic, (3) at least 2 sources that will be used.

May 2: **Outline:** Submit 1-page outline of the project writeup, and 1-page outline of presentation. Describe the figures/screenshots, links, demonstrations that will be included.

May 16: **Sign up** for a presentation slot.

variable (one week before presentation) **Presentation dry-run:** Schedule a time to meet with the instructor & TA to review slides, demonstrations, and overall presentation plan.

Jun 4: Submit **draft of the complete writeup**.

Jun 11: Submit **final version of the writeup**.

$^1$no class Monday May 26, in observance of Memorial Day.
Letter Grades

Your final grade in the course will be computed from the following categories:

- 50% homeworks
- 40% final project
- 10% “attendance” quizzes

A final grade of 90% in the class will guarantee a letter grade of A- or above, 80% will guarantee a B- or above, etc.

However, since your instructor is not always the best judge of homework difficulty, letter grade cutoffs may be adjusted in favor of the students. If there is great unrest about letter grades, I can present some hypotheticals (“if I had to assign letter grades today, ...”).

Other Policies

Cheating: Academic dishonesty (including plagiarism and cheating) will not be tolerated. Consult the university's student conduct code for more details. I will follow the guidelines given there, and seek out the maximum allowable penalty for violations that occur in this course.

Accommodation of Disabilities: Accommodations are collaborative efforts between students, faculty, and Disability Access Services (DAS). Students with accommodations approved through DAS are responsible for contacting the faculty member in charge of the course prior to or during the first week of the term to discuss accommodations. Students who believe they are eligible for accommodations but who have not yet obtained approval through DAS should contact DAS immediately at 737-4098.