CS 5434: Defending Computer Networks

Fall 2015

Instructor: Stuart Staniford
sgs235@cornell.edu
(backup: stuart@cayuganetworks.com)
http://www.cs.cornell.edu/~sgs235/

Course Description and Syllabus

Brief Description:

In this course, we discuss attacks on operational computer networks, with a focus on how to prevent them, or detect them if we fail to prevent them; study the reasons why real-world software tends to be vulnerable, and how attackers exploit those vulnerabilities; talk about the lifecycle of network attacks – methods of reconnaissance, gaining control of bulk volumes of computers via scanning, by worms, or by client-side attacks such as drive-by downloads from malicious websites; discuss the control of the resulting botnets of computers and the motives of attackers such as criminal syndicates and intelligence agencies; cover network-level defenses such as firewalls, encryption and virtual private networks; cover technical approaches for detecting attacks both on the network and on the host; talk about legal and ethical issues for network defenders.

Course Prerequisites:

- CS 2022 or equivalent, (C language)
- CS 3410 or equivalent (Architecture),
- CS 4410 or equivalent (Operating Systems),
- Or consent of instructor.

Note that class assignments are conducted in C (mainly) and Javascript. C programming is a prerequisite to the course. We will provide a very short tutorial introduction to Javascript, but you should be prepared to do additional study if that language is unfamiliar. Both languages are tools every contemporary computer scientist should be able to use.

Lectures:

Tuesday/Thursday 10:10am-11:25am.
Olin 165

Class Website (live soon):

http://www.cs.cornell.edu/courses/cs5434/2015fa/

Instructor Office Hours:
Tuesday 11:30-12:30, Gates 335.

Teaching Assistants: Zhiyuan Teo (zt27@cornell.edu) + TBD.

Piazza: To be set up.

Rough Lecture Syllabus:
1. The technical nature of software vulnerabilities and techniques used for exploiting them.
2. The pressures of commercial software development, and why firms very rarely produce secure software, even though they should.
3. Basics of monitoring a network, intro/refresher on TCP/IP. Switches, wireless access devices, routers.
4. Network reconnaissance techniques – ping sweeps, port scans, etc.
5. Algorithms for detecting port scans on the network.
6. Firewalls and network segmentation as a defense against inbound attacks.
7. Detecting exploits with string matching approaches (Snort and similar).
8. Network layer approaches to evading detection.
9. Large scale attacks – worms and distributed denial of service.
10. HTTP client attacks as a way around the firewall. Drive-by downloads and social engineering.
11. Defending against HTTP client attacks. Web-proxies, in-browser defenses, anti-virus systems.
12. HTTP Server attacks – cross site scripting, injections, etc.
13. SMTP attacks – spear-phishing, and defenses against it.
14. HTTPS: Encryption and virtual private networks as a means to maintain confidentiality.
15. The modern enterprise network: what a large-scale network looks like, and emerging trends affecting it (BYOD, cloud).
16. Legal and ethical issues in defending networks.

Reading Materials
There is no textbook for the course. Instructor lecture Powerpoints will be available online for most lectures. However, these should not be viewed as a substitute for your own note-taking.

There will be assigned readings of papers, which comprise part of the course material and which you may be quizzed on. The assigned readings for the first few lectures are:

- Aleph1. *Smashing the Stack for Fun and Profit*. http://www-inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf

- Matt Connover. *w00w00 on heap overflows*. http://netsec.cs.northwestern.edu/media/readings/heap_overflows.pdf
- Scut. *Exploiting Format String Vulnerabilities*. http://crypto.stanford.edu/cs155/papers/formatstring-1.2.pdf
- Blexim. *Basic Integer Overflows*. http://www.phrack.org/issues.html?issue=60&id=10
- Mitre. *Common Weakness Enumeration*. http://makingsecuritymeasurable.mitre.org/docs/cwe-intro-handout.pdf
- Steve Christey. *Unforgivable Vulnerabilities*. http://cwe.mitre.org/documents/unforgivable_vulns/unforgivable.pdf
- Christey et al. *Structured CWE Descriptions*. http://cwe.mitre.org/documents/structured_descriptions/index.html

Evaluation

Your grade will be based on the following types of evaluation (with weight):

- 20% in-class quizzes. There will be periodic short quizzes in class, multiple choice with short calculations designed to test basic recall and comprehension of the previous week's material. Quizzes are closed book.
- 50% homeworks and practical assignments. The course is organized around a series of practical assignments that each take 2-3 weeks and mostly involve building something from scratch relevant to the material of the course.
- 10% midterm. A full class period midterm around the middle of the course will test your understanding of the material up to that date. Midterm is closed book.
- 20% final. There will be a cumulative exam testing understanding of all material to date.

Lateness

The grade of homeworks and projects that are turned in late will be reduced by 20% per each day, or part of a day, of lateness.

Academic Integrity

Students are expected to follow Cornell's code of academic integrity at all times:

http://cuinfo.cornell.edu/Academic/AIC.html

Specifically, in-class quizzes are to be done without consulting anyone or anything other than the student's own memory. Use of phones, tablets, laptops, prepared notes, neighbors, or any other external aid will be considered a violation of academic integrity.

Similarly, for homework assignments, students may consult with each other in general terms, but must perform all steps of the assignment themselves, create their own work, and write up their own results.

For coding projects, code should be developed from scratch, using only libraries available on the system. Cut and paste from internet code is not permissible, nor is borrowing of code from other class participants.

Computer Security Ethics

In this course, you will be learning computer attack techniques which are **immoral, illegal, and against university policy** to use in the wild. We have to teach you the techniques that attackers use in order that you understand what is involved in network defense. However, you could get in **very serious trouble** for running exploits or network reconnaissance techniques against computers and networks that aren't explicitly sanctioned in this course for educational purposes. Therefore, be careful to keep all your activity confined to computers and networks that you own personally, or facilities provided explicitly for the course.

Finally…

Don't be afraid to ask for help. If you are struggling, we'd way rather you approach us and get help before the problem becomes serious. Use office hours or email.