CS 5434: Defending Computer Networks

Instructor: Stuart Staniford
sgs235@cornell.edu
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),
- CS M.Eng. standing,
- Or consent of instructor.

Lectures:

Tuesday/Thursday 10:10-11:25
Hollister 314.

Class Website:

http://www.cs.cornell.edu/courses/cs5434/2013fa/

Instructor Office Hours:

Tuesday: 1:30pm-2:45pm.
Wednesday: 1:30pm-3pm.
Office hours will either be in 4108 Upson or in the lab in 317 according to need of assignments.

Teaching Assistant: TBD.

Lab facilities:

We will make use of the Linux Lab in Upson 317 for certain assignments in which we need a dedicated safe playground to try attacks and defenses. Lab schedule arrangements will be announced later (as we must share the lab with robotics folks).

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 attacks as a way around the firewall. Drive-by downloads and social engineering.
11. Defending against HTTP attacks. Web-proxies, in-browser defenses, anti-virus systems.
12. SMTP attacks – spear-phishing, and defenses against it.
13. HTTPS: Encryption and virtual private networks as a means to maintain confidentiality.
14. The modern enterprise network: what a large-scale network looks like, and emerging trends affecting it (BYOD, cloud).
15. Legal and ethical issues in defending networks.

Reading Materials

There is no textbook for the course. Instructor lecture Powerpoints will be available online for some 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):

- 30% in-class quizzes. There will be a total of three in-class quizzes. These are designed to ensure that you are paying attention in class and doing the reading, and should be mostly straightforward if you are.
- 30% homework assignments. There will be a number of homework assignments. Most will be practical lab-based exercises using common network security tools. Examples could include actually port scanning a network, set up a firewall, use a vulnerability scanner, monitor a network with an open-source network intrusion detection system, and look for malicious files with an open-source anti-virus tool. Hopefully, we'll work up to some kind of hack-athon.
- 40% class project. You will build a non-trivial piece of C code from scratch to do an interesting task in network security. You will write a document describing its algorithms and architecture (10% of total grade) and demonstrate how well it works at an interim milestone (10%) and towards the end of the course (20%). Project will likely be done in small groups. Details will be released a couple of weeks into the course.

Lateness

The grade of homeworks and projects that are turned in late will be reduced by 25% per each day, or part of a day, of lateness. Eg, if homework is due at the beginning of a lecture and you turn it in at the end, your score on that homework will be reduced by 25%. If you turn it in the following day, your score will be reduced by 50%, and so on.

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 lab-based 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 class 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 lab 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.