Computer Security I

CS 493/693, Fall 2019 - Dr. Lawlor (Engineering 134)

Announcements

- Final overall course letter grades and detailed percent scores are on NetRun (and UAOnline). Have a good break!
- Project final writeups will be due on Blackboard (log in first) by the end of Wednesday, December 11. This should be very short, a few pages maximum, summarizing what you did, and what you learned. 693 students should format their writeup like a scientific paper--no specific length is required, but you should have some actual citations.
- The final exam (review doc here) will be in class Tuesday, December 10, 10:15 a.m.-12:15 p.m. in our usual classroom. (We actually have a presentation to finish during that timeslot too.)
- HW4: hands-on buffer overflow examples is on NetRun, and due anytime Monday, December 9.
- Project presentations are December 3 and December 5. Sign up for a presentation timeslot in this Google Doc spreadsheet. Rather than mess with plugging and unplugging cables, install the Zoom application and connect to 907 474 7678 to share your screen.
- No class this Thursday due to Thanksgiving.
- Project draft writeup is due on Blackboard (log in first) by the end of Thursday, November 21. This should be very short, a few pages maximum, summarizing what you did, and what you learned. 693 students should begin to format their writeup like a scientific paper.
- HW3: Networks and Firewalls is due on Blackboard (log in first) by the end of Tuesday, October 29.
- Project proof of concept code is due Thursday, October 24 on Blackboard (log in first). This version should have a 1-paragraph README.txt describing what it is, and it needs to run and have at least some of the features of the final version, but does not need to do everything you wanted, and does not need to be pretty or polished.
- Midterm exam grades are available on NetRun's grading area.
- HW2: Drive Forensics is due by the end of Tuesday, October 8 on Blackboard (log in first).
- Project background presentations will be in class on October 1 and 3. These are 7 minute project **background** presentations, which should cover the relevant prior work in the field, interesting results so far, and briefly present your plan for the project. (But you're not expected to have finished building anything new yet!)
    - Sign up for a Zoom account with your UA credentials and download the Zoom client at https://alaska.zoom.us
    - The class meeting link in the zoom app: 907 474 7678
    - Or in browser: https://alaska.zoom.us/my/lawlor
- Project topic discussions will be in class on Thursday, September 19.
- HW1: openssl hands-on examples is on NetRun, and due anytime Thursday, September 12. (Extended due to widespread OpenSSL problems.)
- HW0: adversarial programming is on NetRun, and due anytime Tuesday, September 3.
- Use your @alaska.edu email to set up your NetRun account, then log into NetRun here. If you don't see a CS 493/693 class listed under your saved files on NetRun, email me and I can fix it immediately

Course Notes

- 11/26 Securing the Perimeter
- 11/20 Advanced buffer overflow attacks
- 11/18 Buffer overflow attack intro and metasploit intro (slides)
- 11/14 Cloud security: firewalls, IAM
- 11/12 Cloud architecture and AWS Lambda
- 11/07 Windows Domain authentication, and DPAPI / mimikatz
- 11/05 Web authentication, cookies, and CSRF
- 10/31 Network API design
- 10/29 Intrusion Detection Systems: Snort
- 10/24 Securing web servers with Flask
- 10/22 HTTP protocol design and low level server intro
- 10/17 Firewalls and the TCP-HTTP-HTTPS layers of the protocol stack
- 10/15 Networks: packet sniffing and the MAC-IP layers of the protocol stack (see also: Networking Cheat Sheet)
- 10/10 Midterm exam in class
- 10/08 Review for midterm exam
- 10/01 and 10/03: Project background presentations
- 09/26 Recurring security failures
- 09/24 Containers (and example zip), setuid, and LD_PRELOAD
- 09/19 project topic discussions, and change detection
- 09/17 Disk Encryption: using crypto to prevent disk forensics
- 09/12 Forensics: working with machine images
- 09/10 Isolation: processes to VMs to firewalls, user and system accounts
- 09/05 Cryptography for networks: Key exchange and public key cryptography
- 09/03 Cryptography overview: cryptographic hashes and symmetric ciphers
- 08/29 Interactive Google Doc: Course Topics
- 08/27 Slides: Definition of "Secure", adversarial basics, Sun Tzu, map of computer security.
- The course syllabus has grading info, course topics, my office hours, and other good stuff.

Computer Security Background Reading

Broad Summaries

- OWASP Top 10 web application vulnerabilities
- OWASP Cheat Sheets for common web app vulnerabilities
- MITRE ATT&CK Matrix
- CVE: Common Vulnerabilities and Exposures tracking

Security Blogs / News

- Schneier on Security: good summary of security news in a social context from a technical person. Schneier wrote the 'blowfish' and 'twofish' ciphers, among others.
- Krebs on Security: excellent in-depth reporting on dark markets, carder sites, and ransomware. He's been going after eastern european organized cybercrime lately.
- Threatpost: short newsy summaries of new security vulnerabilities
- Kaspersky Labs: readable but solid technical analysis from a Moscow company.

- Hacker News: security news summary site from India.