lectures

recorded, attendance not required

prerequisities

CS 3710 — I understand there's some variation...

knowledge of C, assembly (CS2130)

homework assignments

many approx. one week assignments

mostly due Friday at 11:59pm ET – but see calendar

some reverse-engineering oriented

several demonstrating an exploit

some demonstrating vulnerability discovery/mitigation technique

weekly quizzes

weekly written quizzes

released after Wednesday lecture

due before Monday lecture

starting after second week of class

exam/final homework

final exam (written), as scheduled

final ‘challenge’ homework as pseudo-second-part-of-exam

note on course changes

some question/flexibility re: topics

hoping to do more versus last time I taught:

- reverse engineering tools (e.g. Ghidra)
- program analysis tools (e.g. angr)
- some non-memory-safety topic: sandboxing, web security

textbook

no required textbook

some lecture material based on textbook stuff

> Peter Szor, "The Art of Computer Virus Research and Defense"
> (and may use other security textbooks)

for exploit stuff, a good reference:

> Anley, Heasman, Lidner, Richarte, "The Shellcoder's Handbook, Second Edition" (2007)

office hours

posted on calendar on website

piazza, etc.

linked on Collab

use private questions if assignment code, etc. involved

On Ethics

don't use someone's computer without their permission

- or in excess of what they've permitted

don't assume it's just a harmless prank

- unintended (but likely) consequences

don't assume the system owner would give you permission

- if you're afraid to ask, it's not okay

On Law

probably illegal (Federal and/or State crime):

accessing computers without authorization

even if nothing is done with the access

deliberately overloading a service

“backhacking” into a malware operator’s machine

deploying a worm that patches security holes

DADT's awkward history

Davidson conceived as course on *malware*

- including exploits likely used by malware

...until 2019 was our only regularly offered security elective

but often other faculty taught it as general security class

- now have 3710 for that purpose

also have Network Security (CS 4760)

- nominally cryptographic protocols, data integrity, attack surfaces
- possibly also covers scanning, web security, ...

malware changes

historically, a lot of 'self-spreading' malware

- viruses, worms, ...
- (we'll discuss what these terms mean later)

these days, not the most common ways to get malware

- network-based exploits installing malicious software
- malicious/unwanted software distributed through app stores/etc.

exploit changes

historically: memory-unsafety exploits

biggest source of insecure software for a long time

probably still biggest, but...

memory safety slowly becoming less of a problem

how web browsers/mobile OSes/etc. work more important

a rough plan

x86-64 assembly

works on department portal/NX, etc.

(basic) reverse engineering

self-spreading malware (viruses, worms)

signature-based malware detection

anti-anti-malware cat and mouse game

memory vulnerabilities

vulnerability mitigations; sandboxing

vulnerability discovery + less-basic program analysis