

Systems and Network Security

Course Overview

Instructor: Khaled Diab

What's wrong with this picture?



What's wrong with this picture?



Course Staff

- Instructor: Khaled Diab
 - PhD, SFU, 2019
 - Research: Networking and systems
 - Affiliation: Network systems lab
 - Web: <http://www.sfu.ca/~kdiab>
- TA: Carmen Zhuang
 - Research: Security

WWW

- Course website:
 - <https://netsys-security.github.io/sp20/>
 - Syllabus, policy, schedule, slides, assignments, project
- Piazza:
 - <https://piazza.com/sfu.ca/spring2020/cmpt479980>
 - Discussion board, announcements
- Coursys:
 - <https://coursys.sfu.ca/2020sp-cmpt-980-x1/>
 - Submissions, grades

Communication

- kdiab@sfu.ca
 - Use my email for topics that are sensitive, confidential, etc...
- Piazza
 - Use this if your question/discussion would be beneficial for other students
- **Please** be professional and plan ahead

Office Hours

- Khaled:
 - Fridays (12pm – 1pm) at TASC1, room 9010
 - Email me to book an appointment.
- Carmen:
 - TBA

Course Goals

- Learn how an **attacker gains control** of a system
- Learn how to **defend** a system
- Gain **hands-on experience** in various security topics

Two Key Themes of this Course

- How to think like an attacker
 - To develop the “security mindset”
- Technical aspects of security
 - Reproducing attacks
 - Building defensive solutions

Topics

- System security:
 - Control-flow hijacking and defenses
 - Return-oriented programming
 - OS security
 - (Tentative) Sandboxing and Fuzzing
- Network security:
 - TCP/IP attacks
 - DoS and DDoS attacks
 - Internet naming security
 - Internet routing security
 - IDS and Firewalls
- (Tentative) Hardware security:
 - Intel SGX
 - Spectre and Meltdown attacks

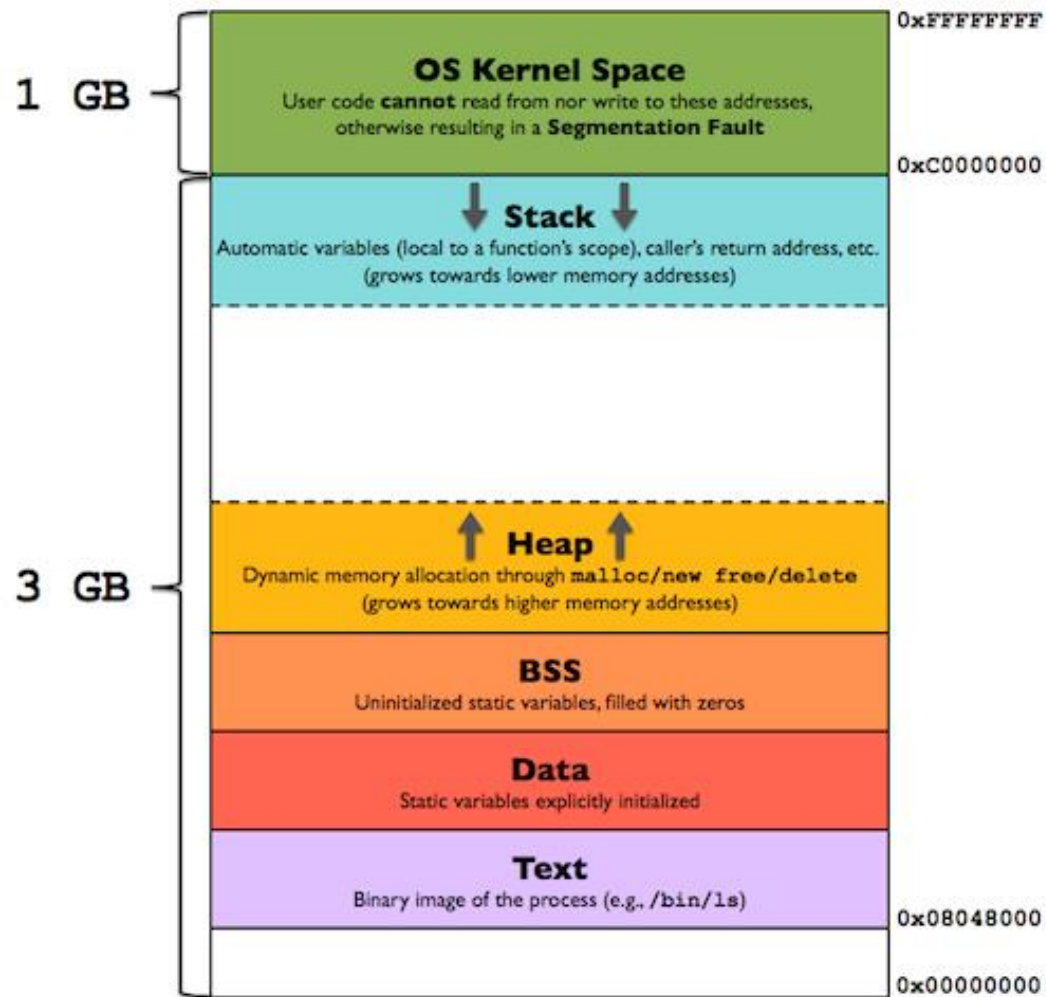
This course is not about...

- **Not** about cryptography
 - An important topic. Yet, we assume that security flaws are from coding mistakes or protocol weakness ☹️
- **Not** about all the topics in security
 - Security is broad!
 - E.g., web security, database security, social engineering
- **Not** about the latest attacks
- **Not** about blockchains

Prerequisites

- Required: CMPT 300
- Assumed:
 - operating systems (e.g., memory layout, execution semantics)
 - computer networks (e.g., IP networks, Internet naming and routing)
 - strong programming skills in C/C++ and Python
 - ability to write working Assembly code
 - knowledge of software dev. tools in linux (gcc, gdb, objdump, ld, git, etc.)
 - ability to learn new languages, tools and frameworks
- I expect you to do quite a bit of work.

Assess your knowledge base



```
int (*func)();  
func = (int (*)( )) code;  
(int)(*func)();
```

```
mov ebx, 42  
mov eax, 0x1  
int 0x80
```

Assess your knowledge base

- Networking
 - Wireshark labs: <https://www-net.cs.umass.edu/wireshark-labs/>
 - E.g.,: TCP lab: https://www-net.cs.umass.edu/wireshark-labs/Wireshark_TCP_v7.0.pdf

Credits: Computer Networking: A Top-Down Approach, 7th ed., J.F. Kurose and K.W. Ross

Course Materials

- *There is no good book that covers all the topics*
- Materials are research papers, book chapters, related articles etc.
- Use the slides to guide your study

Grading

- No midterm or final exam!
- Final Project (Group of 2–3): 35%
- Assignments (Individual): 30% (3 x 10%)
- Research Reading (Individual): 12%
- Quizzes: 18% (3 x 6%)
- Participation: 5%

Final Project (BYOP)

- This is your opportunity to explore or dig deeper in a specific security-related topic.
 - Related to **systems** and **networking** topics
 - Can be a research-related project
 - Reproducing known and recent attacks, or security-related systems
 - Searching for a vulnerability: Analysis of a program, misconfiguration in the network
 - Other topics: Smart home security, ML-based Firewalls IDS

Final Project (BYOP)

- Has to have an implementation component
- Highly recommended to discuss with the instructor and/or in the discussion board
- Four major milestones/checkpoints
 - The first one is on Jan 31st
- Details on website soon

Assignments

- Three assignments
 1. Shellcode and buffer overflow
 2. Packet sniffing and spoofing
 3. TCP/IP attacks

Reading

- A major activity in this course
- You will **read** and **summarize** a subset of the papers
- More details are posted to the website page.

Quizzes

- Three quizzes.
- One every 3—4 weeks
- Format:
 - Written quiz
 - Programming contest (e.g., CTF)

Participation

- In-class: I expect students to take active and regular roles in discussion, asking/answering questions, etc.
- Discussion board:
 - discuss the assignments and projects and other class materials
 - you can also use it to exercise the “security mindset”
 - Discussing recent security incidents
 - Posting and discussing resources and news
 - ...

Late Submission Policy

- Late submissions will **not** be graded.
- Unless
 - (1) there is an excused absence (e.g., illness with sick note, emergency) **and**
 - (2) student made arrangements with the instructor prior to the deadline.

Academic Honesty and Conduct Policies

- No tolerance to violations of academic integrity
- Students of any academic dishonesty incident will:
 - Get an 'F' grade and
 - Be referred to the appropriate University/School bodies for further action.

Ethics

As Uncle Ben said...



Don't try this at home

- Attacks discussed in class are illegal to execute
- Goal of this course is not to teach you how to attack systems!
 - But, to teach you how to defend systems by knowing how the attackers think
- Never use any of the attacks on a network connected to the Internet!
 - Even if it seems simple (e.g., TCP RST)
- Project/assignments?
 - code should run in an isolated env (e.g., VM)
- If in doubt, please contact me!

Ethics Forms

To receive a non-zero grade in this course, you must sign the CMPT 479/980 ethics form by 11:59pm on January 17, 2020.

- URL: <https://forms.gle/XzRogNnLaZLf6GEm7>
- Late forms will not be accepted.

Todo 0

- Read the “how to read a paper”
- Read the “project startup document”

Todo 1

- Read and understand the syllabus
- Sign the Ethics form

Todo 2

- Get to know your classmates, and form project groups
- Start thinking about project ideas

Todo 3

- Prepare an answer for “What do you think security is?”

Next Lecture

- What is “security” anyway?
- What are the main principles of security?