



CSC 405

Computer Security

Alexandros Kapravelos
akaprav@ncsu.edu

Administration

- Class website
 - <https://kapravelos.com/teaching/csc405-s21/schedule/>
- Piazza
 - <https://piazza.com/ncsu/spring2021/csc405>
- Mail to instructor (for private matters)
 - akprav@ncsu.edu
- Recorded classes
 - <https://mediasite.woffware.ncsu.edu/online/Channel/csc-405-001-sprg-2021>

Material

- What material will we be using?
 - Unfortunately, there is no good book on systems security
 - Use the slides that I will post on the web site
 - Related papers/readings and online material (from the syllabus)
- Here are some useful online books that provide additional information:
 - [The Shellcoder's Handbook: Discovering and Exploiting Security Holes](#)
 - [Hacking, The Art of Exploitation](#)
 - [The Tangled Web A Guide to Securing Modern Web Applications](#)

Grading

- What are the requirements to get a grade?
- Homework Assignments - 80% of grade
- Participation - 20% of grade
 - Class Participation
 - Piazza questions/answers
 - Watching the lectures
 - Quizzes

Topics

We are going to cover three modules:

Computer Security Basics

Software Security

Web Security

You need to understand

- Networks and Operating Systems
- Basics of systems theory and implementation
 - E.g., file systems, distributed systems, networking, operating systems, ...
- You will build stuff. I expect you to:
 - know how to code (in language of your choice*)
 - I will use mix of pseudocode, Python, Assembly, JavaScript, PHP and C
 - be(come) comfortable with Linux/UNIX

Goals

Learn how an attacker takes control of a system

Learn to defend and avoid common exploits

Learn how to architect secure systems

Assignments

- Individual homework assignments
- These are going to be **hard!**
- You are going to implement attacks and defenses
- Discovering a vulnerability is a frustrating, but very rewarding in the end!

- The assignments have a unique nature
 - They require from you some **exploration**
 - They are **VERY** different from any assignments you had so far
 - Most of them will have two parts:
 - **Identify** the vulnerability
 - **Exploit** the vulnerability

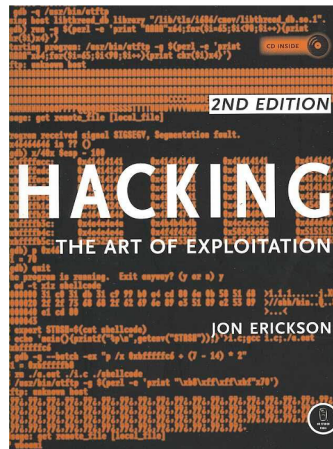
Lecture format

- Our lectures are going to be pre-recorded
- You will have to watch the lectures and study any related material
- We will use piazza to resolve any lecture-related questions -> weekly Q&A!

HackPack CTF

- Capture the Flag security competition
- 6 hours live hacking
- ~~• We'll have pizzas & sodas~~
- **April 16th 9am-5pm**
- It will count as one homework assignment
 - For the homework-part you will be able to work on the challenges over the weekend
 - Participation is mandatory to the CTF event, if you cannot make it you have to inform me beforehand
- There will be prizes for top places!

HackPack CTF prizes 2017

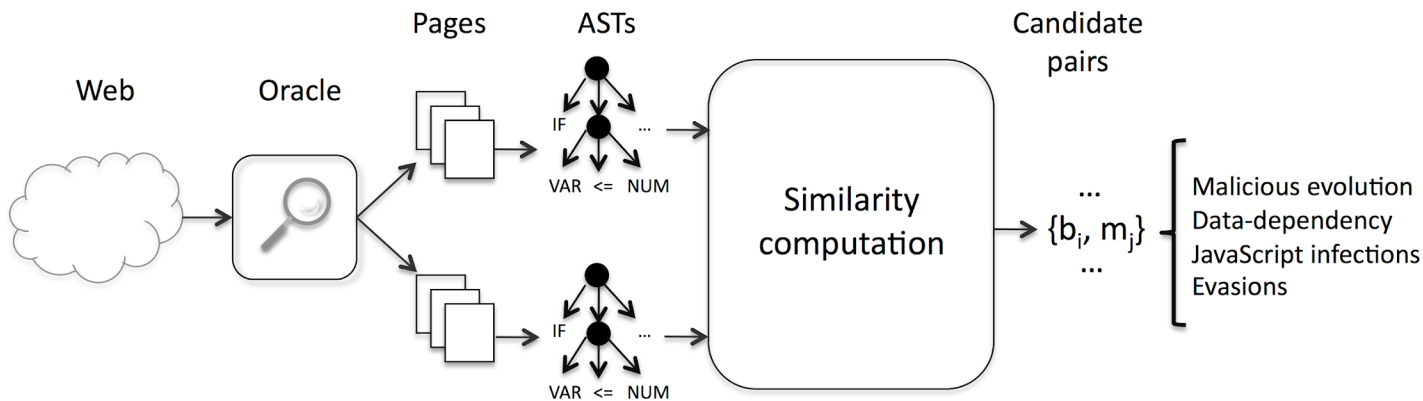


Readings

- There is a large amount of readings in this course covering various topics. These readings are intended to:
 - Support the lectures in the course (provide clarity)
 - Augment the lectures and provide a broader exposure to security topics
- **Students are required to do the reading!**
 - Some of the questions on the exams will be off the reading on topics that were not covered in class

Cheating policy

- Cheating is not allowed
- We run tools
- If you cheat you will probably get caught and get a failing grade in the course
- All academic dishonesty incidents will be reported without exception



Ethics

With great power comes great responsibility

- Topics will cover technologies whose abuse may infringe on the rights of others
- When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit written permission from the instructor.

Your Security Zen

At the end of every lecture we will have a short discussion on a recent security topic

Use piazza or [hackpack slack](#) #random channel if you see in the news interesting security incidents!

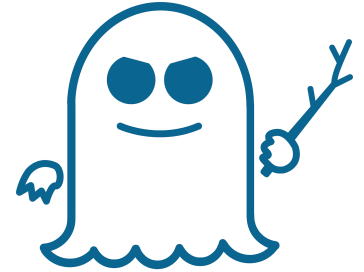
Here's one from a previous year





Your Security Zen

Meltdown and Spectre



two major security flaws in the microprocessors inside nearly all of the world's computers (Intel, AMD, ARM)

Spectre: no easy fix, we have to redesign processors

Meltdown: 30% slow down

There are proof of concepts in the wild that can read host kernel memory from inside a KVM guest

Sources: <https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html>,
<https://meltdownattack.com/>