CS5231: Systems Security

Lecture 1: Overview

About This Module

- Principle and practice of systems security
  - Understanding security principles through practice
  - Learning skills of programming, system administration, and etc.
- Research frontier of systems security

Uniqueness of This Module

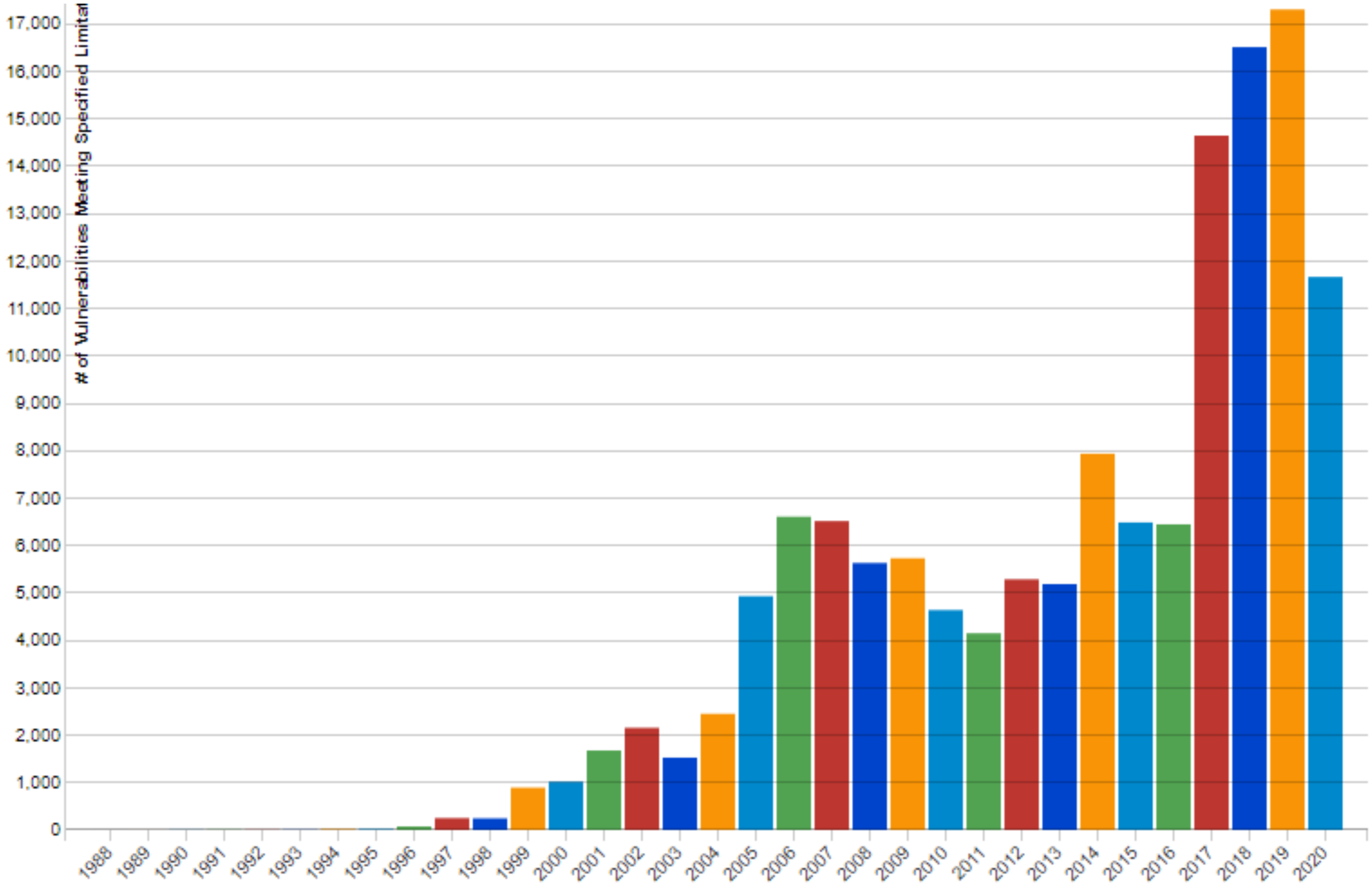
- Think in a different angle
  - How various systems can fail?
  - How to prevent such failures?
- Learn to think like a hacker, behave like a defender
  - Make no assumptions of hackers
- Heavily based on system programming
  - Have fun!

The Security Problem

What are the recent security incidents in news?

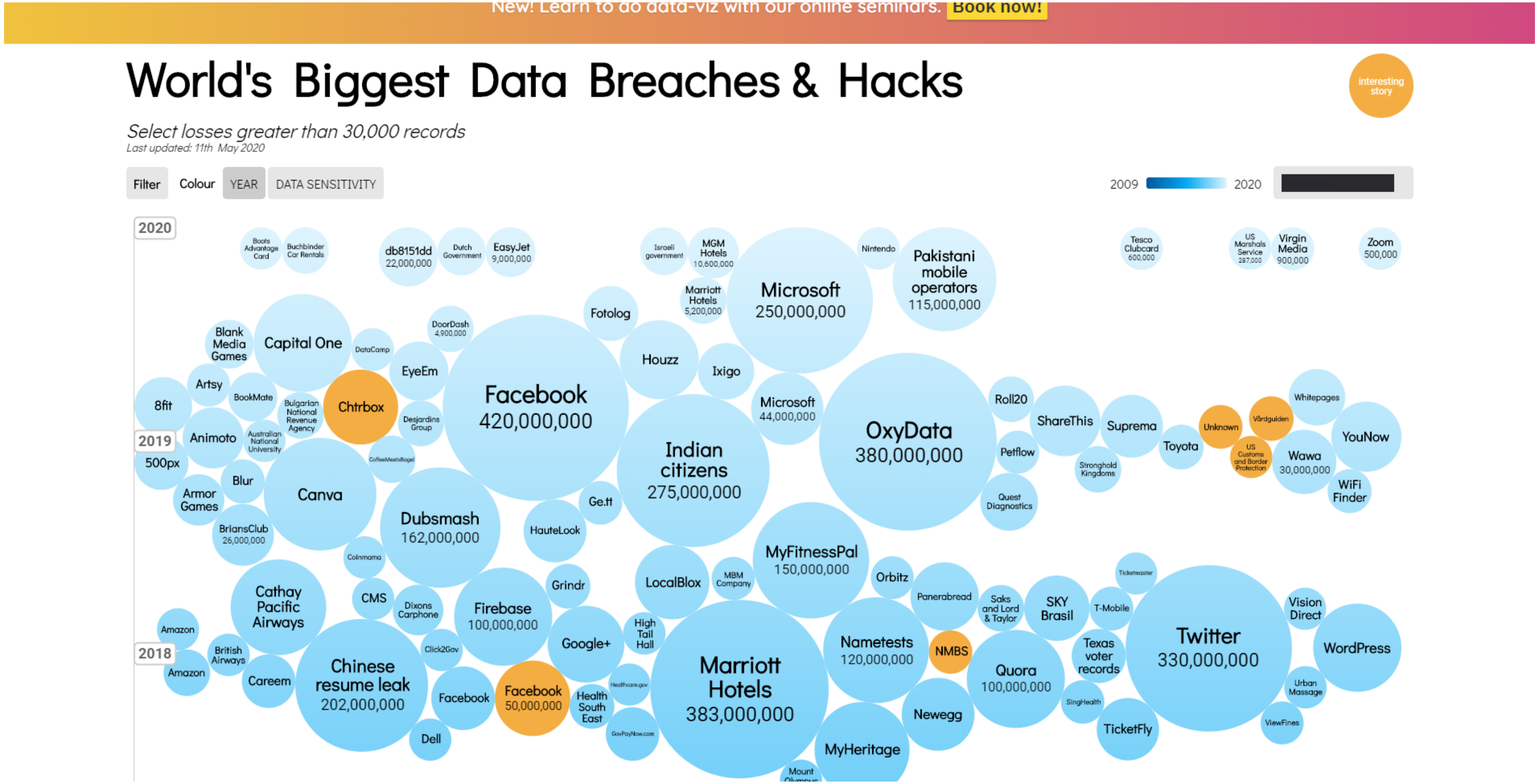
Software Vulnerabilities Over Time

# of vulnerabilities per year



Source: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all

Data Theft of Personal Records



New! Learn to do data-viz with our online seminars. Book now!

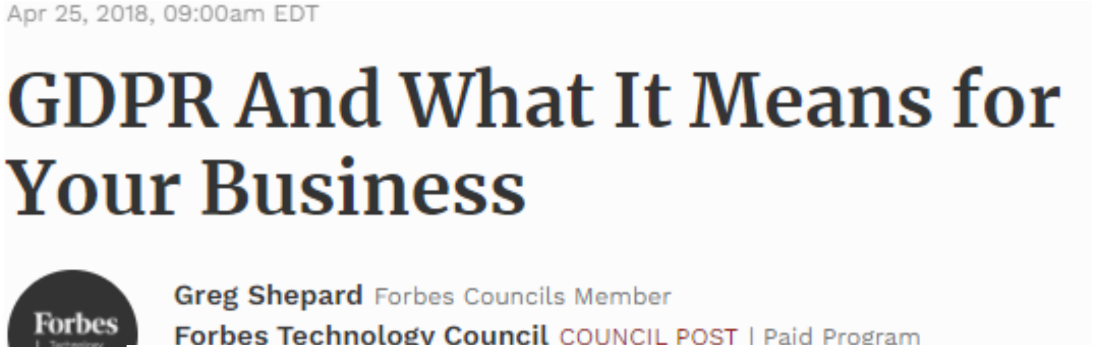
World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

Last updated: 11th May 2020

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Privacy Regulations are changing

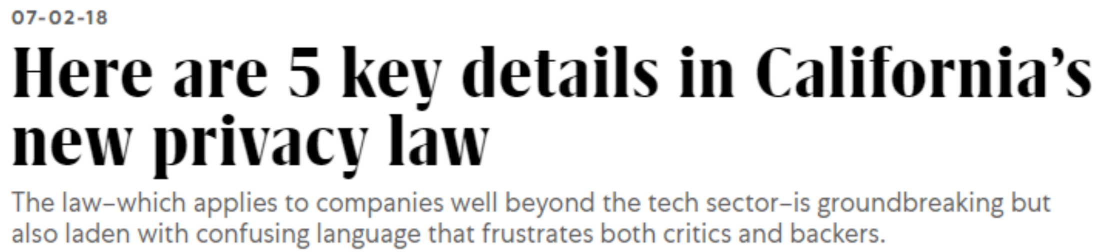


Apr 25, 2018, 09:00am EDT

GDPR And What It Means for Your Business

Greg Shepard Forbes Councils Member

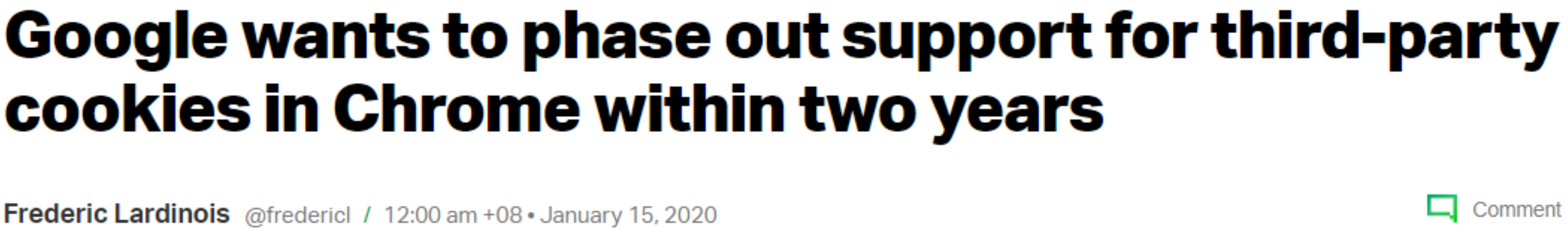
Forbes Technology Council COUNCIL POST | Paid Program



07-02-18

Here are 5 key details in California's new privacy law

The law–which applies to companies well beyond the tech sector–is groundbreaking but also laden with confusing language that frustrates both critics and backers.



Google wants to phase out support for third-party cookies in Chrome within two years

Frederic Lardinois @fredericl / 12:00 am +08 • January 15, 2020

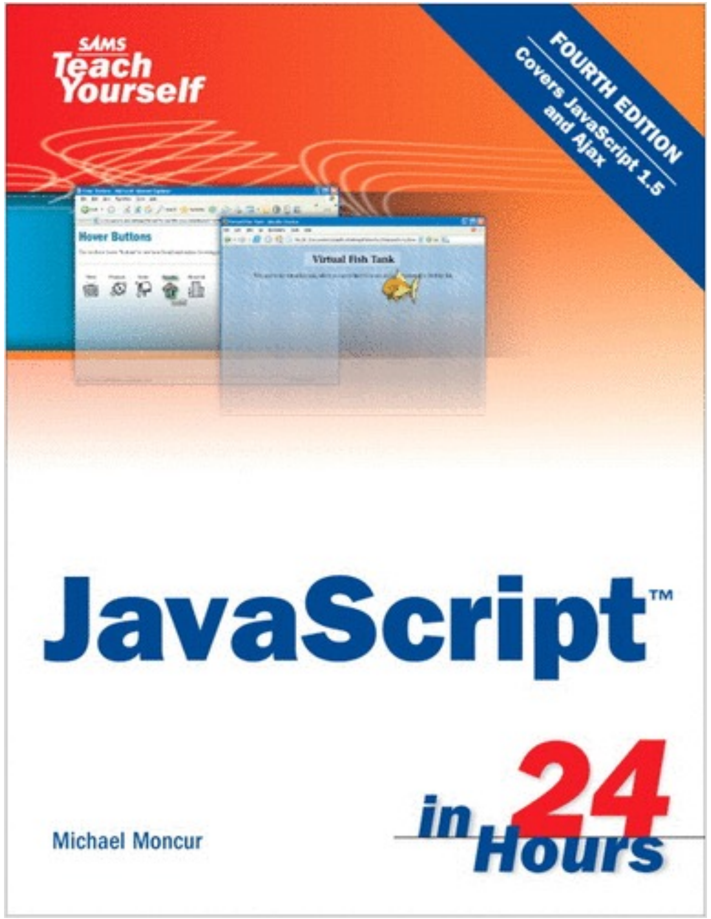
Comment

Additional Ref (GDPR fines): https://www.enforcementtracker.com/

Why Does This Happen?

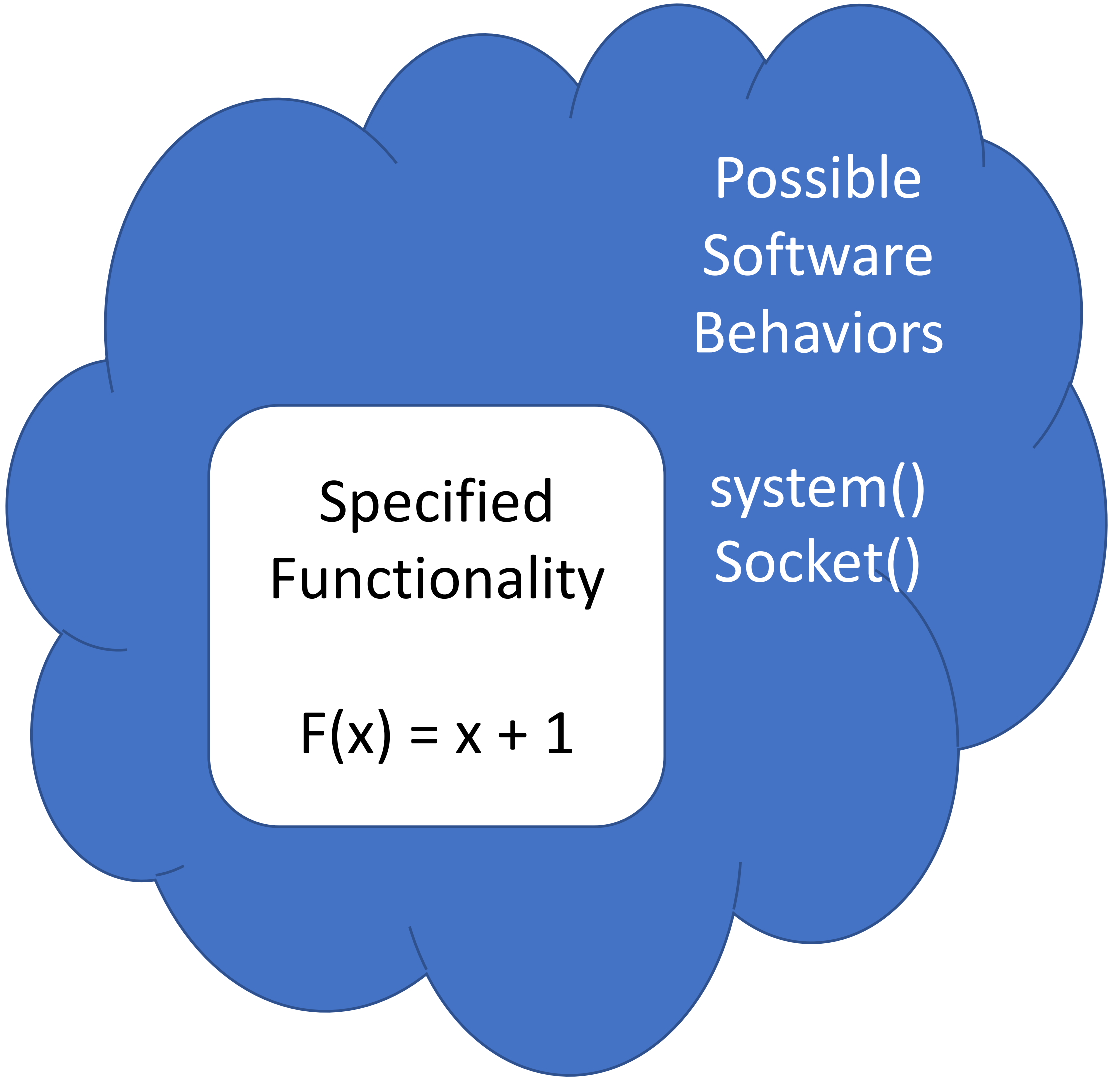
- Functionality: the primary concern during design and implementation.
  - Security is the secondary goal
  - Unawareness of security problems
- Unavoidable human mistakes
  - Awareness
  - Lazy programmer
- Complex modern computing systems

Impatient Programmers



- Maybe enough for learning basic functionality
- Never enough for to learn subtle implications of functionalities
- Result: programs can do more than you expect

Security: Mission impossible



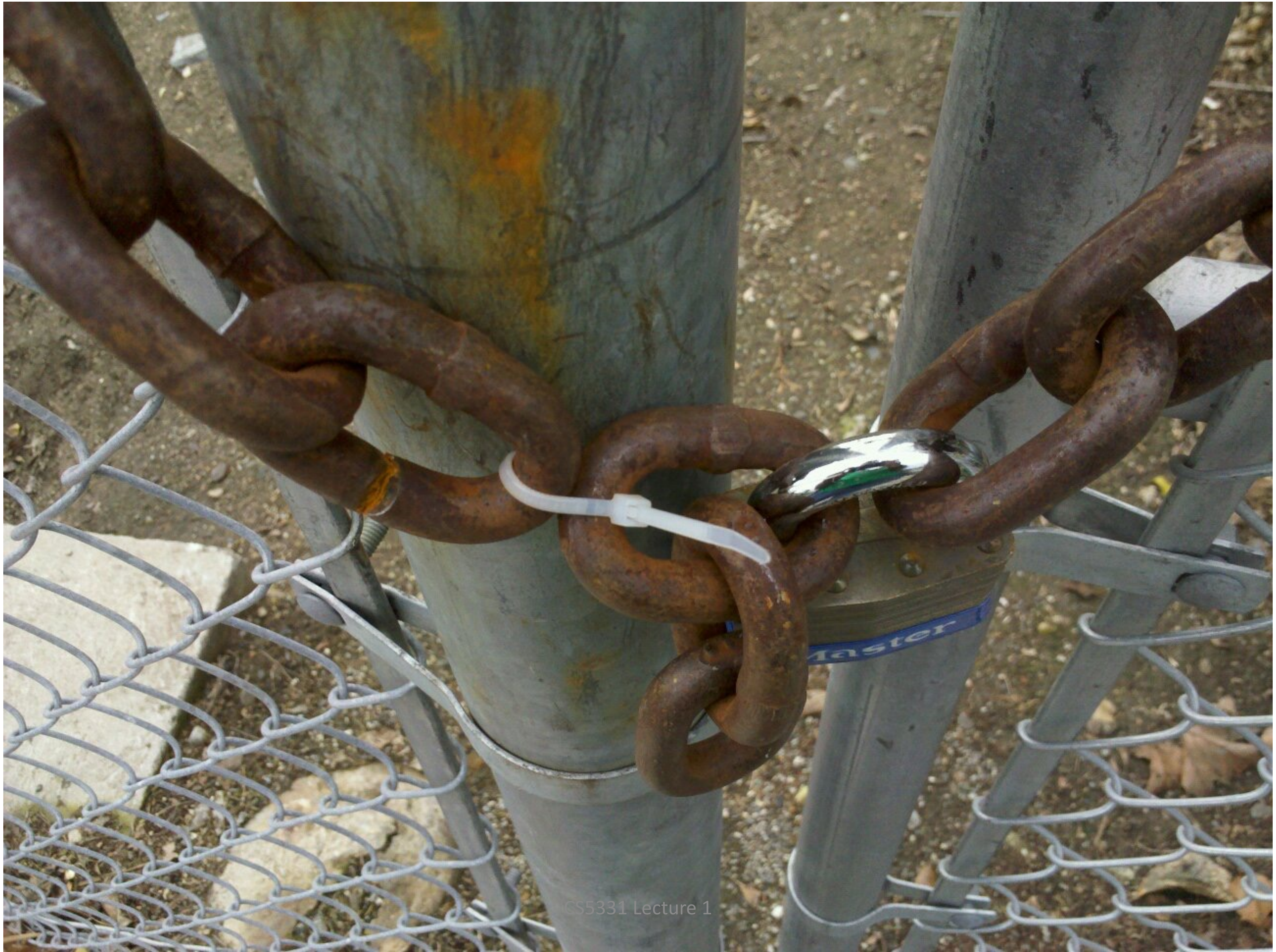
- But in practice, we need to make the security problem under control.
- Need better understanding of whole system

The Axioms of Security

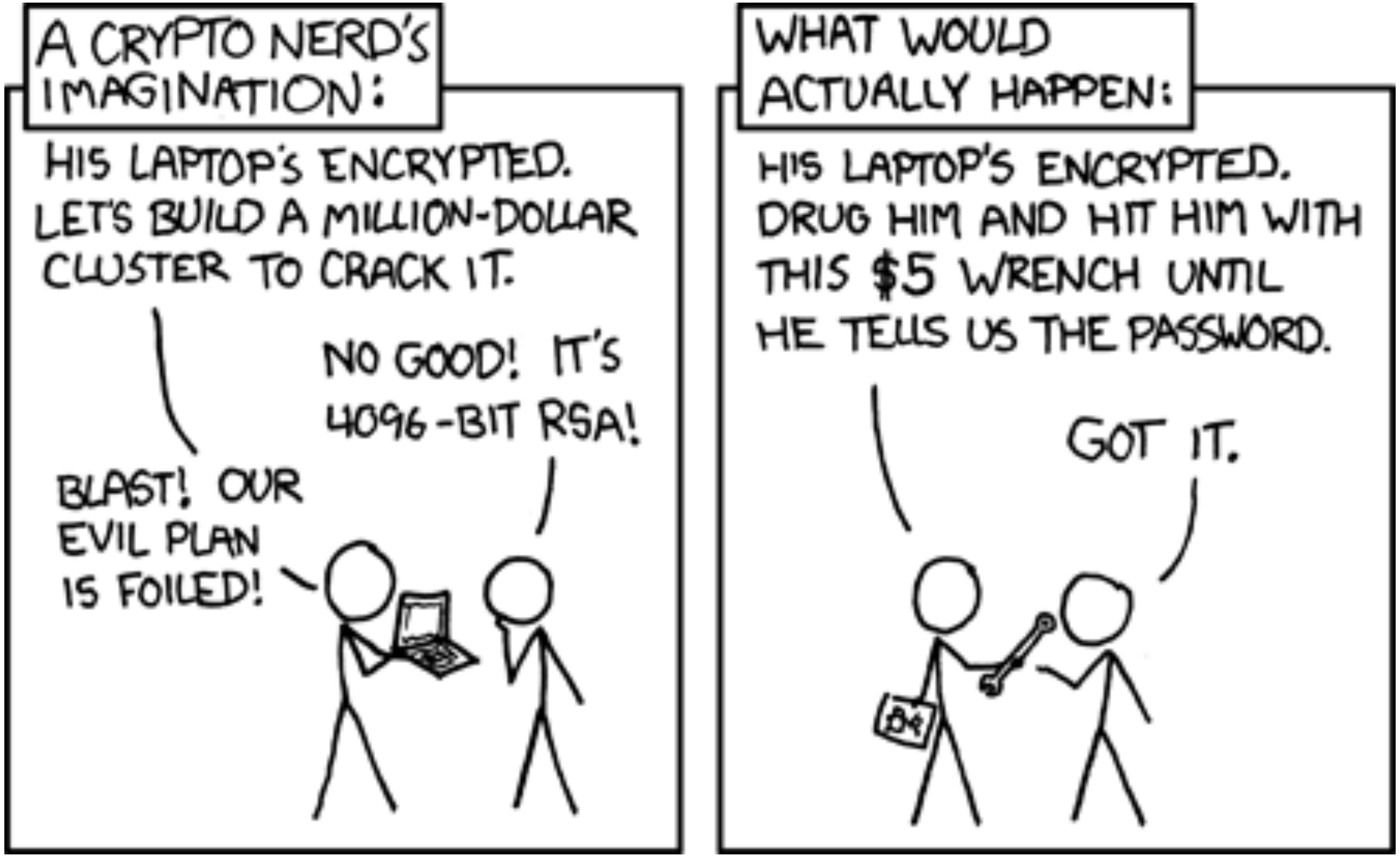
Principle of Easiest Penetration

- Security is about every aspect of a computing system
  - Hardware, software, data, and people.
- Principle of easiest penetration:
  - Any system is most vulnerable at its *weakest point*.
  - Attackers don't follow any rules. Don't underestimate their creativity.

Security can be no stronger than its weakest link.

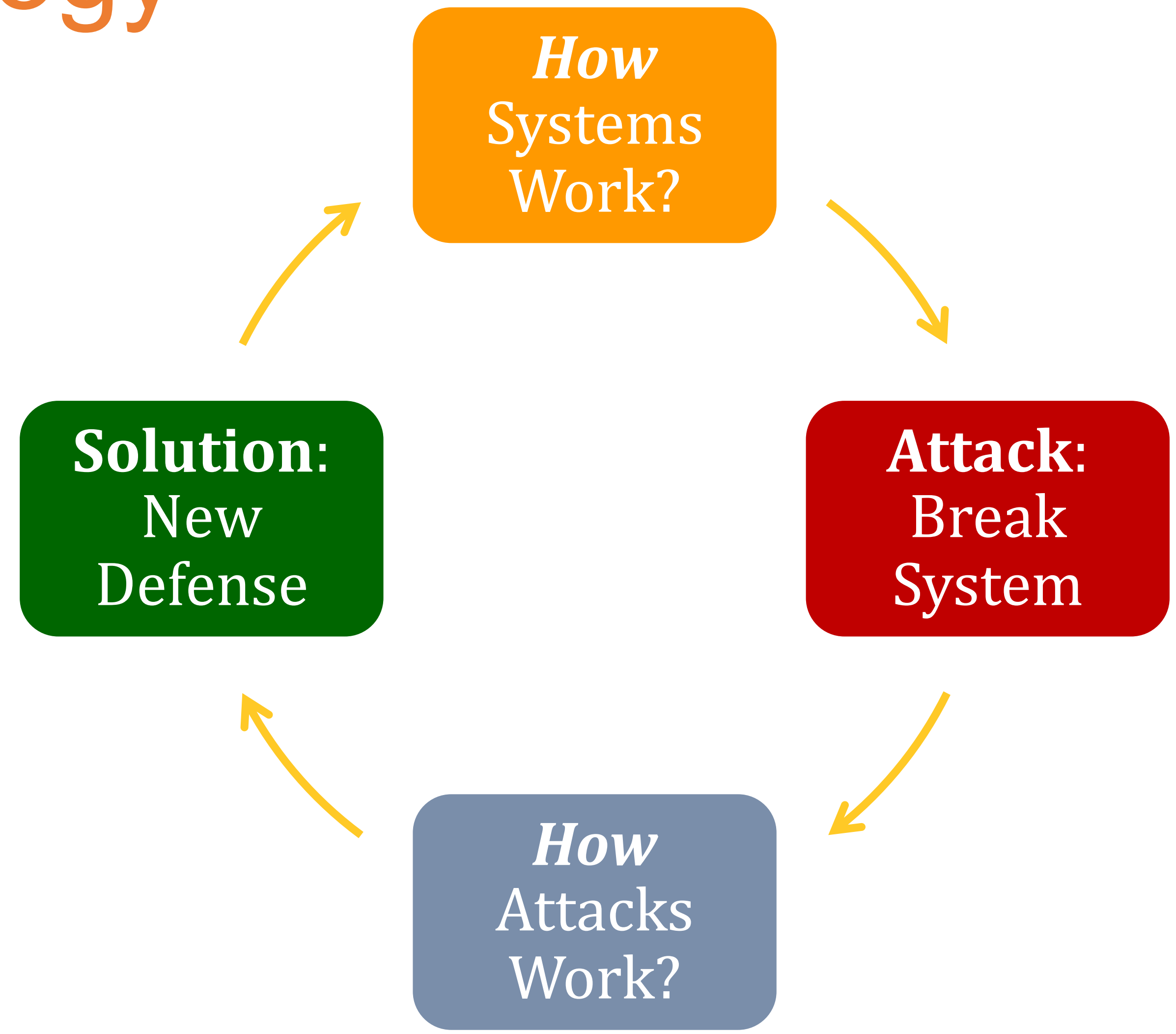

Master

The Real Problem


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Methodology of Security

Methodology



How Systems Work?

Attack: Break System

How Attacks Work?

Solution: New Defense

Learning to Attack

- If you know the enemy and know yourself, you need not fear the result of a hundred battles.

  知己知彼，百战不殆。

  Sun Tzu, Art of War

- To prevent attack, we need to learn how attack happens

Ethical Use of Security Information

- We discuss vulnerabilities and attacks
  - Most vulnerabilities have been fixed
  - Some attacks may still cause harm
  - Do *not* try these at home
- Purpose of this class
  - Learn to prevent malicious attacks
  - Use knowledge for good purposes

Administrative Issue

Administrative Issues

- In-class tests/quiz: 25-30%
- Individual assignments: 45-50%
  - Three homework assignments
- Final group project: 25%

Individual Homework Projects

- Sample topics of programming assignments
  - Memory error and attacks
    - Assembly, C, gdb
  - Linux kernel security mechanisms
    - C

Group-based Final Project

- Project Goal:
  - Apply our methodology: Deeply understand of a large system, understand attacks, and design solutions.
- Each group is expected to have three to four students
  - Joining forces for more interesting results
  - Limited slots in final presentation
  - Please announce your group information to the TA mailing list

Project Proposal

- Due date: Mid-September
- What to submit:
  - Problem description
  - Your solution and its novelty, list of reference
  - The platform and tools used in project
  - Project schedule
- You need to make sure your group is capable to handle the technical challenge independently

Progress Report

- Due date: Mid-October
- How is your progress compared to your proposal?
- Literature survey
- Initial approach description
- If you have difficult or question, raise them early

Final Report and Presentation

- Final report due at the starting of exam week (soft deadline)
  - Following the typical format of technical report or research papers used in our class

- Final presentation: last two weeks in class
  - 10 to 15 minutes for each group

Notifications & Communication

- Watch out for Canvas announcements
- You are expected to be there for lectures!
  - Lots of details are covered beyond lecture notes…
- Please use email cs5231ta@googlegroups.com with for all email communication related to the module.
- Teams Channel “Consultation” for general consultation, private message for quick-response matters

Honesty & Collaboration

- TA and instructor will not “see / debug” code
- All questions go to Canvas forum and Teams Consultation
  - Unless you have personal case …

- Academic Honesty
  - You may discuss high-level approach to solving or share public sources of information via the forum.
  - But, independently solve the assignment
  - Not OK to find answers to the assignment questions (past students, instructors, other students, friends, Internet)

- Ethics: Responsible Disclosure
  - If you find a system vulnerable, inform the company / team responsibly
  - Not ok to exploit or sell vulnerability information.

Academic Dishonesty

A simple rule in NUS:

If reported or caught cheating, in any way, all students involved will get an **F grade**

- Plagiarism is a serious offense in academia
- Information for plagiarism definition and prevention
  - `http://www.cit.nus.edu.sg/plagiarism-prevention/`
- We use the *Turn It In* tool to check all submissions
  - Submissions are compared with document on the Internet and against one another

The Key Message

Think like an adversary…

- You will work with machine code, not a high-level language
- You will see the principles of secure construction in action
- You will see the gaps between theory and practice
- You will see how threats can be defined incorrectly
- You will see why existing principles can’t always capture concerns

Prerequisites

- Have basic knowledge of:
  - OS, Architecture, Compilers, Systems Programming, Basics of Probability Theory
- Have worked at some point with:
  - C/C++ programming
  - Tools like Linux commands, GDB (see notes)

- Many who take this class don't have the full coverage of these pre-requisites. That is fine. Prepare to pick up the requisite knowledge as you need them.

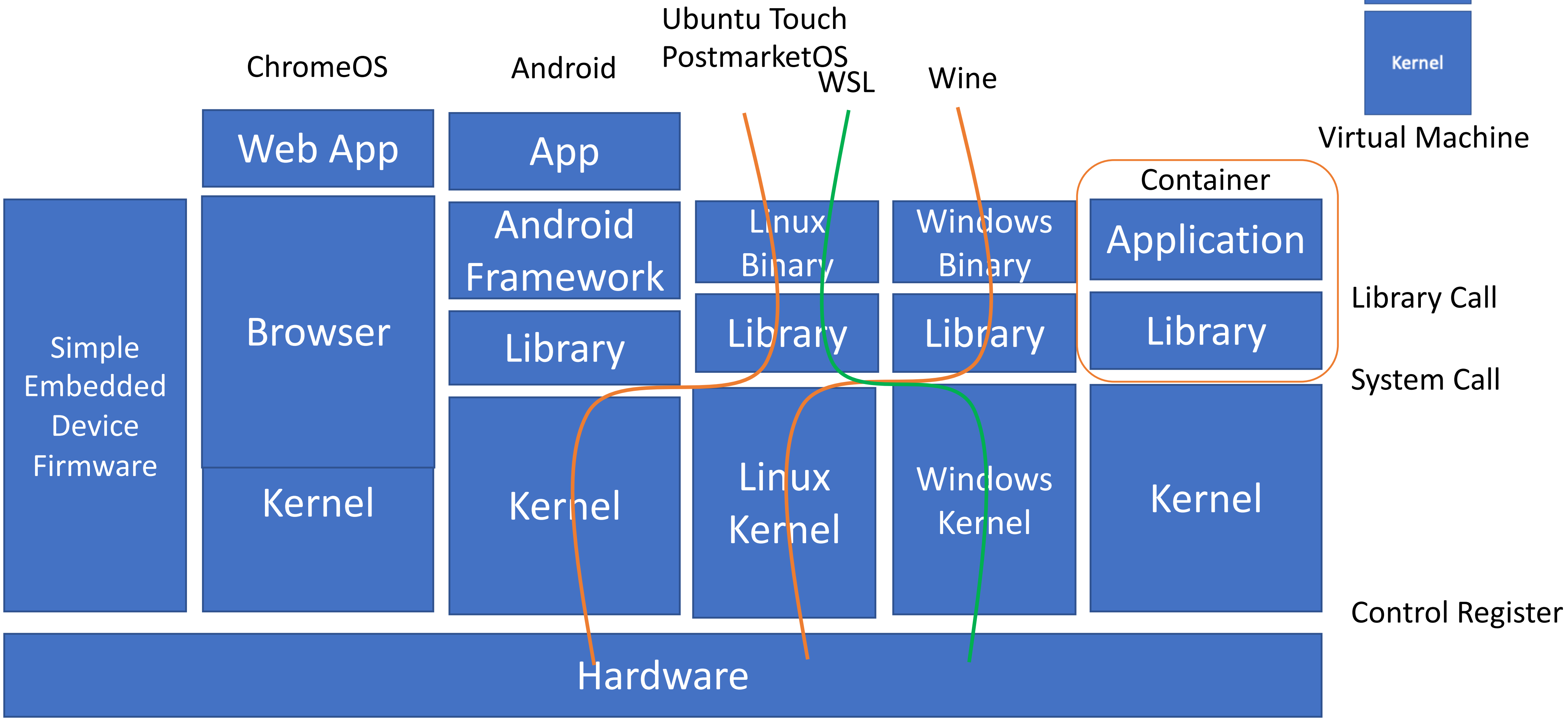
- Talk to the grad and UG office for any matters related to pre-requisites and enrollments.

Technical Skills

- UNIX/Linux administration
- Open source compiler and project management
  - gcc, make, autoconf, gdb, nasm
- Programming languages
  - C/C++, assembly language
- Mobile, system and kernel programming
- Source code version control

One more thing

Layers and Flexibility of Execution Environment



Thanks!

See you next week…