CS165 – Computer Security

Introduction

January 9, 2024

Outline

- Welcome!
- Goals of this course
  - Get to know computer security
  - Master a subset of critical skills in security
- Introduction to the class

Self intro

- Trent Jaeger, CSE Prof.
- Email: trentj@ucr.edu
- eLearn used for announcements, slides, assignments, forum
- Course webpage: https://www.cs.ucr.edu/~trentj/cs165-w24/
  - Link to the course schedule
- Office: Currently WCH 442 – may change
- Office Hours: 3-4pm Tu and 2-3pm W or by appointment
- TA: Zheng Zhang <zheng.zhang@ucr.edu>

Problem – Compromise the Internet

2000s – One vulnerability can take over the Internet

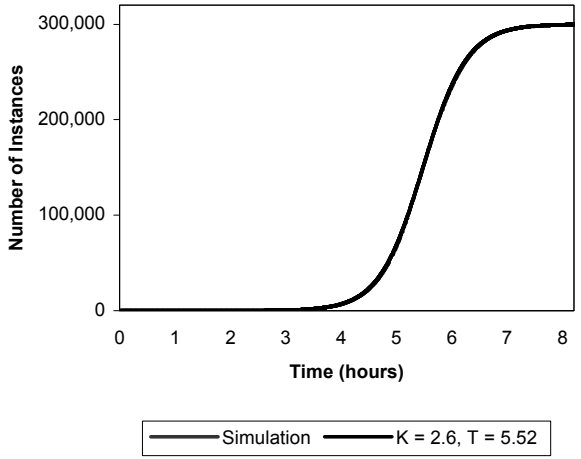
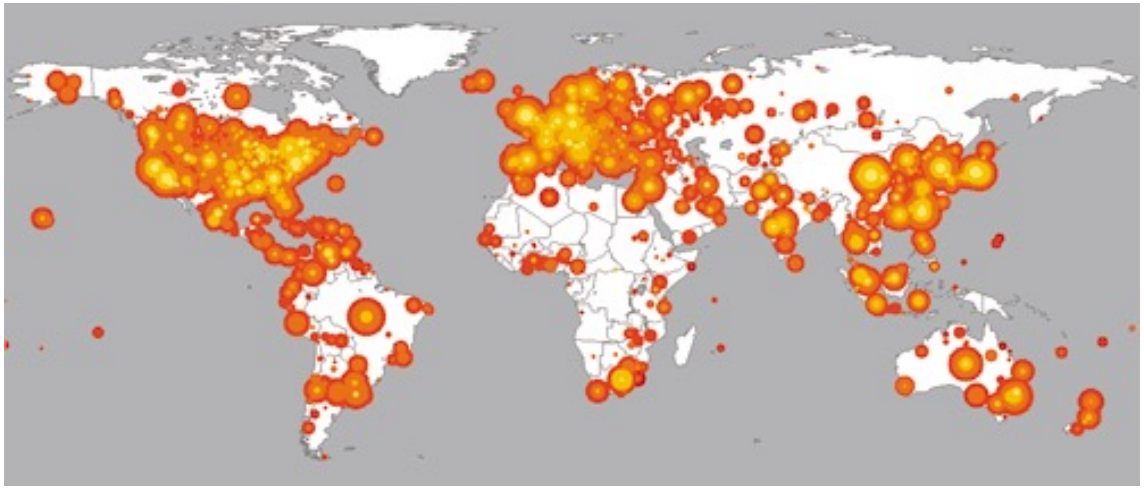
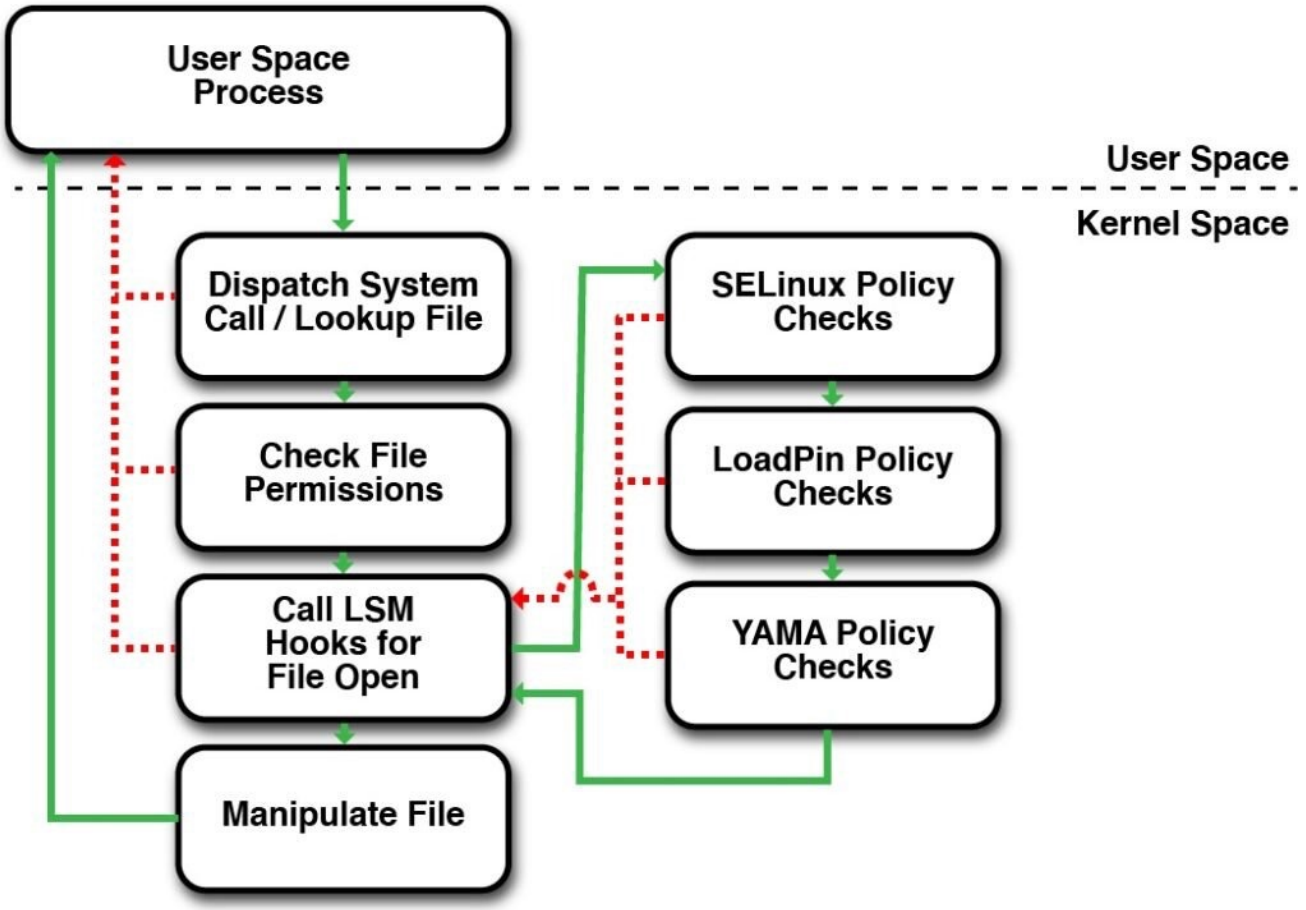


Figure 6: The spread of a simulated worm capable of 10 scans/second in a population of 300,000 vulnerable machines and its comparison to the model developed in Section 2. The simulation and theoretical results overlap completely.



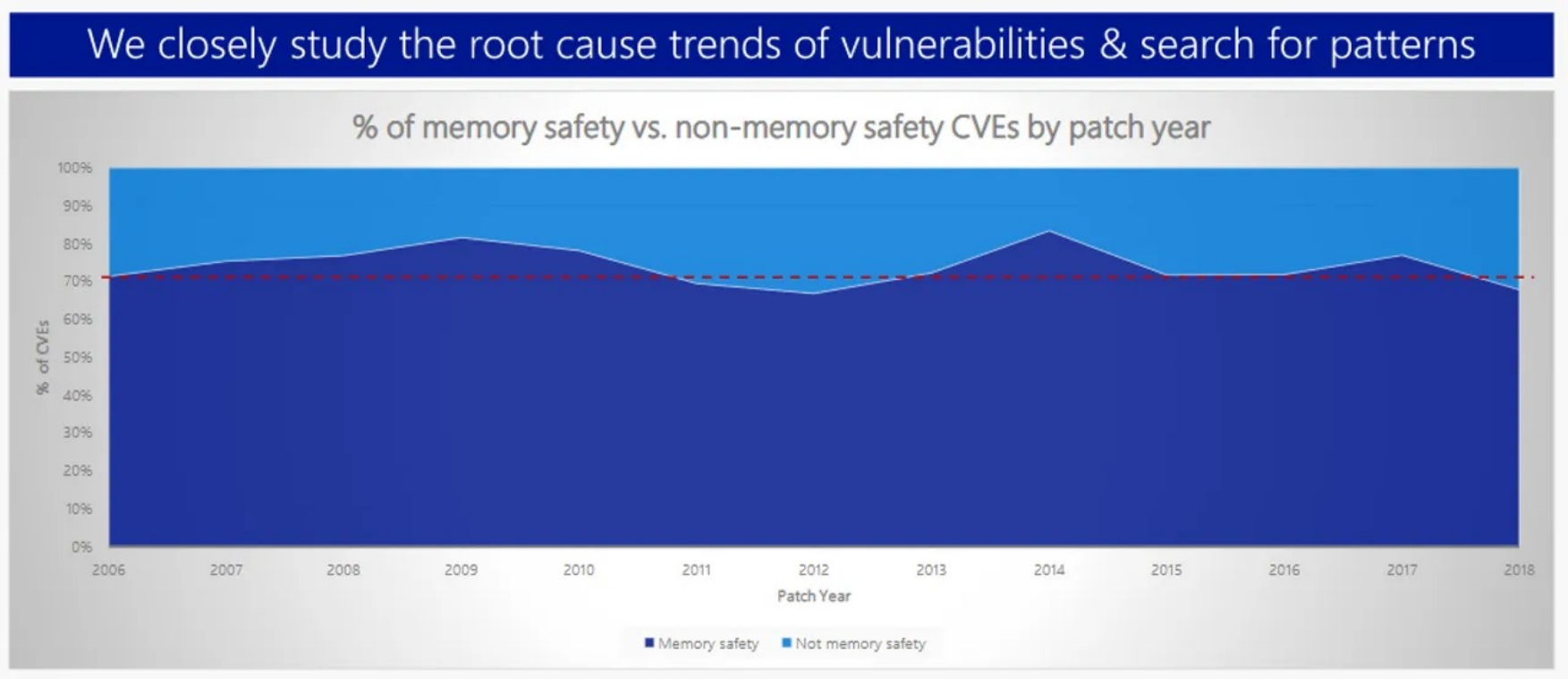
Solution – Linux Security Modules

2000s – Confine "network-facing daemons" to prevent host compromise



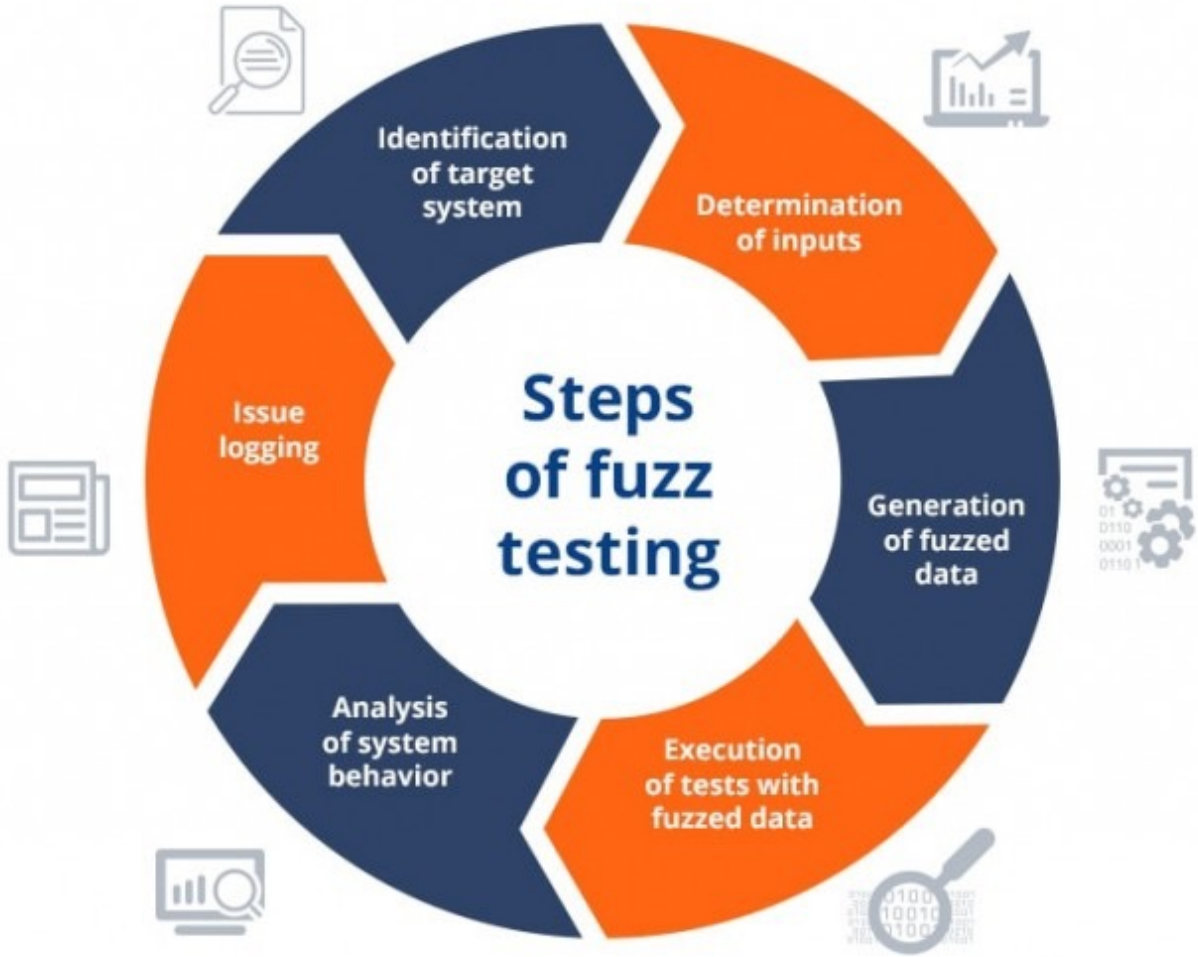
Problem – Buggy Software

Lots of vulnerabilities in software – lots of "memory errors"



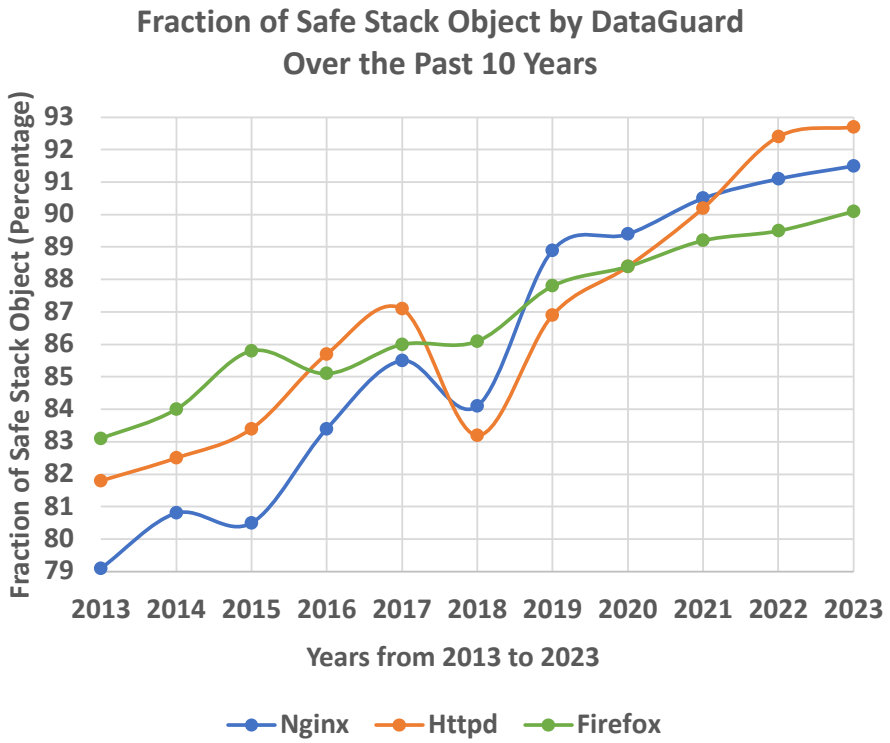
Solution – Fuzz Testing

Automated Generation of Test Cases for Coverage



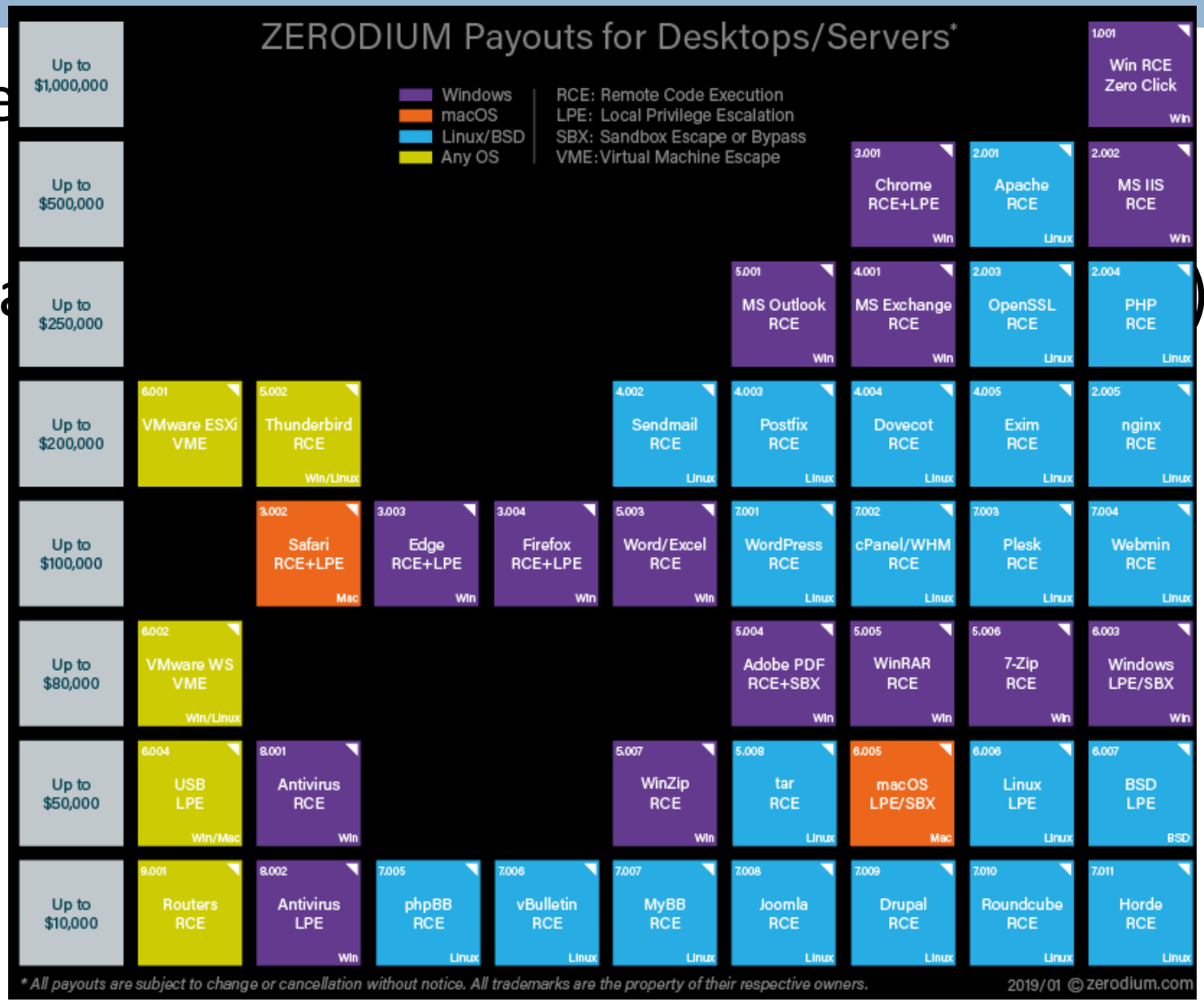
Solution – Fuzz Testing

A Trend of Increasing Fraction of Memory Safe Objects

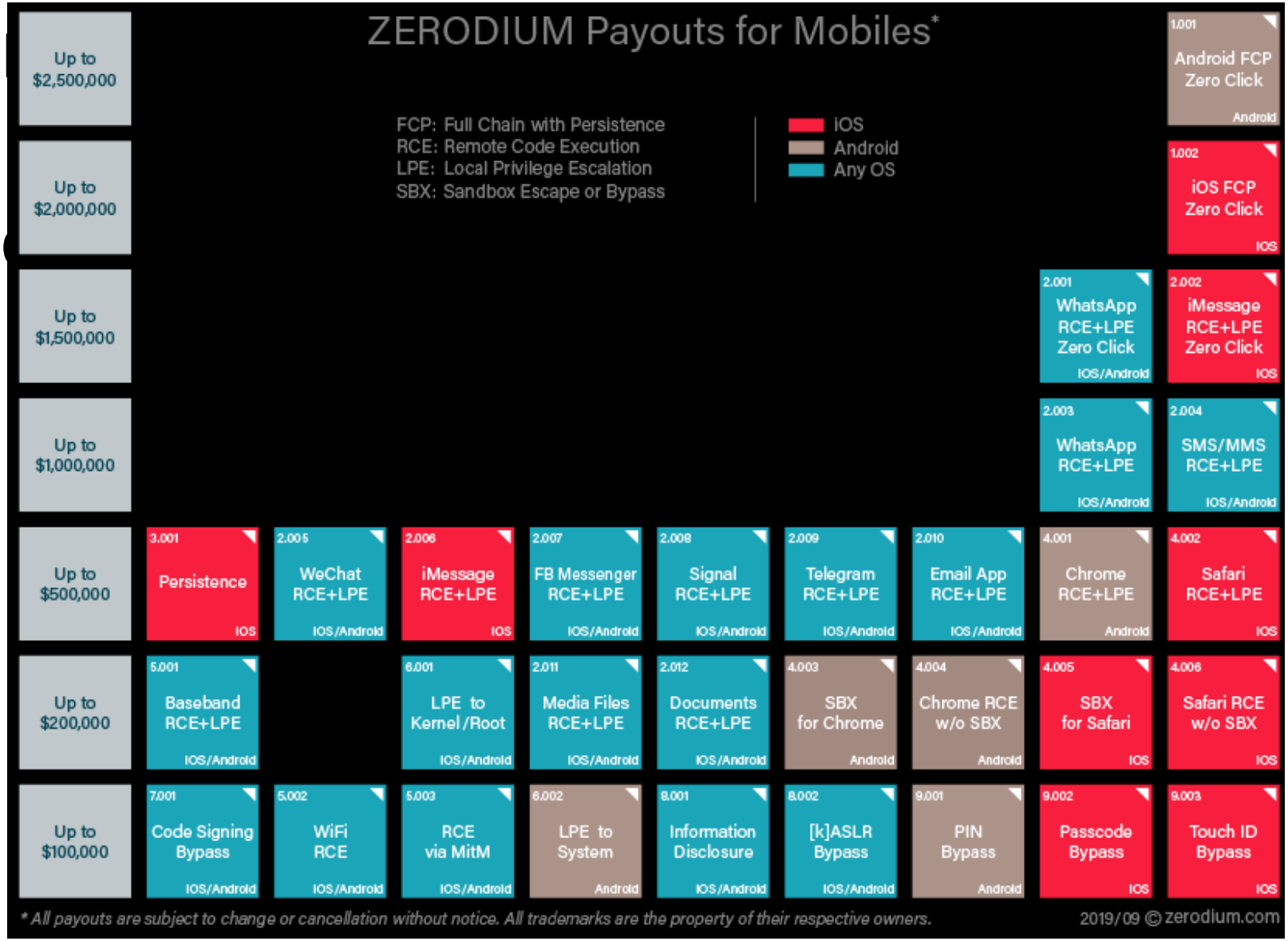


Goals of this course

- Le
  -
- Ga
  -



Goals of this course



Goals of this course

- Learn the principles of computer security
  - Diverse and domain-specific
- Gain hands-on experience (not just theory)
  - Learn to break things
    - $2M bounty for remote jailbreak!
  - and secure systems
    - Write secure code, configure systems securely
    - Analyze a system critically for weaknesses

Goals of this course

- From this class, you'll learn to:
  - Crack passwords
  - Perform memory-corruption attacks
  - Prevent memory-corruption attacks and their exploitation
  - Learn mechanisms to limit impact of exploits
- Become aware of security as a key dimension of software and system design and implementation

Getting an A

- This class requires knowledge of computer organization, operating systems, networking
  - CS61, CS161, CS153, CS164 (a little bit)
- And a mature understanding of software and systems in general

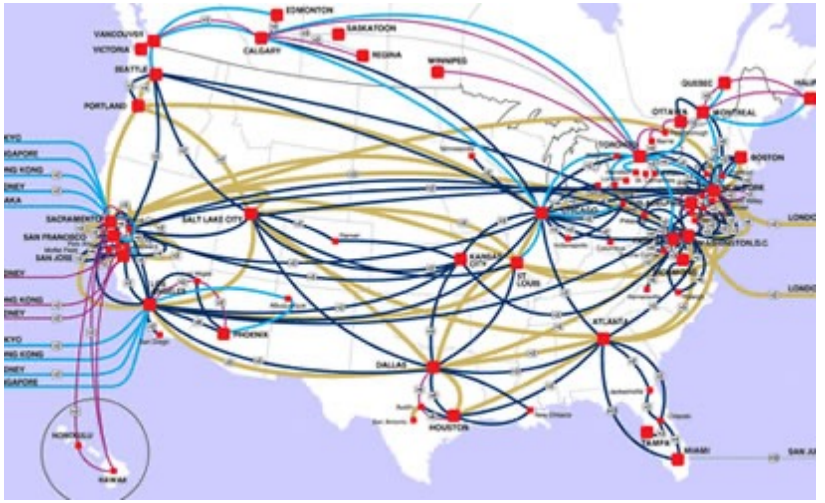
Outline

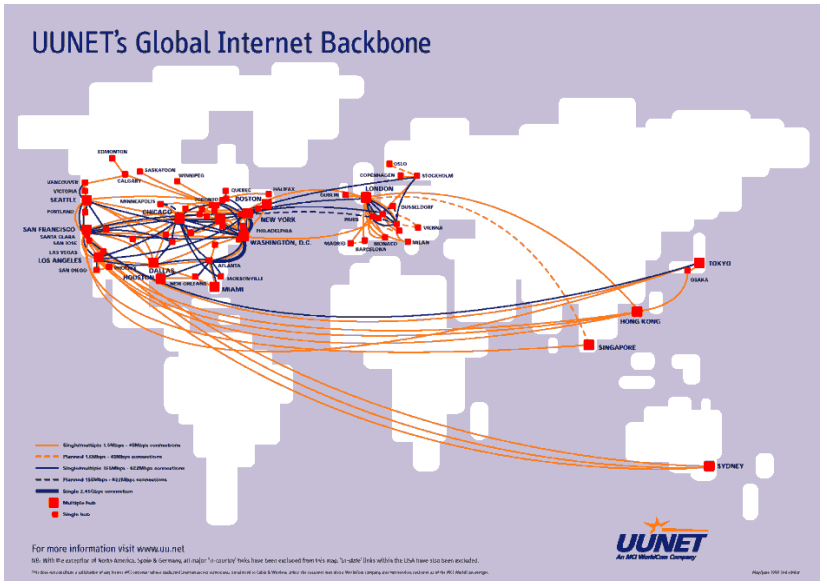
- Welcome!
- Goals of this course
- Introduction of the class
- Exercises
- Grading

Computer

Network

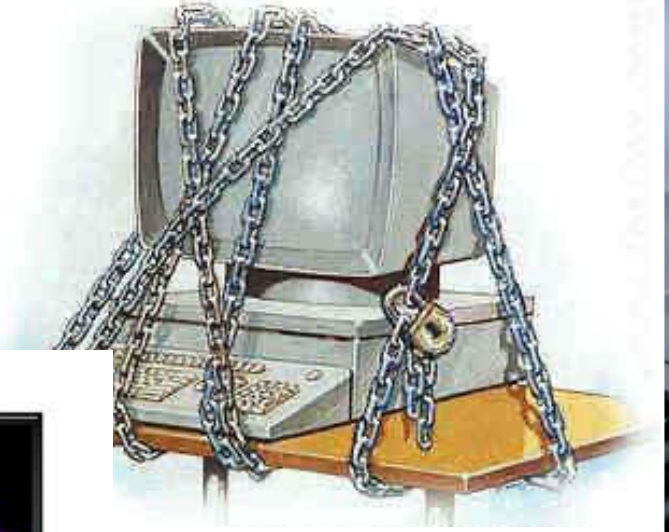

OC192
OC48
OC12
DS3
AT&T




UUNET's Global Internet Backbone
For more information visit www.uu.net
UUNET
An MCI WorldCom Company

/is/labs/lim-lab/image/4.CPS.jpg


HOW SAFE IS YOUR
COMPUTER?




IS IT SAFE?

Recent news

Data breach in March 2023

Facebook 50M accounts

Dyn DDoS attack

Insider threats

What is security about?

Security and security mindset

- "The study of how a system behaves under adversarial actions"
  - Intelligent attackers actively trying to lead the system to misbehave or do unexpected things

- Security vs. System
  - II II
- Corner cases vs. Common case

Play Games vs. Security Games

Play Games vs. Security Games

- Both deal with a set of man-made rules!
- Man-made rules have bugs (which can be exploited)!
  - Think about tax systems…
  - Warren Buffett's tax rate is lower than his secretary's
    - 17.3% on $39.8 million taxable income
    - Heck, it's lower than my tax rate
  - The more complex, the more dangerous

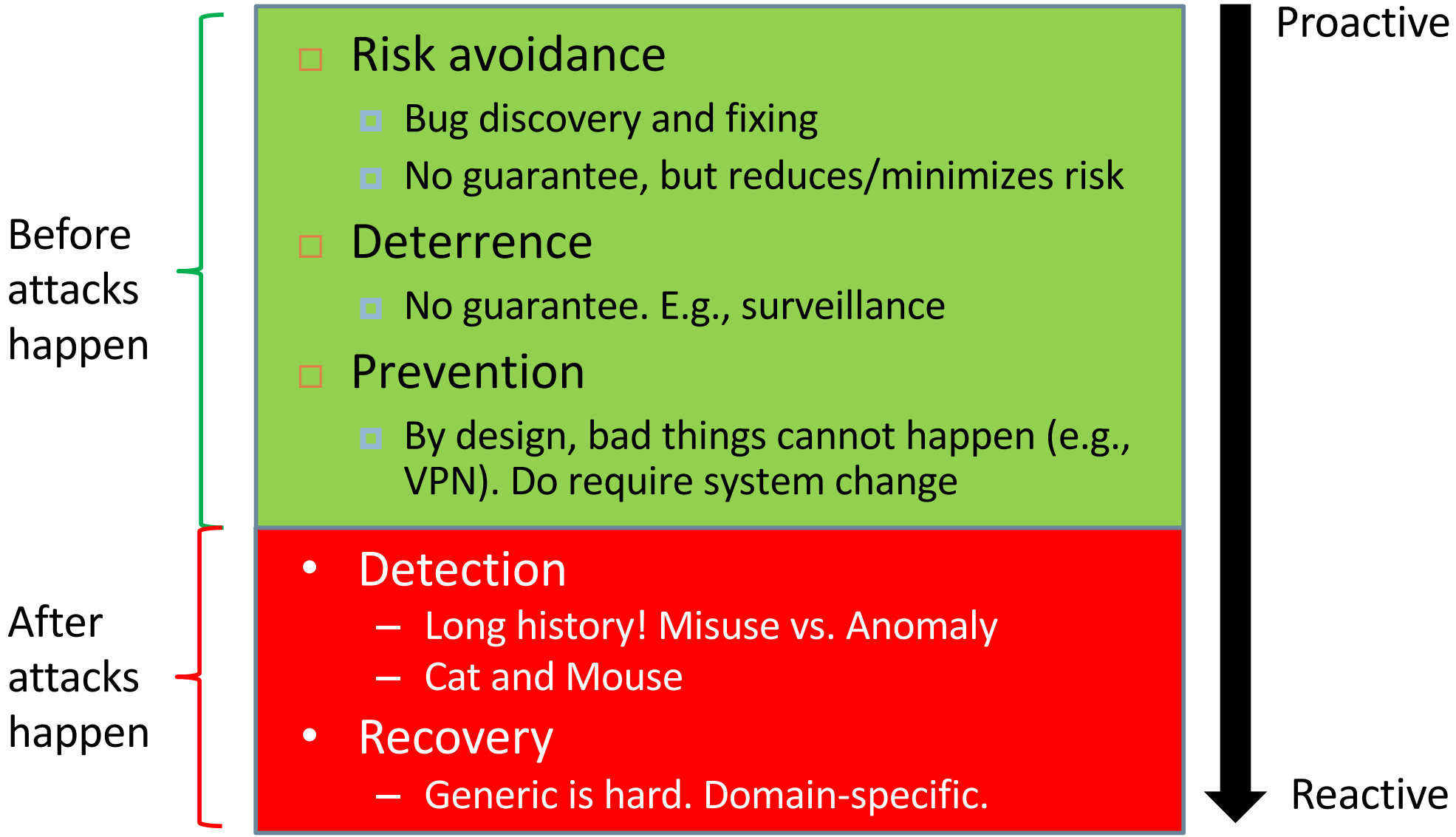
Thinking like an attacker

- Analyze game rules with different goals (threats)
  - Break into a door? Steal? Fake identity?
  - Exercise: How to steal my password or ATM PINs?
- Think outside the box
  - Make program run differently than expected
  - Exploit unexpected effects (e.g., side channels)
- Challenge security assumptions
  - Define the Threat Model
- One successful attack that exploits a vulnerability is good enough!

Thinking like a defender

- Discover loopholes in game rules and fix them
  - With respect to a Threat Model
  - Need to cover all corner cases (is currently HARD!)
  - Always catch-up
- Design favorable rules
  - Prevention of bad consequences (also HARD!)
  - Need to allow legitimate functionalities (which may lead to bad consequences)

Goals of defenders



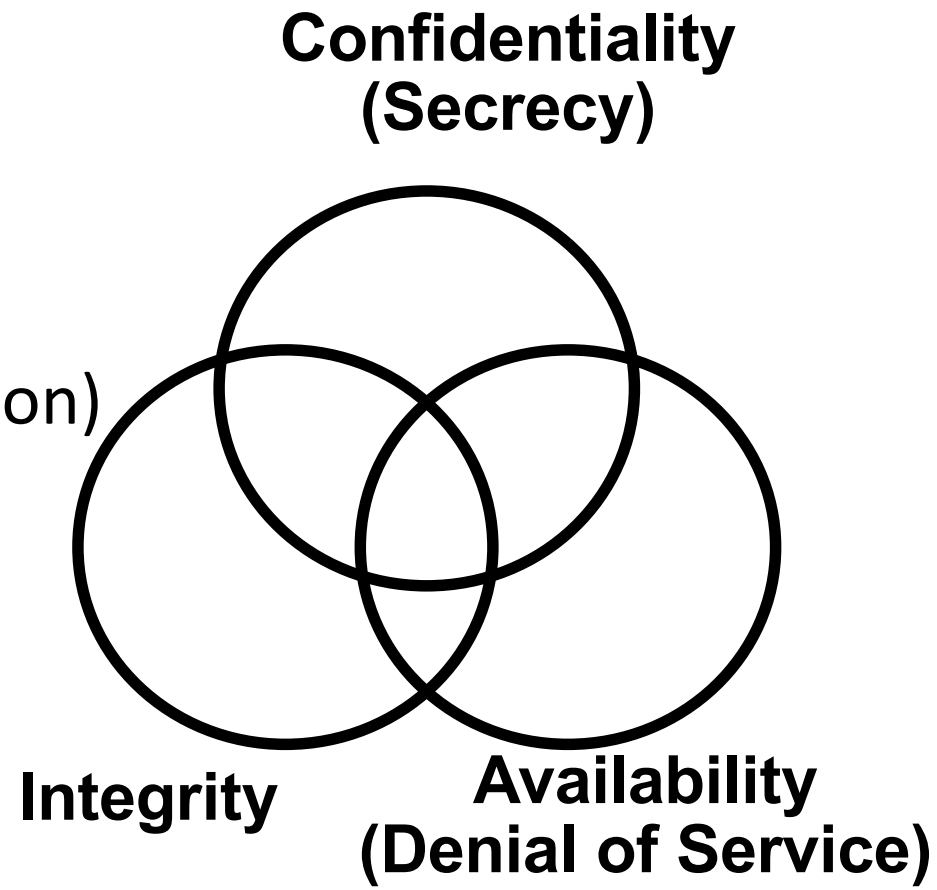
Case study (detection): how people ensure physical security

Allow “non-malicious/dangerous” people in →

Case study (detection): how people ensure cyber security

Basic Goals in Security (CIA)

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources



Threat model

- What resources/ capabilities / motivations the attacker has? What defenses are in place?

VS

Weakness < Vulnerability < Exploit < Attack

Topics

- Passwords
- Software security
- System security
- Network security

Not a theory
or
crypto class

Outline

- Welcome!
- Goals of this course
- Introduction of the class
- Exercises
- Grading

Course Info and Readings

- Course Management via Elearn (Canvas)
- Textbook
  - Tools and Jewels. Paul van Oorschot. Online.
- Readings for each class determined by the class schedule
  - https://www.cs.ucr.edu/~trentj/cs165-w24/schedule.html
    - Linked from syllabus in elearn and …
    - https://www.cs.ucr.edu/~trentj/cs165-w24/
- Optional Textbook
  - Hacking: The Art of Exploitation (2nd Edition), by Jon Erickson
    - *Useful for understanding attacks.*

Grading

- 4 Projects : 25%
- 2 homeworks: 10%
- 1 midterm: 25%
- 1 final: 35%
- Participation: 5%
  - Questions, answering others' questions, forum activities, intellectual contribution

Late policy

- 4 slack days for homework or project (combined)
- 2% bonus points if you do not use any
  - All or nothing
- UCR Academic Integrity Polices & Procedures
  - Linked to syllabus

Laws and Policies

- Respect others' privacy and rights
- Federal and state laws criminalize computer intrusion and wiretapping
  - e.g., Computer Fraud and Abuse Act (CFAA), Electronic Communications Privacy Act (ECPA)
- University of California Electronic Communications Policy
  - You can be expelled
- Do not share your work outside of class!

Ethics

- This course considers topics involving software exploitation techniques. As part of this investigation, we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class.

- When in doubt, please contact the instructor for advice. Do not undertake any action that could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor Jaeger.

Questions