Secure Software Systems

CYBR 200 | Fall 2018 | University of the Pacific | Jeff Shafer

BIZ & IT —

Wanted: Weaponized exploits that hack phones. Will pay top dollar

Exploit broker Zerodium ups the ante with $500,000 to target Signal and WhatsApp.

DAN GOODIN - 8/23/2017, 12:30 PM

Wikipedia

https://arstechnica.com/information-technology/2017/08/wanted-weaponized-exploits-that-hack-phones-will-pay-top-dollar/

Zerodium

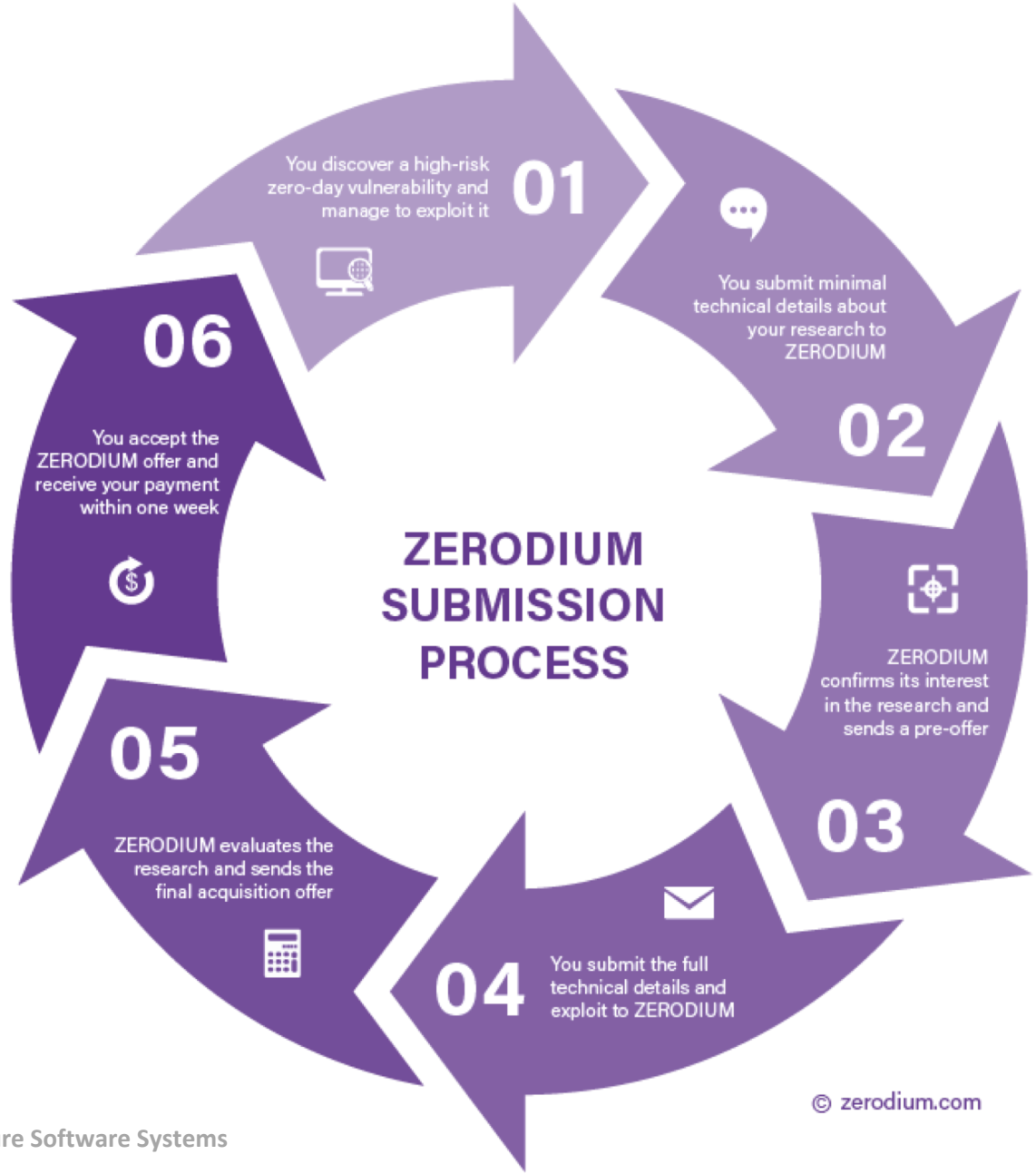
- Information security company from Washington DC
- Pays cash bounties for *unreported* zero-day vulnerabilities with working exploits and high security risks
  - https://zerodium.com/program.html
- Discloses them (only) to its customers (corps+govs)

Zerodium Price List

- iPhone
  - Remote Jailbreak w/Persistence, zero click
  - Up to **$1,500,000**
- Messaging apps (iMessage, WhatsApp, Signal, Facebook)
  - Remote code execution (RCE) w/local privilege escalation
  - Up to **$500,000**
- Apache Web Server on Linux (RCE)
  - Up to **$150,000**
- Wireless Baseband (RCE)
  - Up to **$150,000**

Just a *few* of many examples!

Zerodium Process



- If your software program is even *marginally* popular, it is a target
  - By legitimate researchers and firms (e.g. Zerodium)
  - By criminals
- Big money here!

Motivating Question

- **What do you, as a programmer, need to know about security (software *and* hardware) to write safe code that protects privacy/integrity/security?**
  - Secure software design
  - Secure coding
  - Security testing and auditing
  - Applied Cryptography

Course Overview

Websites

Main website

- https://cyberlab.pacific.edu/

Canvas CMS (gradebook only)

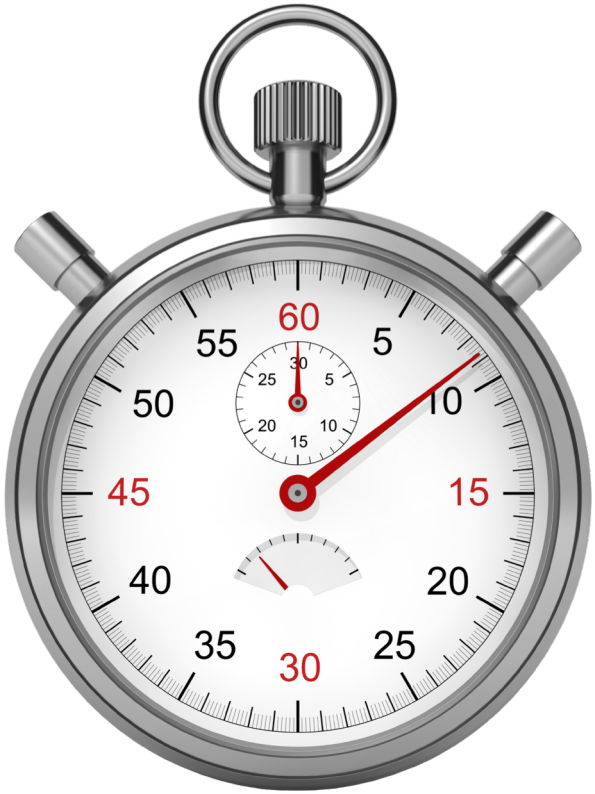
- http://canvas.pacific.edu

Textbook

- **No official textbook**
- May require technical paper readings prior to class lectures/discussion
  - Will announce in advance

Courseware Version 0.1a

- Only 15 weeks in a semester
  - **The clock is ticking now!**
- What to cover?



Lecture Topics

- Intro to Security
- Architectural approaches
  - Confinement
  - Trusted computing
- Cryptography
  - Symmetric vs Asymmetric
  - MACs and digital signatures
  - PKI
- Audit
- Authentication
  - Humans, Passwords, Tokens, Certs, …
- Authorization (Access Control)
  - Discretionary vs Mandatory
  - Run-time enforcement
- Software Analysis
  - Static analysis
  - Fuzzing

Grading

- **55%** - Projects
- **15%** - Midterm Exam
- **15%** - Final Exam
- **15%** - Labs

Course Projects


TESTING
BETA
TESTING


JAMES MONTGOMERY FLAGG
I WANT YOU
FOR
NEARES
COURSE
FEEDBACK!

Give and Take

I Promise…

- To keep the projects fun
- To be flexible with *requirements* and *deadlines* as we work through the projects

… If You Promise

- To communicate often with me
  - How long did the project take?
  - What was easy?
  - What was hard?
  - What additional resources (lectures, examples, …) would help?
  - Should we do this project next year?

Course Projects

- **Project 1 – Case Study**
  - **How are security flaws introduced and discovered in real-world, messy, complex products?**
  - Study bug reports, mailing lists, commit logs, … for a real program with publicly reported vulnerabilities
    - Understand program architecture
    - Understand what happened and its risks
    - Understand how it was fixed
  - Written report + oral presentation to class
  - Group project

Course Projects

- **Project 2 – Application Development**
  - **How can we put our theoretical knowledge to practice? (Ans: BIG PROGRAMMING PROJECT!)**
  - Must implement system involving: Authorization, Authentication, Audit, Confidentiality, and Integrity
  - You pick topic. Possible examples:
    - Network synchronized **bitcoin wallet**
    - Network synchronized **password manager**
    - **Secure chat program** (e.g. Signal)
    - **Electronic voting system**
    - **Medical Records system**
  - Group project, code + report + presentation

Schedule

This Week

- Tue August 28
  - Intro lecture
- Thur August 30
  - Project 1 Discussion
  - Security Policy & Aspects

Next Week

- Tue September 4
  - Threats, Harm, and Vulnerabilities
  - Goals and Requirements
- Thur September 6
  - Assurance

Questions?

- Questions?
- Concerns?