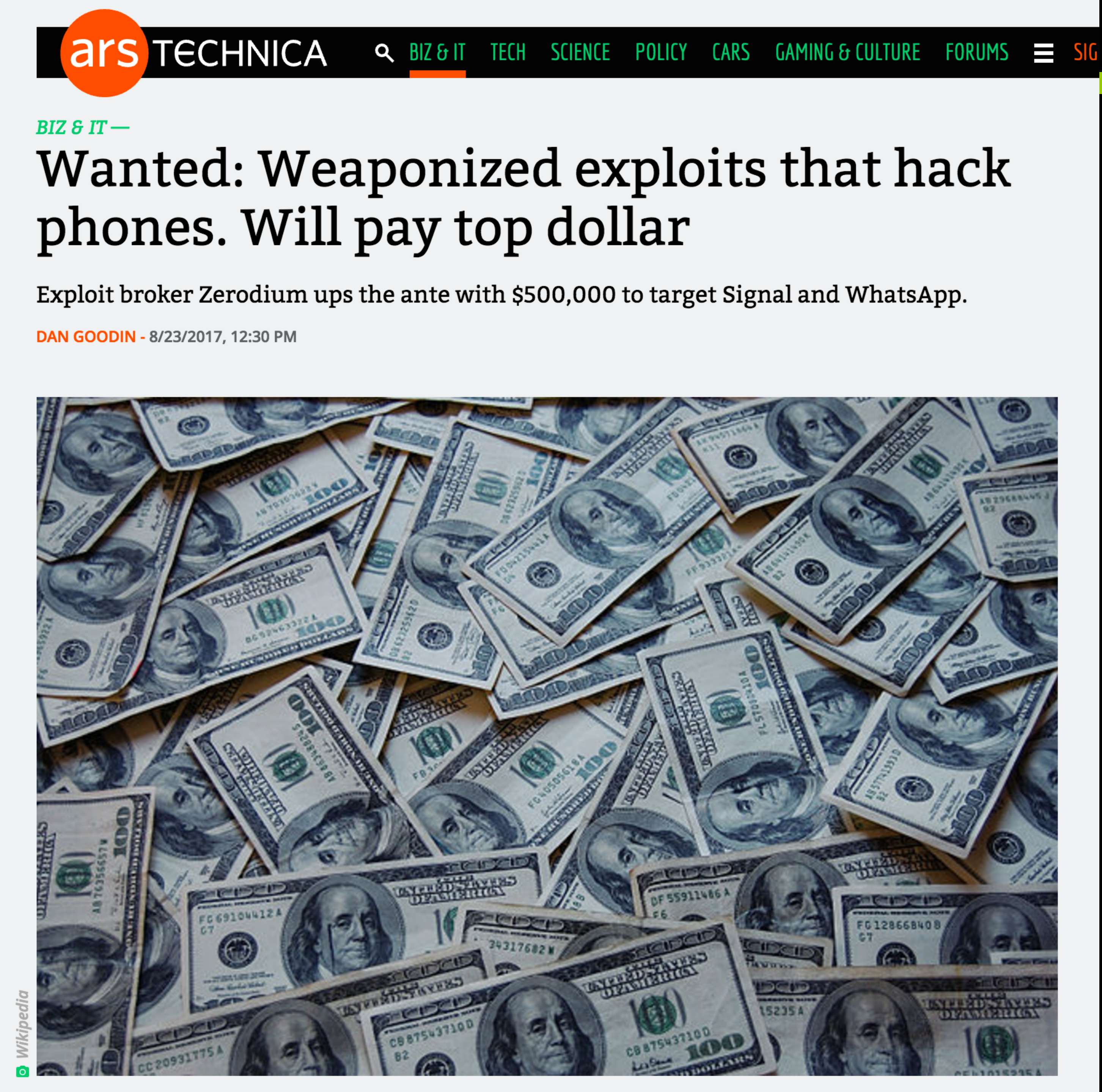
Secure Software Systems

CYBR 200 | Fall 2017 | 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

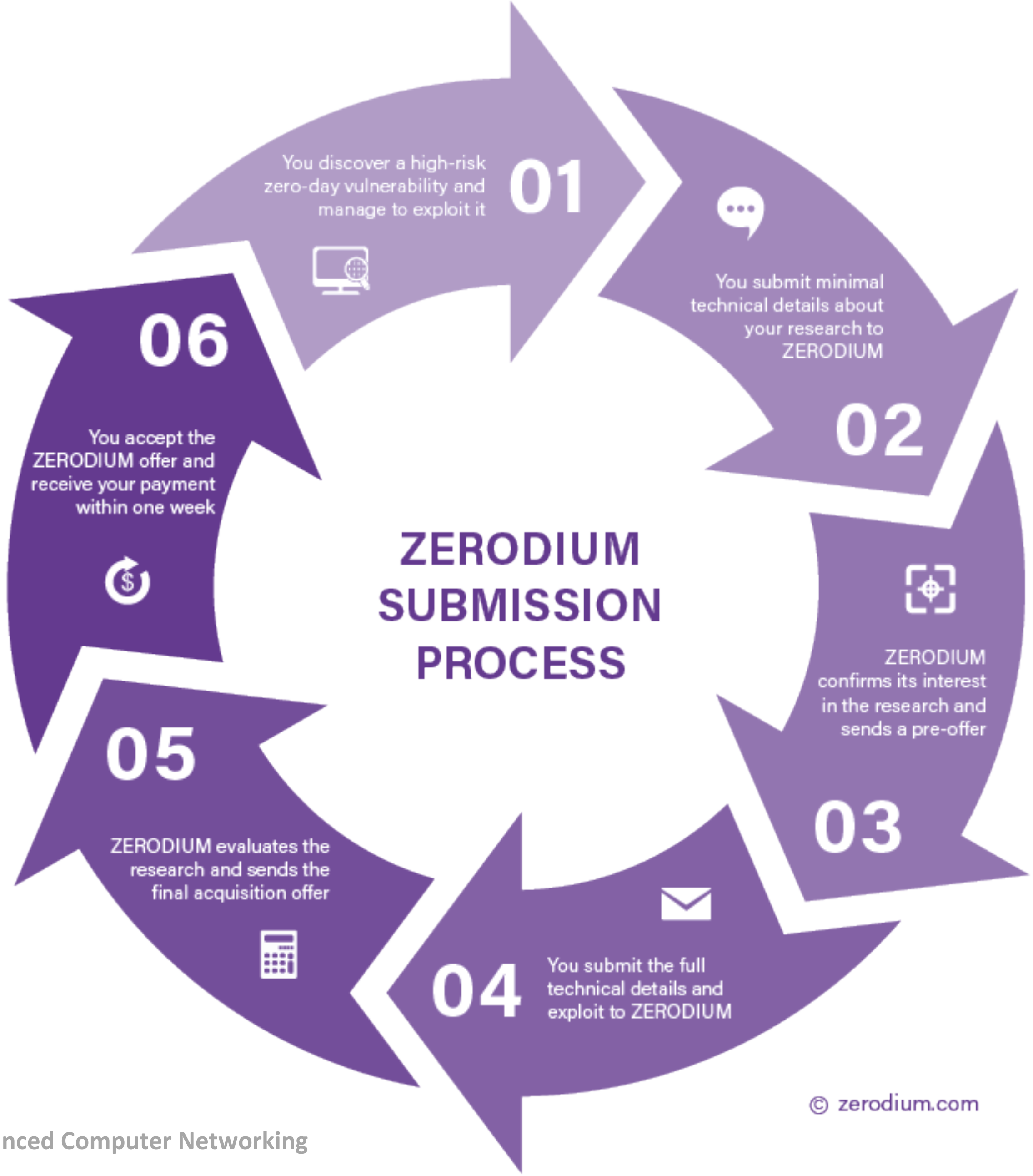
- Information security company from Washington DC
- Pays cash bounties for *unreported* zero-day vulnerabilities with working exploits and high security risks
  - https://zerodium.com/program.html
- Discloses them (only) to its customers (corps+govs)

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



ZERODIUM SUBMISSION PROCESS

01 You discover a high-risk zero-day vulnerability and manage to exploit it

02 You submit minimal technical details about your research to ZERODIUM

03 ZERODIUM confirms its interest in the research and sends a pre-offer

04 You submit the full technical details and exploit to ZERODIUM

05 ZERODIUM evaluates the research and sends the final acquisition offer

06 You accept the ZERODIUM offer and receive your payment within one week

© zerodium.com

- 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)

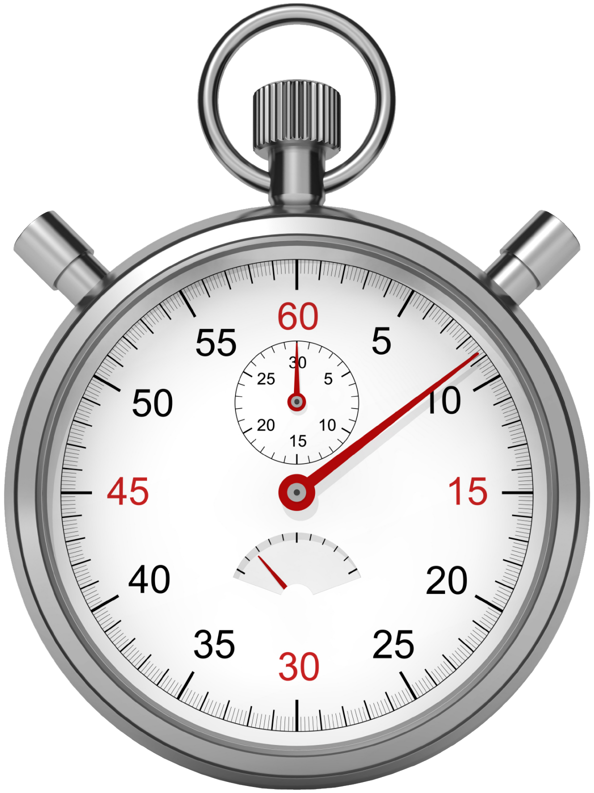
- http://canvas.pacific.edu

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
- Authentication
  - Humans, Passwords, Tokens, Certs, …
- Audit
- Authorization (Access Control)
  - Discretionary vs Mandatory
  - Run-time enforcement
- Software Analysis
  - Static analysis
  - Fuzzing
- Language Approaches
  - Type systems
  - Proof-carrying code

Grading

- **20%** - Project 1
- **40%** - Project 2
- **15%** - Midterm Exam
- **15%** - Final Exam
- **10%** - Instructor Whim (TBD)
  - In-class labs? Homework assignment?
  - *If not needed, other assignments will scale to 100%*

Course Projects

TESTING
BETA
TESTING

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

- Mon August 28
- Wed August 30
  - Intro lecture
- Fri September 1
  - Intro lecture
  - Start Project 1

Next Week

- Mon September 4
  - **Labor Day – No class!**
- Wed September 6
  - Architectural Approaches to Security
- Fri September 8
  - Architectural Approaches to Security

Questions?

- Questions?
- Concerns?