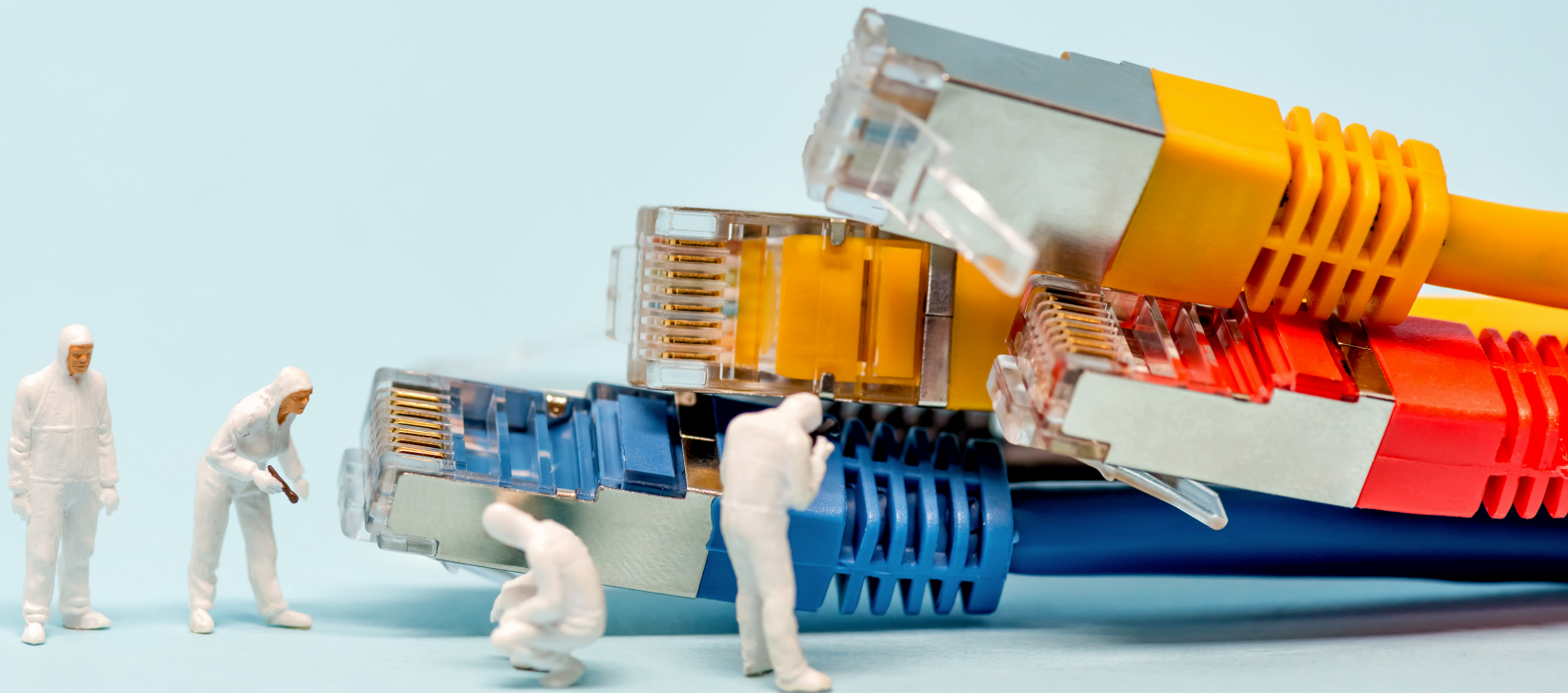


# Advanced Computer Networking

CYBR 230 | Fall 2018 | University of the Pacific | Jeff Shafer



# Motivating Question

- **How do [wired/wireless/mobile] networks work, and where do we even begin to secure them?**
  - Routing, network, and application-layer protocols
  - Tools for network mapping, analysis, and security
  - Cellular and mobile technologies

# Course Overview



# Websites

## Main website

- <https://cyberlab.pacific.edu/>

## Canvas CMS (gradebook only)

- <http://canvas.pacific.edu>

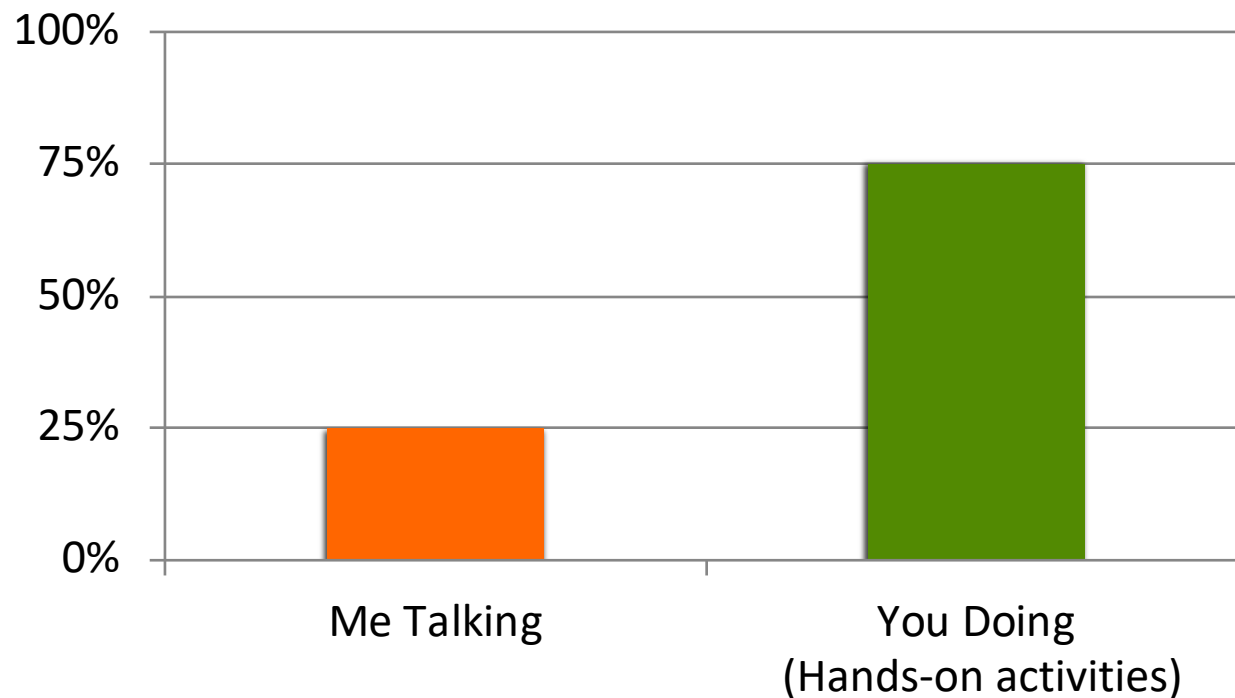


# Textbook

- **No official textbook**
- **Please suggest useful online or print references throughout the semester**
  - Goal is to make the cyberlab website a comprehensive resource

# Class Time

➤ The goal\* in designing this course:



\* Actual time in any specific class may vary

# Lecture Topics

- Network layer
  - IPv6
- Transport layer
  - QUIC – Quick UDP Internet Connections
- Application Layer
  - HTTP/2
  - DOH – DNS over HTTP
- Wireless
  - 802.11 / WPA3
  - Bluetooth(?)
- Network monitoring tools
- Other topics?
  - Software Defined Networking (SDN)
  - TOR - Routing, overlay networks, and cryptography
- **Whatever background information is required for projects**
- **Other topics you are interested in?**

# Grading

## ➤ **100% - Projects**

- Implementation
- Written documentation
- Oral presentation

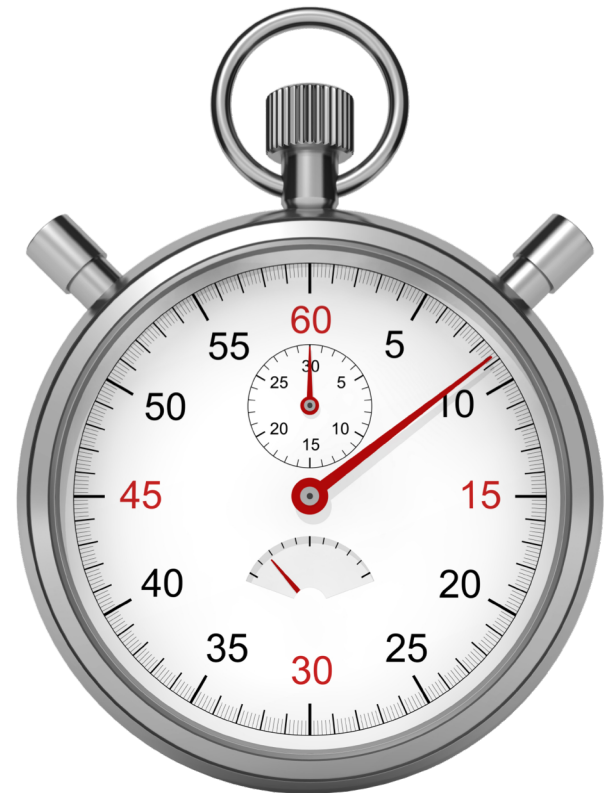
No homework, no exams

# Course Projects



# Courseware Version 0.2a

- Networking is a huge field
  - Too much content to cover
- Only 15 weeks in a semester
  - **The clock is ticking now!**
- What to cover in projects?
  - Network protocols?
  - Transport protocols?
  - Application protocols?
  - Wired/wireless/mobile?













# Courseware Version 0.1a

- Congratulations on your new role!
  - **Guinea pig / beta tester**
- *Last year's class were also guinea pigs, and focused significantly on the physical network construction. Could repeat that effort again... but why?*

# 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

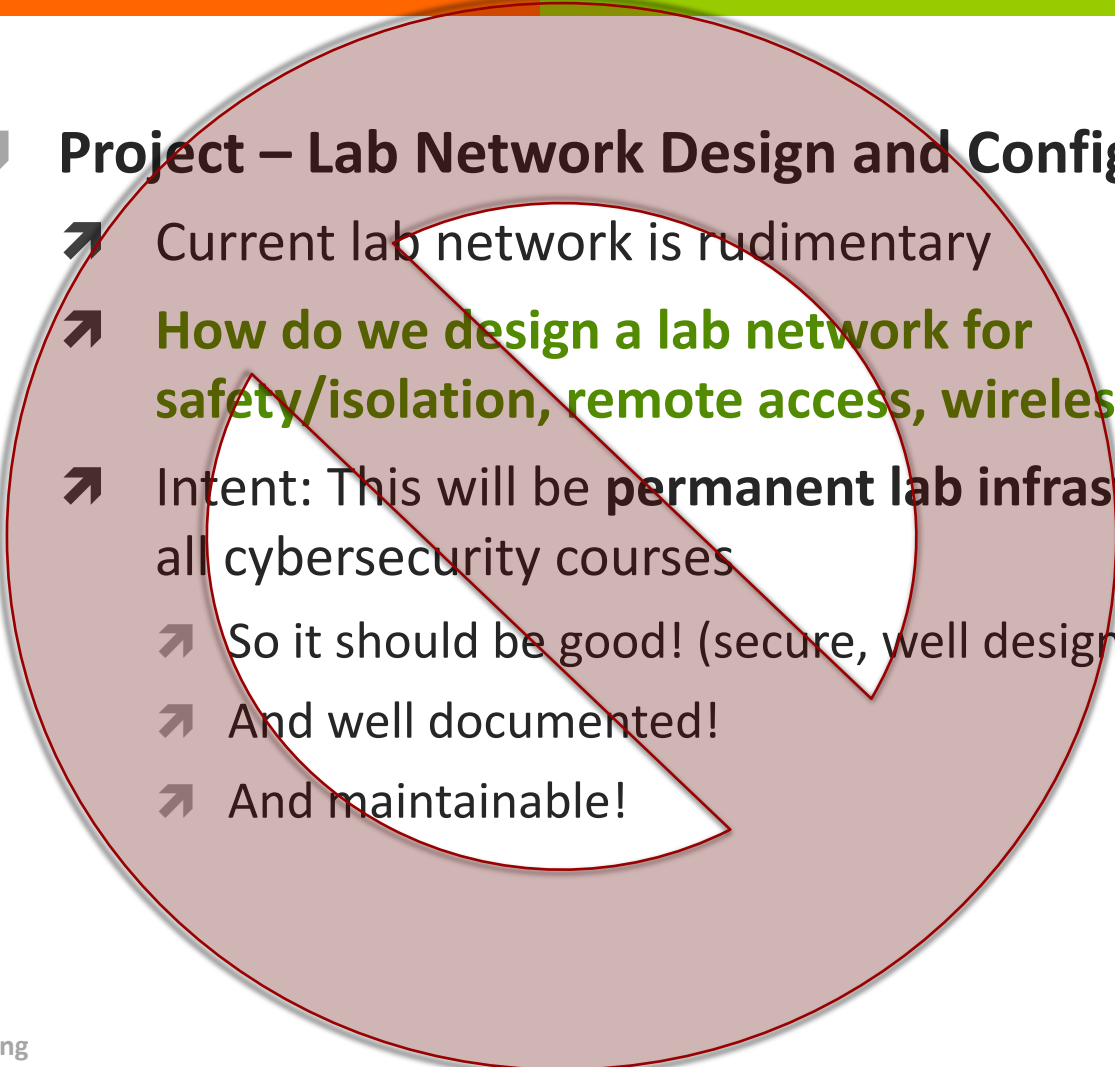
- To communicate often with me
  - How long did the project take?
  - What was easy?
  - What was hard?
  - What additional resources (lectures, examples, ...) would help?
  - Should we do this project next year?







# Course Projects

- 
- **Project – Lab Network Design and Configuration**
    - Current lab network is rudimentary
    - **How do we design a lab network for safety/isolation, remote access, wireless, ...?**
    - Intent: This will be **permanent lab infrastructure** for all cybersecurity courses
      - So it should be good! (secure, well designed, etc.)
      - And well documented!
      - And maintainable!

# Course Projects

## *(Monitoring)*

- **Project – Lab Network Monitoring: Setup**
  - **How do we monitor the network we created?**
  - Full packet capture and flow data
  - Logging logging logging
  - Analysis tools

# Course Projects

## *(Monitoring)*

- **Project – Lab Network Monitoring: Background –vs– Malicious Traffic**
  - Lab network is too quiet
  - **How do we generate some legitimate traffic?**
    - Proposal: Programmatically automate web browsers to surf top-100 sites
  - **How do we generate some malicious traffic?**
    - Proposal: Run actual malware
  - Use monitoring tools to identify presence of malware (signal vs noise of background traffic)

# Course Projects

## *(Monitoring)*

- **Project** – Honeypot Internet monitoring & data collection system
  - Inspired by Thinkst “Canary” devices
  - Impersonate specific “victim”
    - IOT camera?
    - Synology NAS?
    - File server?
    - Web server?
  - Needs to be **protocol accurate** – don’t want attacker to easily tell the difference
  - Hosted on AWS?

# Course Projects

## *(Network Layer - Wireless)*

- **Project – 802.11 Attacks**
  - Force de-authentication and re-auth?
  - RTS/CTS control frame attack?
  - Evil twin attack?



# Course Projects

## *(Network Layer - Wired)*

### ➤ **Project** - Layer 2 Attacks (TBD)


- Spanning tree?
- Cisco Discovery Protocol?
- Dynamic Trunking Protocol?
- 802.1Q? (VLANs) 802.1X? (Port-based access control)
- Examples: <http://www.yersinia.net/>
- Projects would involve writing attack code and detection/monitoring code)



# Course Projects

## *(Transport / Application Layer)*

### ➤ **Project** – Secret Tunnels

- Part 1 - Research all the tunnel methods that the campus network blocks
  - Categorize by obfuscation methods used
  - Explain (hypothesize?) methods of detection
- Part 2 - Find a way to tunnel anyway and implement!  


# Course Projects

## *(Application Layer)*

- **Project - Application Layer Attacks**
  - DNS spoofing attack?
  - DHCP attack?
  - Amplification attack? (Memcached, DNS, NTP, etc...)
    - Anything that can be requested via UDP (easier to forge source address without TCP's 3-way handshake) and has reply message much larger than request
  - HTTP/HTTPS MITM attack?
    - Example: <https://www.bettercap.org/>
  - Projects would involve writing attack code and detection/monitoring code)

# Course Projects

## *(Application Layer)*

### ➤ **Project – DNS Spoofing**

- Part 1 – Write a tool that will produce a malicious DNS response faster than the legitimate DNS server
  - Result: megabank.com goes to attacker IP
- Part 2 – How can you detect this attack?
  - Can you write a plugin for something like the Bro IDS?

# Course Projects

## *(Application Layer)*

- **Project** – HTTP/2 (or DOH, or ....) implementation
  - Either client or server (not both)
  - All headers are compressed
  - Fully multiplexed
  - Server can push file to client without client even requesting it!

# Course Projects

- At some point December arrives and class is finished!
- **Discuss**
  - **Project Preferences?**
  - **Where should we start first?**



# Questions?

➤ Questions?

➤ Concerns?