

Week 14: Lecture B

The Grand Finale & Final Review

Thursday, December 5, 2024

Announcements

- **Project 4: NetSec** due by 11:59PM **tonight**
 - As usual, **2 extra days** to submit late for a 10-point penalty

Project 4: Network Security

Deadline: Thursday, December 5 by 11:59PM.

Before you start, review the [course syllabus](#) for the Lateness, Collaboration, and Ethical Use policies.

You may optionally work alone, or in teams of **at most two** and submit **one project per team**. If you have difficulties forming a team, post on **Piazza's Search for Teammates** forum. Note that the final exam will cover project material, so you and your partner should collaborate on each part.

The code and other answers your group submits must be entirely your own work, and you are bound by the University's Student Code. You may consult with other students about the conceptualization of the project and the meaning of the questions, but you may not look at any part of someone else's solution or collaborate with anyone outside your group. You may consult published references, provided that you appropriately cite them (e.g., in your code comments). **Don't risk your grade and degree by cheating!**

Complete your work in the **CS 4440 VM**—we will use this same environment for grading. You may not use any **external dependencies**. Use only default Python 3 libraries and/or modules we provide you.

Announcements

- **Lecture Quiz** grades finalized
 - Lowest score dropped
- **Attendance/Participation** grades coming soon
 - Based on lecture participation (three absences dropped)
 - Extra credit opportunities (e.g., Wiki PRs) close after today
- **Project 4** grades coming early next week
 - Keep an eye out for the **regrade form** on Piazza

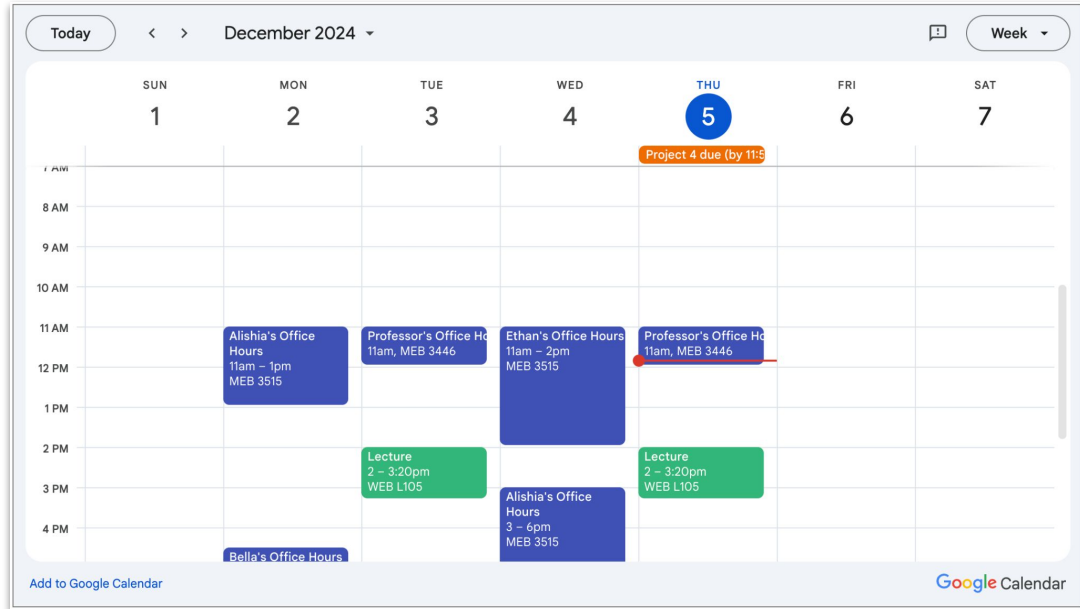
Final Exam

- **Save the date: 1–3PM on Tuesday, December 10**
 - **CDA accommodations:** schedule exam via CDA Portal
- **High-level details** (more to come in this lecture):
 - One exam covering all course material
 - Similar to project/quiz/lecture exercises
- **Cheat Sheet**
 - **One 8.5"x11" paper** with handwritten/typed notes on **both** sides
 - **Suggestion:** Don't just use someone else's—you'll learn better making **your own!**
 - **Suggestion:** Don't just paste lecture slides—you'll learn better by **writing/typing** it!



Office Hours

- **Office hours** end today
 - For pressing issues, contact me to make an appointment
- **Piazza** forum still open
 - Feel free to ask questions and help your peers study
 - Course staff will continue answering questions up **until final exam begins**



Questions?



This time on CS 4440...

Course Wrap-up
Final Exam Overview
Exam Review

Before we continue...

Thank you for making my fifth semester at The U really fun!

I wish all of you success in your future studies, careers, and lives.

Swing by my office anytime (MEB 3446) if you ever want to chat.



Semester Recap

- An introduction to security topics in:
 - Communications
 - Applications and OS's
 - The Web and Networks



Semester Recap

- An introduction to security topics in:
 - Communications
 - Applications and OS's
 - The Web and Networks
- Gained hands-on experience with:
 - Cryptanalysis
 - Exploit writing
 - Packet analysis



Semester Recap

- An introduction to security topics in:
 - Communications
 - Applications and OS's
 - The Web and Networks
- Gained hands-on experience with:
 - Cryptanalysis
 - Exploit writing
 - Packet analysis
- Security has advanced **a lot** since...



Semester Recap

- An introduction to security topics in:
 - Communications
 - Applications and OS's
 - The Web and Networks
- Gained hands-on experience with:
 - Cryptanalysis
 - Exploit writing
 - Packet analysis
- Security has advanced **a lot** since...
 - But many **these same attacks still happen!**

Kishan Bagaria @KishanBagaria

texts team took a quick look at the tech behind nothing chats and found out it's extremely insecure

it's not even using HTTPS, credentials are sent over plaintext HTTP

backend is running an instance of BlueBubbles, which doesn't support end-to-end encryption yet

@nothing · Nov 15

Evangelidis · @AkisEvangelidis · Nov 15

ing Chats - Messages are end-to-end encrypted on any servers - once a message is delivered, it is decrypted locally from your personal device.

```
{
  "iss": "https://securetoken.google.com/bluebubblemessaging-dev",
  "aud": "bluebubblemessaging-dev",
  "auth_time": 1700079302,
  "device_id": "..."
}
```

Overview | Contents | Summary | Chart | Notes

```
1 {
2   "name": "gmail.com"
3   "token": "ic10iJSUzI1N1sIntpZC161"
4 }
```

Headers | Text | Hex | JavaScript | JSON | JSON Text

```
1 "accountID": "mlUserF20"
2 "userID": "4sGfRrqJkegb"
3
```

11:46 AM · Nov 17, 2023 · 614.8K Views

Semester Recap

My hope: that you will go out into the world and preach the **importance** of **strong cyber security!**

Gained hands-on experience with:

- Cryptanalysis
- Exploit writing
- Packet analysis

Security has advanced **a lot** since

- But many **these same attacks still**



Describe what you learned in this course in a single word:

Nobody has responded yet.

Hang tight! Responses are coming in.



Describe your overall experience with this course in one word:

Nobody has responded yet.

Hang tight! Responses are coming in.



CS 4440 ~~v1.0~~ ~~v2.0~~ v3.0

- First semester's issues (v1.0)
 - Lectures ending early
 - Python learning curve
 - Help on prerequisites (GDB, etc.)
 - Overload from Homework + Projects
 - TAs unfamiliar with course material



CS 4440 ~~v1.0~~ ~~v2.0~~ v3.0

- First semester's issues (v1.0)
 - Lectures ending early
 - Python learning curve
 - Help on prerequisites (GDB, etc.)
 - Overload from Homework + Projects
 - TAs unfamiliar with course material
- Improvements last semester (v2.0)
 - More review content
 - "Course Wiki" with tutorials
 - Replaced Homeworks with Quizzes
 - Projects now delivered as web pages
 - TAs that have taken the class



CS 4440 ~~v1.0~~ ~~v2.0~~ v3.0

- Improvements this semester (v3.0)
 - New freely-hosted **textbooks** on website
 - **Supplementary Content** for each lecture
 - **Open-sourcing Course Wiki** (and extra credit!)
 - **Guest Lecturers** (partly due to my travel)
 - A variety of quality-of-life fixes behind the scenes



How much did you utilize Course Wiki?

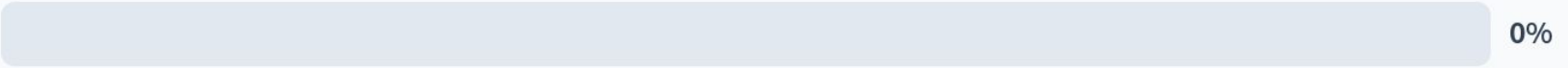
A lot!



Some.



Not at all...



Did you use the Supplementary Content / Textbooks?

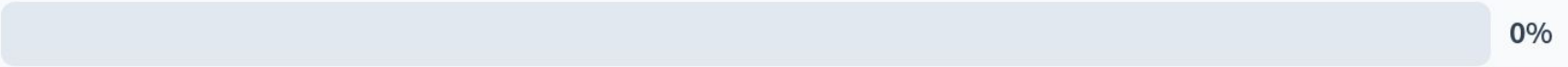
A lot!



Some.



Not at all...



What other content would you have liked to see on the Wiki?

Nobody has responded yet.

Hang tight! Responses are coming in.

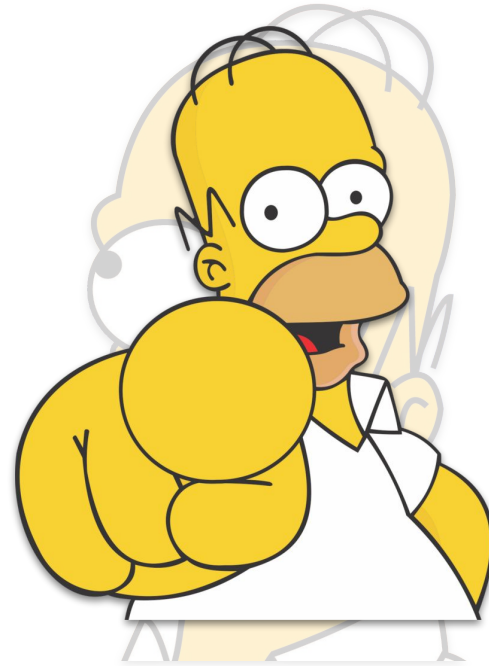


- Room for improvement (**v3.0**):
 - Better in-class poll exercises
 - More Wiki content
 - Add-ons, cool tricks
 - Video demos / tutorials
 - Memory inspection
 - Attack debugging
 - Packet analysis
 - Instructor speaking too fast (**sorry!**)
 - Projector sporadically dying?




CS 4440 ~~v1.0~~ ~~v2.0~~ ~~v3.0~~ **v4.0**

- Room for improvement (**v3.0**):
 - Better in-class poll exercises
 - More Wiki content
 - Add some cool tricks
 - V
 - Interested in **TA'ing**?
Join the team!
ta.cs.utah.edu
 - In
 - Projector sporadically dying?



Want to learn more?

- **CS 4440:** Introduction to Computer Security 
- **CS 5490:** Network Security
- **CS 5961:** Modern Cryptography
- **CS 5963:** Cyber-physical Systems & IoT Security
- **CS 5963:** Applied Software Security Testing (my course)
- **And more exciting courses are being planned!**

End-of-semester Course Evals

- **I want your feedback!**
 - 3rd time teaching this course 😊
 - **Help me improve the class!**
- Due by **December 19th**
 - <https://scf.utah.edu>
 - **Please please please!**



End-of-semester Course Evals

- I want your feedback!
 - 3rd time teaching this course 😊
 - Help me improve the class!

- Due by Dec 15
 - <https://survey.com>
 - Please pl

If 85% of the class (82 of 96 students) submits an eval, we will add **5 points of extra credit** to your Participation grades!

HELP ME HELP YOU

Before we continue...

- **Please take a few minutes to submit your course evaluations**
 - To give you privacy, I will leave the room for **7 minutes**

scf.utah.edu/blue



Final Exam Overview

The Final Exam

- Date: this coming **Tuesday, December 10**
- Duration: **1–3 PM**
- Location: **WEB L105** (same location as lecture)
- Cheat Sheet:
 - **One 8.5"x11" paper** with handwritten or typed notes on **both** sides
 - **Suggestion:** Don't just use someone else's—you'll learn better making **your own!**
 - **Suggestion:** Don't just paste lecture slides—you'll learn better by **writing/typing** it!

The Final Exam

- **Structure:** **seven** multi-part questions
 - True or False
 - Short answer
 - System design
 - Exploit writing
 - Security analysis

- It will require **analysis** and **synthesis**

Topics (non-exclusive)

■ **Security properties**

- Integrity
- Confidentiality
- Authentication
- Availability

■ **Secure Design**

- Thinking like an attacker
- Threat modeling
- Kerckhoffs's principles

Topics (non-exclusive)

- **Cryptography**
 - Randomness and pseudorandomness
 - Hash functions and MACs
 - Stream ciphers
 - Block ciphers
 - Modes of operation
 - Confusion and diffusion
 - Initialization vectors
 - Padding
 - Substitution vs. transposition
 - One-time pads

Topics (non-exclusive)

- **Public-key Crypto**
 - Basics of RSA
 - RSA for confidentiality
 - RSA for integrity
 - Interplay with symmetric-key crypto
 - When to use what and why
 - Key exchange
 - Diffie-Hellman
 - RSA
 - Digital signatures

Topics (non-exclusive)

- **Application Security**
 - Vulnerabilities and Attacks
 - Buffer/integer overflows
 - Code injection and reuse
 - Return-oriented Programming
 - Drawing and analyzing the stack
 - Defenses
 - ASLR vs. DEP
 - Application isolation
 - Memory isolation
 - Virtual machines
 - Sandboxing
 - Containers

Topics (non-exclusive)

- **Web Security**
 - SQL-injection
 - HTTP vs HTTPS
 - Same-origin policy
 - XSS
 - Reflected
 - Stored
 - CSRF
 - GET vs POST
 - Certificates
 - CAs
 - Chaining

Topics (non-exclusive)

- **Network Security**
 - Packet sniffing
 - Email spoofing
 - Man-in-the-middle attacks
 - DoS and DDoS attacks
 - Reflection
 - Amplification
 - DNS poisoning

Topics (non-exclusive)

- **Authentication**
 - Three factors
 - Brute forcing
 - Rainbow tables
 - Salted hashing
 - Password reuse

Topics (non-exclusive)

- **Malware**
 - Malware
 - Spyware
 - Ransomware
 - Viruses
 - Worms
 - Rootkits
 - Botnets

Topics (non-exclusive)

- **Miscellaneous**
 - Software testing
 - Black/grey/white-box
 - Side channels
 - Timing and power
 - Optical
 - Reverse engineering
 - Applications
 - Challenges
 - Adversarial ML
 - Evasion attacks
 - Poisoning

Practice Exam Review



Next time on CS 4440...

The Final Exam