ECE560
Computer and Information Security

Fall 2020

Introduction and Course Policies

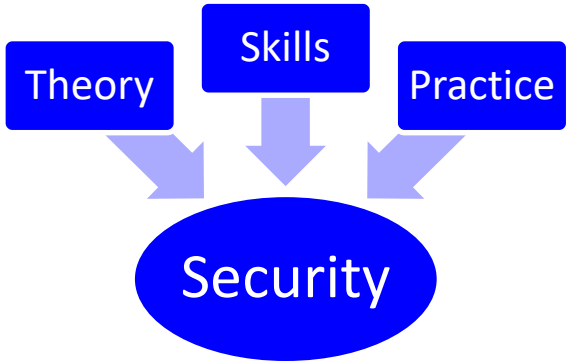
Tyler Bletsch
Duke University

Instructor and TAs

- Professor: Tyler Bletsch
  - Office: ~~Hudson Hall 106~~ Zoom
  - Email: Tyler.Bletsch@duke.edu
  - Office Hours: see course site
- Teaching Assistants:
  - See course site
  - Some are on this zoom!
    (I hope)

Course objective: Evolve your understanding of security

- **Theory**:
  - How do I think systematically about security?
  - What constructs are available for me to use?
  - How do I understand *new* threats and defenses not covered in the course?
- **Skills**:
  - What tools are commonly used to do the above?
  - How can I manipulate data and automate things to make the above practical?
- **Practice**:
  - "Stick time": Actually doing it.
  - Both attacking and defending.



Getting Info

- **Course Web Page**: static info

  http://people.duke.edu/~tkb13/courses/ece560/

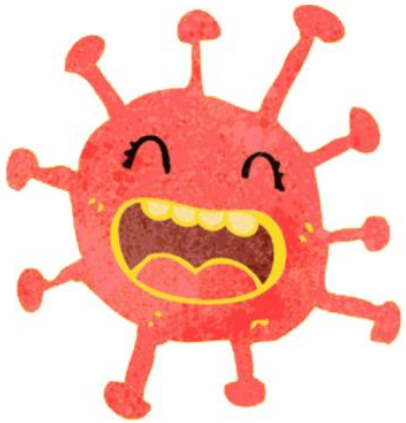
  

  - Syllabus, schedule, slides, assignments, rules/policies, prof/TA info, office hour info
  - Links to useful resources

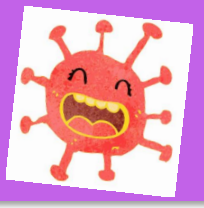
- **Piazza**: questions/answers
  - Post all of your questions here
  - Questions must be "public" unless good reason otherwise
  - **No code or copyable answers** in public posts!

- **Sakai**: just assignment submission and gradebook

Stuff that's different because we're hybrid during COVID-19



Planning for failure or planning for success?



- How to definitely be miserable, depressed, and fail

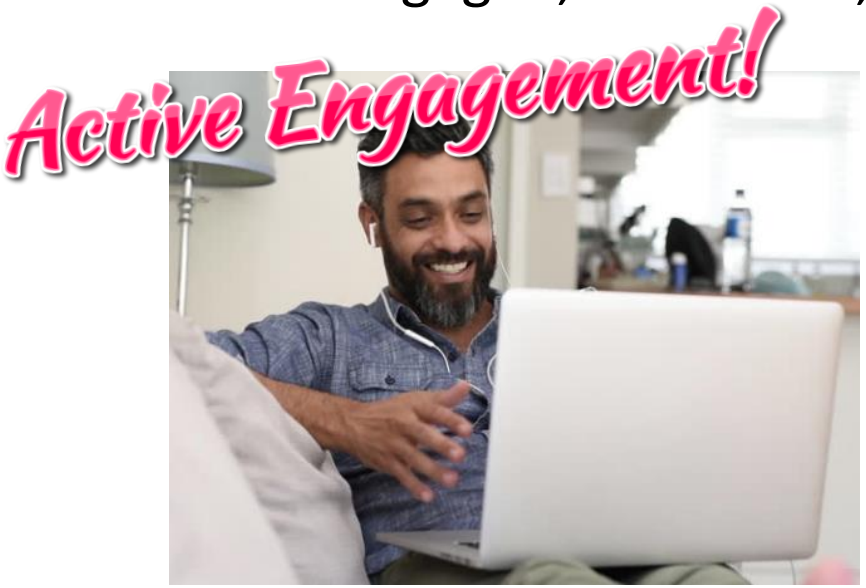
welp time to "attend" my "class" 😒

ughhhhhhhhhhhhhhhhhhhhhhhhh

(Later)

oh no how do you computer?!??

- How to be engaged, interested, and pass



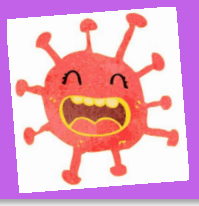
I have a question that I'm asking out loud in real time with real people, thus engaging my brain, getting valuable socialization, establishing a rapport with my peers!

Also I have a beard now!

(Later)

im fine here too

Hybrid course policies for online people!



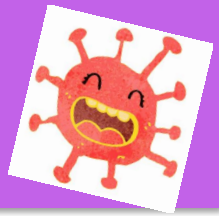
- The course is **synchronous**
  - **Video *<u>on</u>* please**: You were going to wear clothes and sit upright if this were in person, why change that?

- Live attendance of **lecture** is expected
  - I may add quizzes if this doesn't appear to be working
- Recordings will be made available for reference later

  (They will always be private to students in the course)

- What if you have **real life reasons** why you can't do the above?
  - You may request to take the course **asynchronously** by emailing me directly.
  - Valid reasons: crazy timezone, complicated living/working situation
  - Invalid reason: preference

CRITICALLY IMPORTANT TO GOOD HAPPY SUCCESS

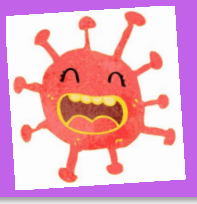


Interrupt me

with

QUESTIONS!!!!

How to interrupt me

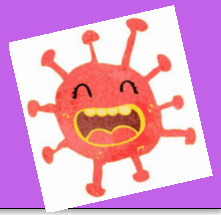


1. Try the “Raise hand” button in Zoom or in real life

2. If I don’t notice in 10 seconds, **unmute and make sounds until I stop**.

“It’s not rude if I’m literally telling you to do it.”

The general vibe here



These are extraordinary times.

The course conditions are extraordinary.

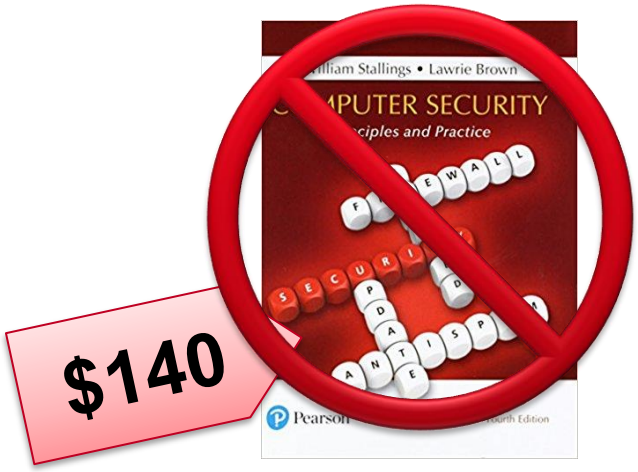
The Duke response has been extraordinary.

The logistics of running a course like this hybrid will be extraordinary.

Let our commitment to each another and to ourselves also be extraordinary!

Textbook

- Text: **Computer Security: Principles and Practice (4th Edition)**, by Stallings & Brown
  - Get the **GLOBAL EDITION**, it's the EXACT SAME BOOK for cheaper.
- The course uses the textbook highly out-of-order, see course site for readings.



ISBN 0-13-479410-9

exact same content!

ISBN 1-292-22061-9

If you go to **addall.com**, you can search all online booksellers at once.

Workload

- Homework assignments – **discussed collaboratively, done individually**
  - Pencil and paper problems
  - Programming problems
  - Technical exercises
  - Attack and defense scenarios
  - Data manipulation and automation tasks

  - *Security is broad and diverse field* →
    Lots of different things to practice →
    Lots of work!!

***Some* collaboration is allowed**

ALLOWED: Collaboration on *approach* or *concepts*.
DISALLOWED: Collaboration on *answers*.

All artifacts you submit must be entirely your own.

Advice for homework survival!

"I spent 20 hours on this one problem!"

- **Don't do that**. Put a fair bit of effort in (~2 hours), then ask for help and put that problem aside.
- Recommended workflow (based on iterative deepening):
  - **Do shallowest problems first** instead of proceeding sequentially:
    Finish all the simple problems; try the harder ones
    - Note questions that block progress; ask in piazza/class/office hours
  - **Put the assignment aside**; do other stuff. Why?
    - Your posted questions will get answered (no blocking!)
    - Your brain will work on problems subconsciously
      (free background processing!)
  - Now do a **deeper pass** -- finish the medium-difficulty ones and dig deep into the harder ones, asking questions and taking a break as before
  - **Loop until done**: {make progress, ask questions, switch to other tasks}
- Your operating system time slices tasks when they block to maximize throughput and efficiency, so why shouldn't you?

Grading Breakdown

Assignment	%
Homeworks	60%
Midterm exam	20%
Final Exam	20%

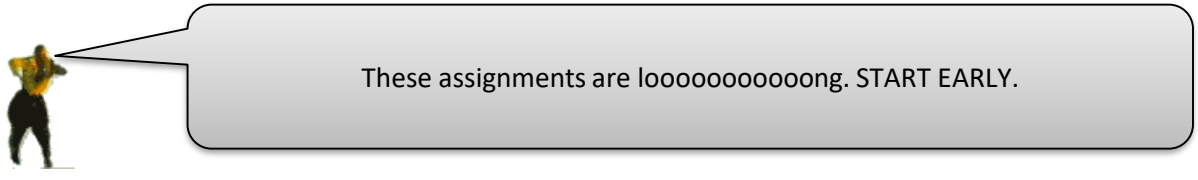
Partial credit is available – provide detail in your answers to seek it!

Late homework submissions incur penalties as follows:

- Submission is 0-24 hours late: total score is multiplied by 0.9
- Submission is 24-48 hours late: total score is multiplied by 0.8
- Submission is more than 48 hours late: total score is multiplied by the Planck constant (in J·s)

~6.6×10^{-34}

NOTE: If you feel *in advance* that you may need an extension, contact the instructor.



Homework Zero

- Due Wednesday night
- Designed to get you familiar with UNIX in general and Linux in particular
- UNIX skills are for more than this course – there's a **reason** people use these tools!
- If you're having trouble, post on Piazza and we can help you.

This is the same Homework 0 sometimes given in ECE/COMPSCI 250.

If you've already done it there, you don't need to do it again – just submit the screenshot from the training system.

Grade Appeals

- All regrade requests must be in writing to the TA
- After speaking with the TA, if you still have concerns, contact the instructor
- All regrade requests must be submitted no later than 1 week after the assignment was returned to you.

Academic Misconduct

- Academic Misconduct
  - Refer to Duke Community Standard
  - Homework content is individual – you do your own work
  - Common examples of cheating:
    - Copying and rephrasing written answers from another student
    - Using code or answers from an outside source
- I will not tolerate any academic misconduct!

- "But I didn't know that was cheating" is not a valid excuse

***Some* collaboration is allowed**

ALLOWED: Collaboration on *approach* or *concepts*.
DISALLOWED: Collaboration on *answers*.

All artifacts you submit must be entirely your own.

Goals of This Course

- Things you will understand after this course:
  - Fundamental security objectives: **Confidentiality, Integrity,** and **Availability**
  - How to develop and describe a **threat model**
  - The types of **security threats and attacks** that must be dealt with
  - How to distinguish among various **types of intruders** and their behavior patterns
  - The **poor programming practices** that cause many security vulnerabilities
  - Major **networking protocols, standards, and tools**
  - **Symmetric and asymmetric cryptography** including message authentication
  - **User authentication**
  - How to reason about and implement **security policies**
  - How to secure **operating systems, databases, hypervisors,** and **cloud environments**
  - The role of **firewalls, intrusion detection,** and **intrusion prevention systems**
  - Security **auditing** and **forensics**
  - **Social engineering** attacks
  - **Ethical and legal aspects** of security

Our Responsibilities

- The instructor and TA will…
  - Provide lectures/recitations at the stated times
  - Set clear policies on grading
  - Provide timely feedback on assignments
  - Be available out of class to provide reasonable assistance
  - Respond to comments or complaints about the instruction provided

- Students are expected to…
  - Receive lectures/recitations at the stated times
  - Turn in assignments on time
  - Seek out of class assistance in a timely manner if needed
  - Provide frank comments about the instruction or grading as soon as possible if there are issues
  - Assist each other *within the bounds of academic integrity*

Computing resources

- We'll make extensive use of VMs from the Duke Virtual Computing Manager: https://vcm.duke.edu/
  - Students in this course will have their VM limit raised to 4
  - These VMs have public internet IP addresses – practice good security!
- Later, you will be given access to VMs running Kali Linux (a distribution of Linux with many security tools pre-installed)
  - Take care of these – if you blow one up, IT has to rebuild it.
- We will use shared target machines from time to time
  - Treat these with respect – unless otherwise noted, you should ONLY do the prescribed actions to them. Do not "attack" systems you are not explicitly told to.

Homework survival tips!

"I spent 20 hours on this one problem!" – Many past students

- Don't do that. Put a fair bit of effort in (~2 hours), then get help.
- Recommended workflow based on **iterative deepening**:
  - Don't go linearly; do shallowest first. Finish low-hanging problems and *start* the harder ones. Note questions as you go.
  - Put the assignment aside and do other stuff. Why?
    - Posted questions get answered in background (no blocking = efficiency)
    - The human brain works on problems subconsciously.
      When you come back, they will be easier! (free processing = efficiency)
  - Then do a deeper pass -- finish medium-difficulty problems and dig further into harder ones. Ask questions and multitask as before. Loop until done.
- Benefits:
  - Makes good use of the full time provided
  - Avoids both procrastination and frustration.

Your OS time slices tasks to maximize throughput and efficiency; why shouldn't you?

Ethics in Security

- There are three flavors of security practitioner in the world:
  - **White hat**: Obey the law, work to make systems secure
  - **Black hat**: Break the law, infiltrate (usually for profit)
  - **Grey hat**: Does both (so still super unethical)
- There is ONE flavor of security practitioner in this course:

- All students must sign and turn in an **ethics pledge** in order to receive credit on any assignments (see course site!)