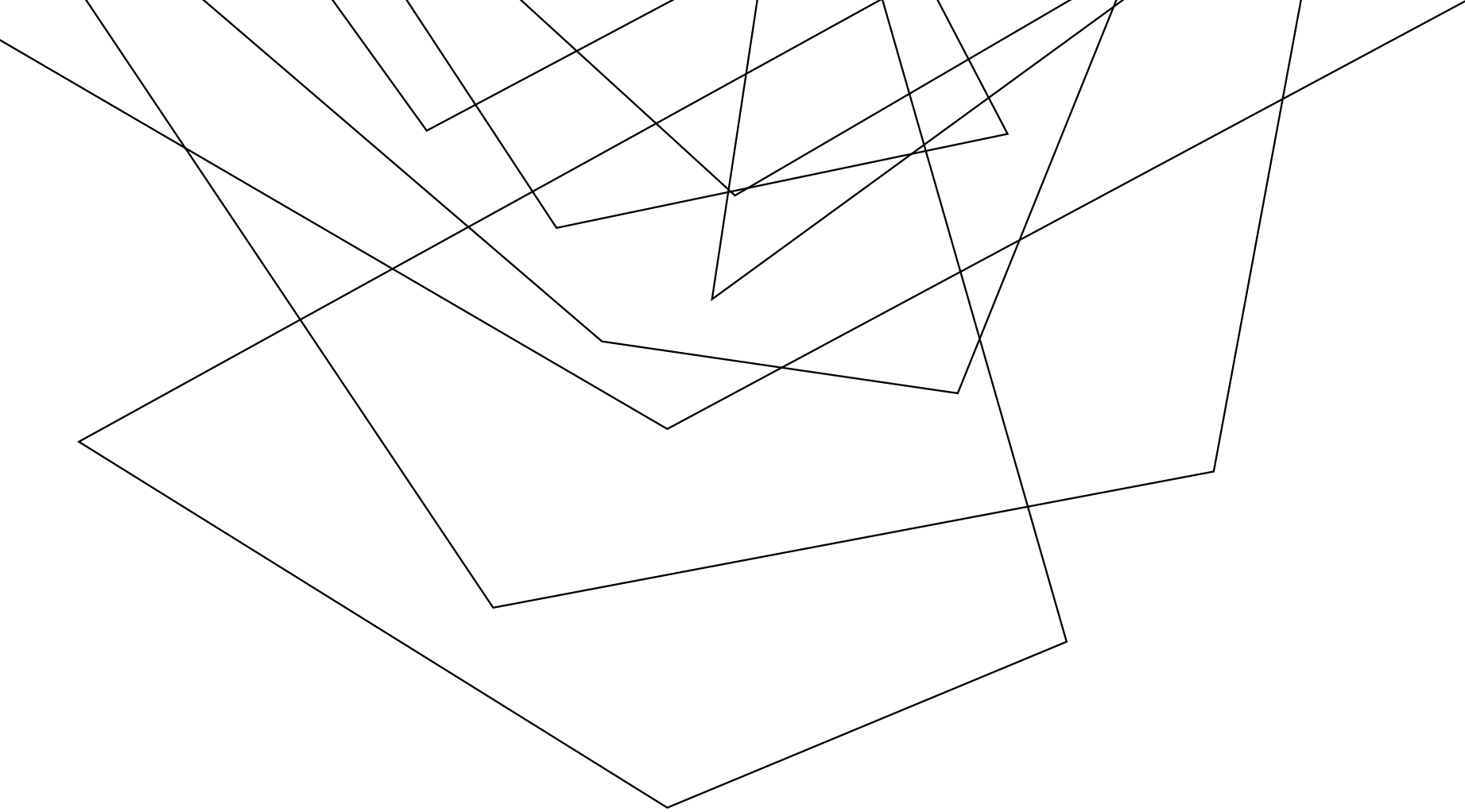


EXERCISE #1

BASELINE KNOWLEDGE REVIEW

Write your name and answer the following on the provided form
(I have pens for this class only)

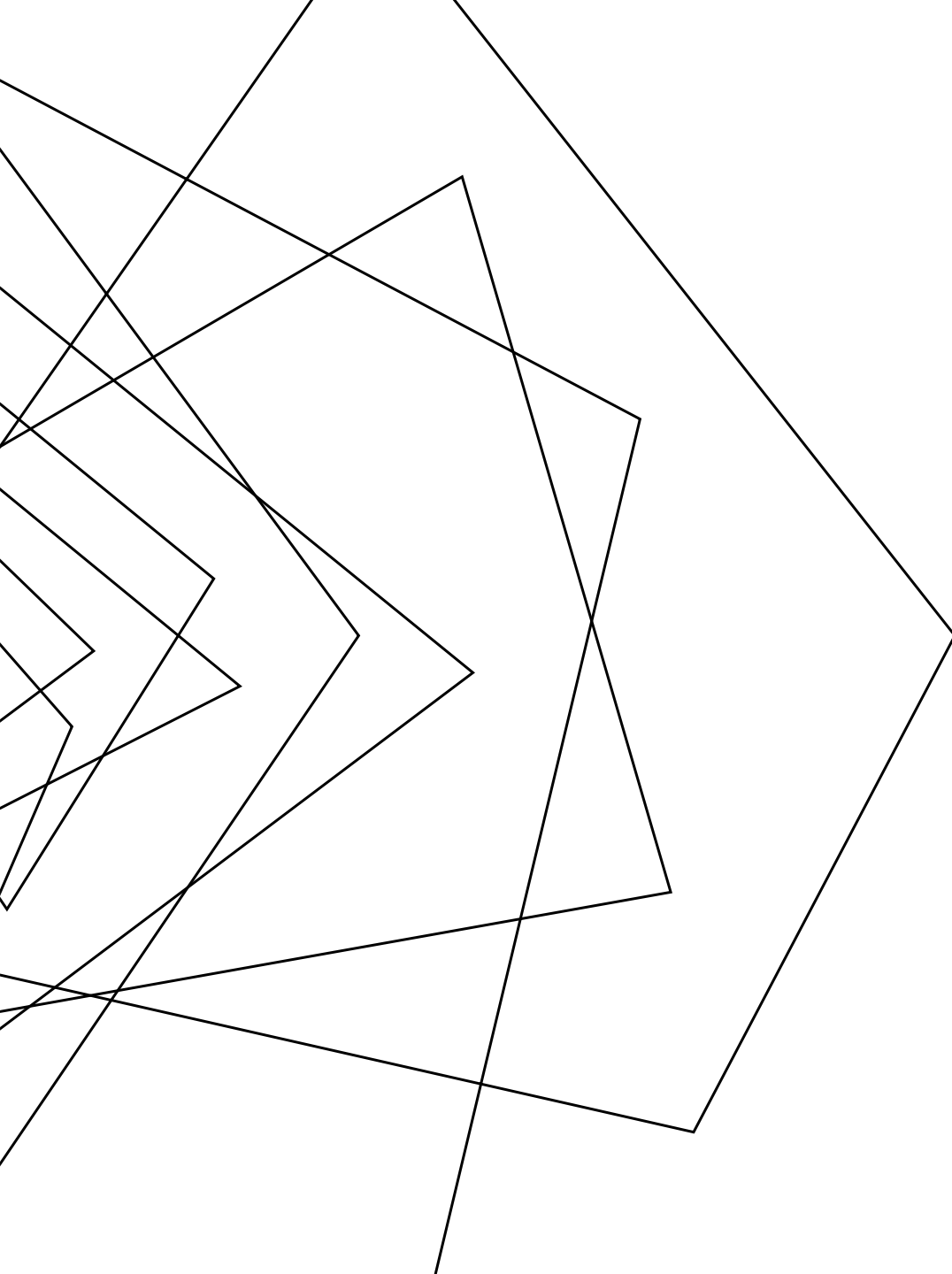
- What is a buffer overflow attack? What are the consequences of such an attack?
- What is static analysis?
- In computer security, to what does the CIA triad refer?

Abstract geometric lines in the top-left corner of the slide, consisting of several thin black lines forming overlapping, irregular polygons and triangles.

OVERVIEW

EECS 677: Software Security Evaluation

Drew Davidson

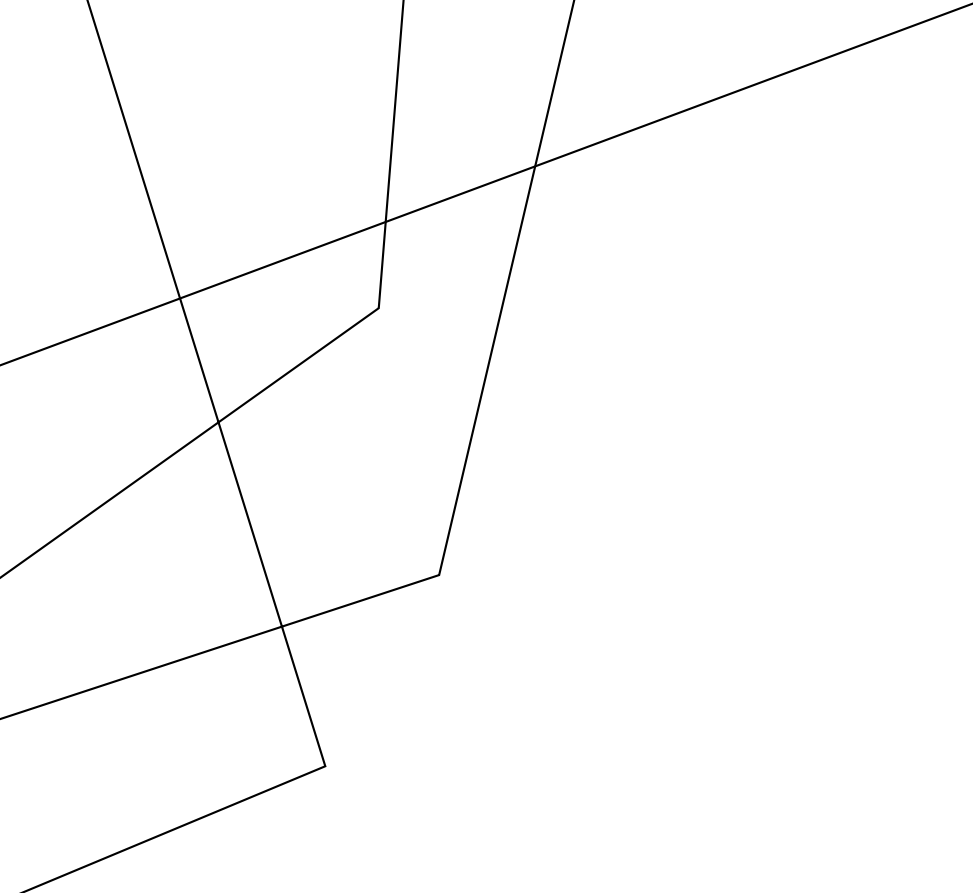


FAST FACTS FROM THE JUMP

I'M RECORDING THIS LECTURE

I'LL POST THE VIDEO AND THESE SLIDES
ON THE CLASS WEBSITE

[HTTPS://ANALYSIS.COOL](https://analysis.cool)



ADMINISTRIVIA AND ANNOUNCEMENTS

ASSIGNMENTS

Entry Survey

- Out **now**
- Due tonight at 11:59 PM on Canvas

Exercise #1

- If you're here, you just got 100%
- If you missed this class, due on Sunday at 11:59 PM
- In the future, you'll need to bring your own pencil + paper

TODAY'S ROADMAP

Orientation

- About me
- About you
- About the course

Evaluating Evaluation



ABOUT ME



**(Associate) Professor
Andrew “Drew” Davidson**

~~Pronouns: he/him/his~~

THE JOB OF A PROFESSOR

ABOUT ME

The actual start of my job offer letter from KU:

Dear Drew

We are delighted that you will be joining the Department of Electrical Engineering and Computer Science (EECS). The terms and conditions of your appointment are set forth in your official offer of employment from the University. This letter provides details and expectations specific to your academic unit.

Responsibilities

Distribution of Effort (FTE).

The 1.0 FTE for this initial appointment is distributed as follows:

- 0.4 FTE Teaching/Advising
- 0.4 FTE Research
- 0.2 FTE Service

I'M A MANDATORY REPORTER

ABOUT ME

<https://civilrights.ku.edu/sexual-misconduct>

I (like nearly all KU faculty and staff) am designated as a **mandatory reporters**.

I'm required to report incidents of discrimination and sexual harassment, including sexual violence, to the Office of Civil Rights & Title IX.

The following positions **are not mandatory reporters** and can keep your information confidential:

CARE (Campus Assistance, Resource, and Education) Coordinator

[785-864-9255](tel:785-864-9255) | care@ku.edu

KU Counseling and Psychological Services (CAPS)

[785-864-2277](tel:785-864-2277) | caps.ku.edu

University Ombuds

[785-864-7261](tel:785-864-7261) | ombuds@ku.edu

MY TEACHING PHILOSOPHY

ABOUT ME

How
Teach?

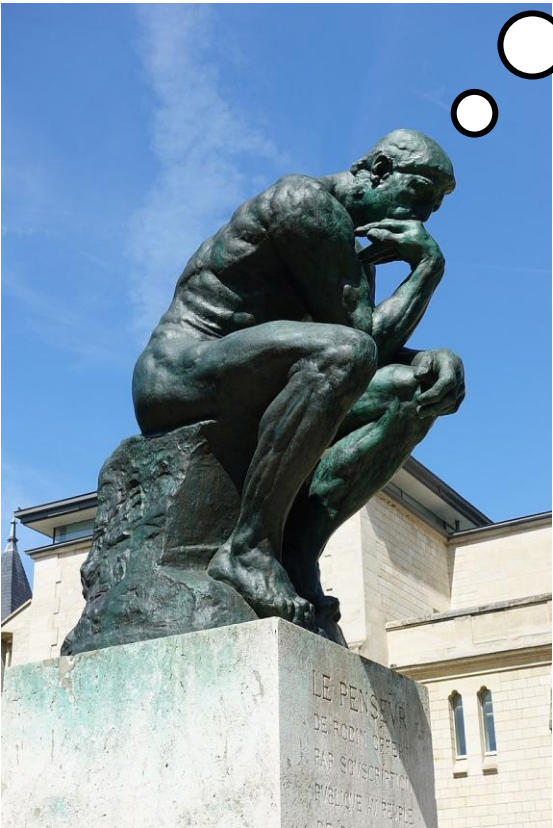
Teach the class I'd like to take

- Treat your time as a valuable resource
- Avoid the annoyances I experienced as a student

Objectives – Teach a class that is

- Entertaining
- Enjoyable
- Informative ← *Most important*

“Like what?”



WHAT TO CALL ME

ABOUT ME

- **Preferred:** “Drew”
- **Ok:** “Professor Davidson”, “Dr. Davidson”
- **Never:** “Andy”, “Andrew”, “Mr. Davidson”, “Dr. Drew”



Dr. Drew (Extremely not me) [1]

[1]: Credit: www.podcastone.com/Dr-Drew-Show

INTERACTING WITH ME

ABOUT ME

(I think) **I am pretty friendly**

- I'll make an effort to learn every student's name
- If you see me outside of class, feel free to say "hi!"

I like when you visit office hours

- Appreciate when you come with a specific question



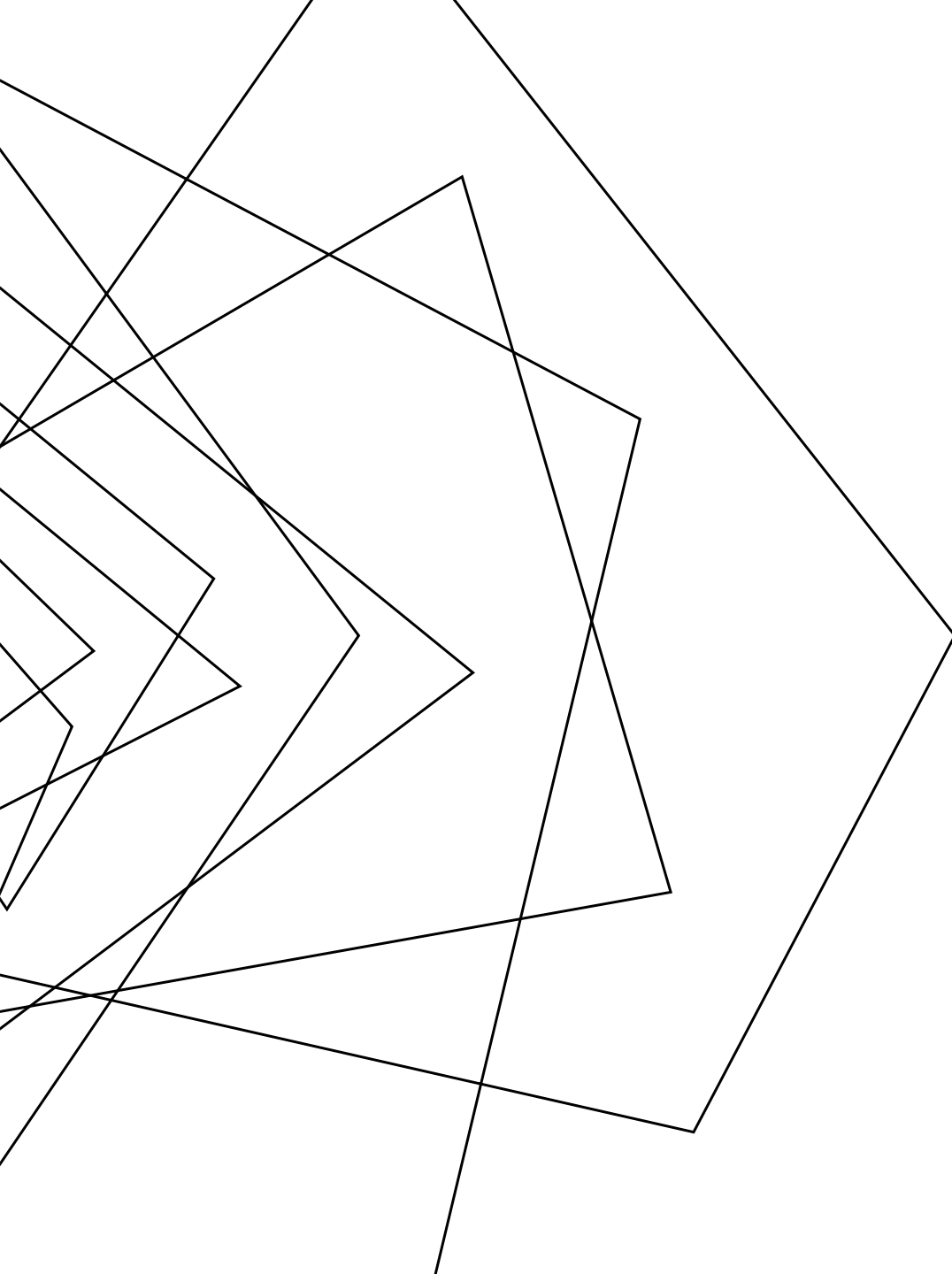
TODAY'S ROADMAP

Orientation

- About me
- About you
- About the course

Evaluating Evaluation





CLASS COMPOSITION

86% UNDERGRADUATE STUDENT

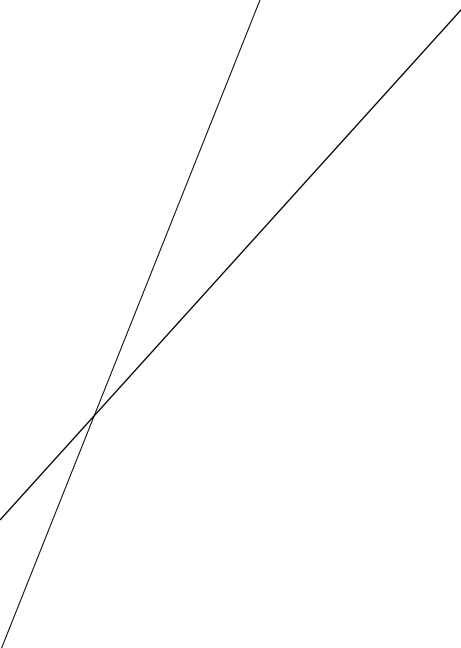
14% GRADUATE STUDENT

COURSE ENTRY SURVEY

ABOUT YOU

To get a better sense of each student, I'm also asking you to complete a brief (private) survey

<https://analysis.cool/survey>

Two thin, dark lines intersecting diagonally in the top-left corner of the slide.

YOUR HYPOTHETICALLY ASKED QUESTIONS (HAQ)? ABOUT YOU

IS DREW A GOOD
TEACHER?

Maybe?

YOUR HYPOTHETICALLY ASKED QUESTIONS (HAQ)? ABOUT YOU

IS DREW A GOOD
TEACHER?

Maybe?

QUALITY

1.0

DIFFICULTY

4.0

EECS665

Feb 28th, 2022

For Credit: **Yes** Attendance: **Mandatory** Would Take Again: **No** Grade: **A-** Textbook: **No**

If you dont enjoy working on class work for hours every day this class may not be for you. The amount of work is absurd, and not even beneficial to your learning. Most of the class is very lost and usually end up learning from each other instead of the lectures.

LOTS OF HOMEWORK

SKIP CLASS? YOU WON'T PASS.

Helpful  0  2



YOUR HYPOTHETICALLY ASKED QUESTIONS (HAQ)? ABOUT YOU

IS DREW A GOOD
TEACHER?

Maybe?

IS THIS CLASS
HARD?

Depends what you mean!



IS THIS CLASS HARD?

ABOUT YOU: HAQ

Depends on your definition of “hard”

“A Lot of work”

- I hope it’s a moderate amount of work

“Success is rare”

- Probably not

“Miserable”

- I want this to be “No”

“Conceptually Complex”

- I want this to be “yes”

Grade Breakdown

Survey - 1%

Quizzes – 39% (planning on 3 total)

Exercises – 10%

Homework – 50%

YOUR HYPOTHETICALLY ASKED QUESTIONS (HAQ)? ABOUT YOU

IS DREW A GOOD
TEACHER?

Maybe?

IS THIS CLASS
HARD?

Depends what you mean!

DO I HAVE TO COME
TO CLASS?

No!

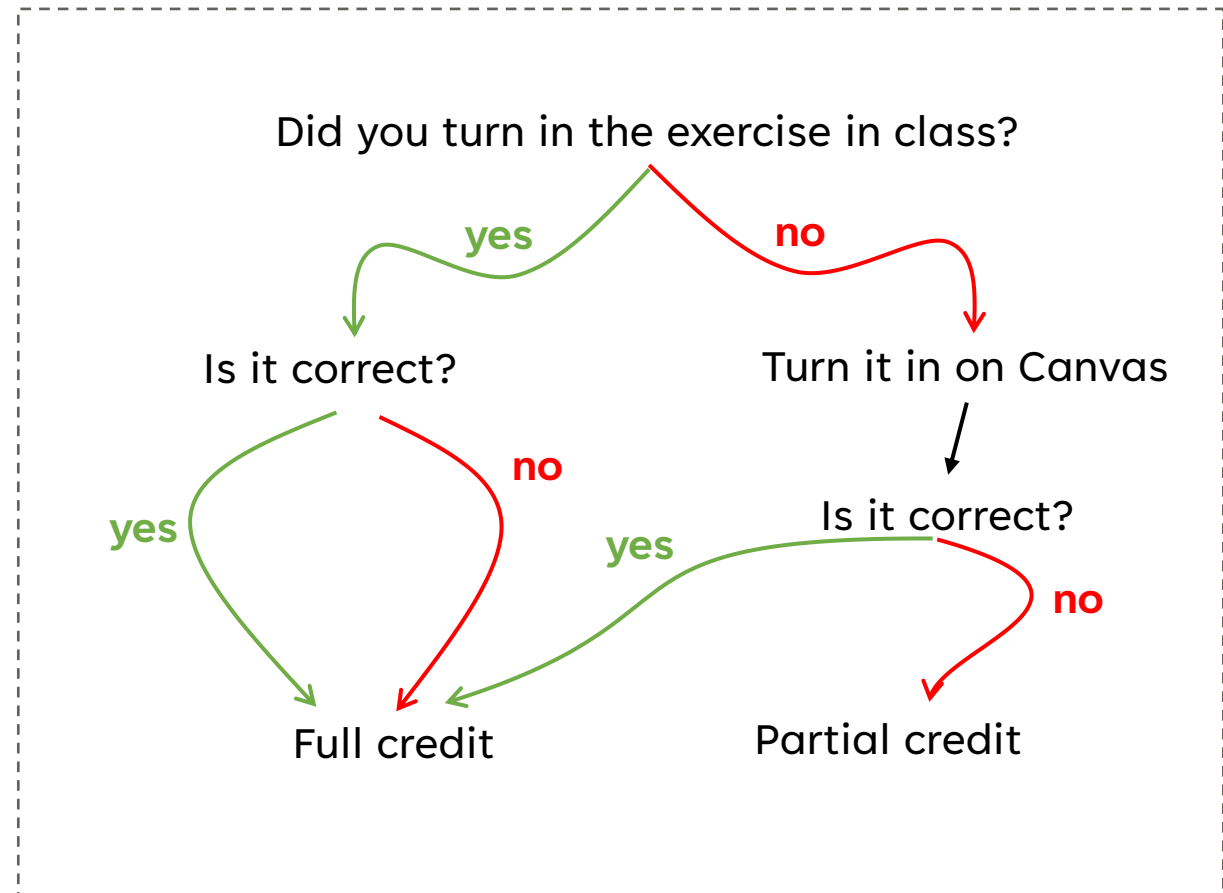
EXPECTATIONS OF YOU

ABOUT YOU

Attendance

- My assumption is that you will engage with this class
- Your attendance is rewarded, but not required

Exercises Decision Flowchart



EXPECTATIONS OF YOU

ABOUT YOU

Administrivia

- Class website: <https://analysis.cool>

You're expected to read the website

- Piazza (link in syllabus and on website)

You're expected to read Piazza

- Canvas

*You're expected to turn in assignments
through canvas*

EXPECTATIONS OF YOU

ABOUT YOU

Depends somewhat on the course you're in

- *EECS 677 vs EECS 777*

EXPECTATIONS OF YOU

ABOUT YOU

Formative vs Summative Assessment

Formative vs Summative



When the chef
tastes the food



When the customer
tastes the food

Sometimes I ask you to do something to **show you how to** do it
Sometimes I ask you to do something to **prove you can** do it

TODAY'S ROADMAP

Orientation

- About me
- About you
- About the course

Evaluating Evaluation



THIS COURSE IS BUILT FOR YOU!

ABOUT YOU

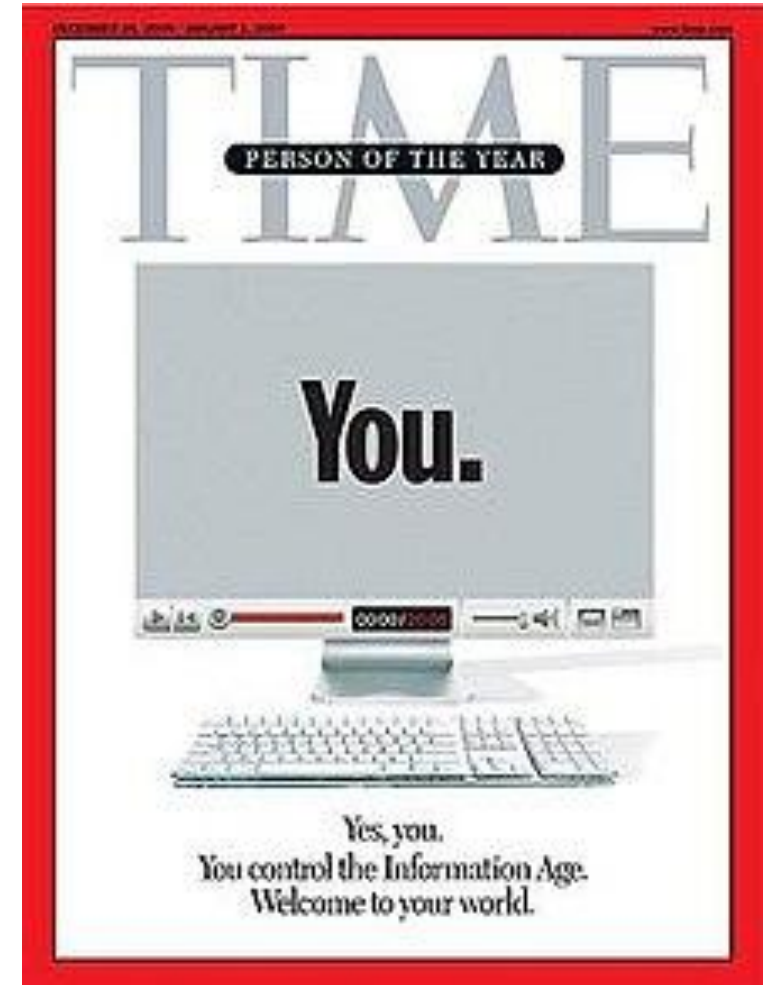
My effort is only as valuable as the result

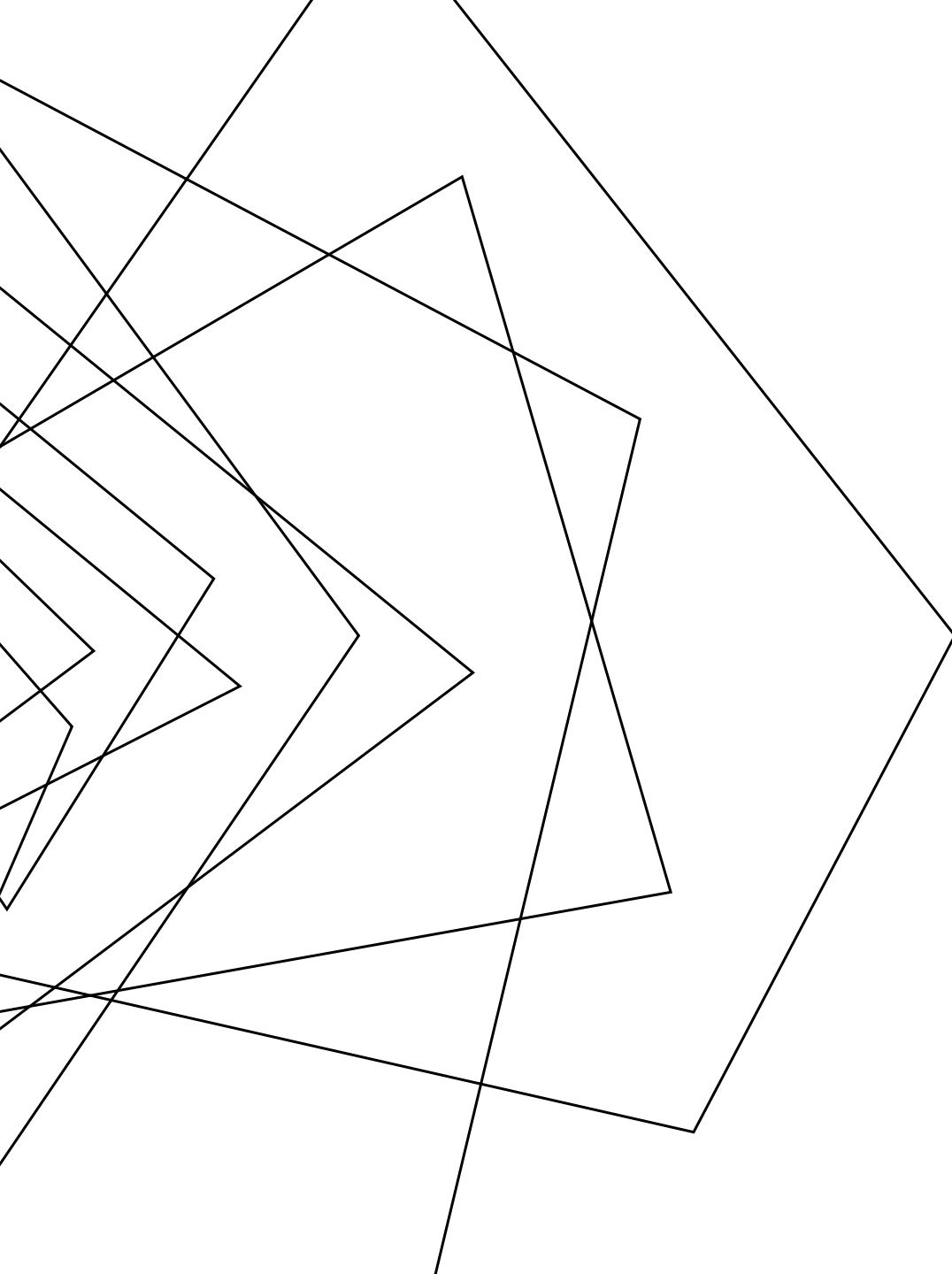
- If you're having trouble, let me know!

I value feedback

- This course improves by matching your needs

- I encourage questions, comments, etc.
(within reason)





COURSE TOPIC

TOOLS AND TECHNIQUES TO EVALUATE
THE SECURITY POSTURE OF SOFTWARE
AND WRITE MORE SECURE CODE

COURSE PERSPECTIVE

ABOUT THE COURSE

Security flaws are design flaws

- Limitations of the toolset / misuse of the toolset
- How do we evaluate and prevent issues?



COURSE PERSPECTIVE

ABOUT THE COURSE

Security flaws are design flaws

- Limitations of the toolset / misuse of the toolset
- How do we evaluate and prevent issues?



BASIC TOPIC BREAKDOWN

ABOUT THE COURSE

Secure Software Engineering

Analysis Techniques

Analysis Tools

**Break it
down!**

TODAY'S ROADMAP

Orientation

- About me
- About you
- About the course

Evaluating Evaluation



ANALYZING SOFTWARE

EVALUATING EVALUATION

How the heck do we tell what software is doing?

“Simpler question: how the heck do we tell what software *that we write* is doing?

One answer: just be really, really careful when you write your code so you don't make any mistakes

Historically insufficient answer

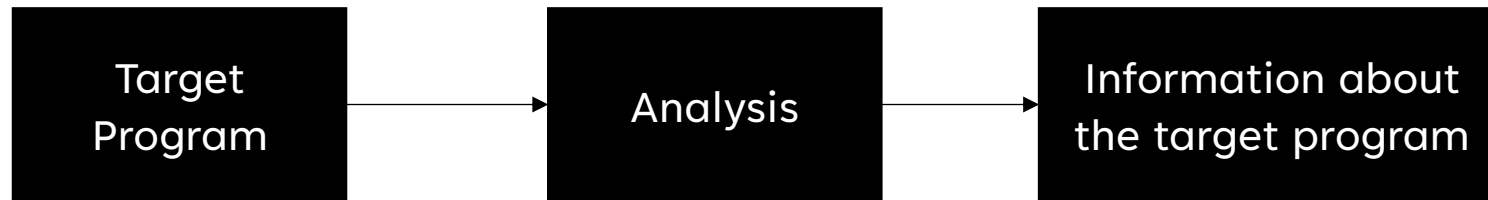


Software, basically

PROGRAM UNDERSTANDING

EVALUATING EVALUATION

A major focus of this class is on treating programs as the target of an analysis



- We'll be quite generous in our notion of what an analysis is
- Nevertheless, some details need to be considered...

LOTS OF OTHER PROBLEMS

EVALUATING EVALUATION

How do we describe programs at all (the source code is a specification after all)

Perhaps we simply detect the presence/absence of a particular set of behaviors

“Does this program send personal data to the network?”

“Does this program allow a user to inject code and run it?”

How do we actually detect the presence/absence of a program property?

Not immediately obvious, with some very disheartening realities!

FORMS OF ANALYSIS

EVALUATING EVALUATION

Static analysis

Analysis that does not run the program

Dynamic Analysis

Analysis that does run the program

TESTING AS ANALYSIS

EVALUATING EVALUATION

Most familiar form of program analysis:

Observation

Determine what is “supposed” to happen under some circumstance

Create an input specification and output specification

Run the program on the input specification, check against the output specification

Really good at proving the presence of some behavior!

Really easy to get started!

Really bad at proving the absence of a behavior!

LECTURE END

[] Fill out the course entry survey

<https://analysis.cool/survey>

[] Read the syllabus

https://analysis.cool/677_syllabus.pdf

or

https://analysis.cool/777_syllabus.pdf

[] Sign up for Piazza

