ADVANCED TOPICS IN MALWARE ANALYSIS

PROF. BRENDAN SALTAFORMAGGIO

SCHOOL OF SCP, ECE, CS

CREATING THE NEXT®

PLEASE CONSIDER THE ENVIRONMENT, AVOID PRINTING SLIDES!

INSTRUCTOR

- Professor Brendan Saltaformaggio
  - “Salt” – “uh” – “for” – “mah” – “gee” – “oh”
  - Informally: “Professor Brendan” is fine too ☺

  - Assistant Professor, SCP and ECE and CS
  - Director, Cyber Forensics Innovation Laboratory (CyFI Lab)
  - Research Interests:
    - Cyber Forensics & Computer Systems Security
    - Binary Analysis & Instrumentation
    - Vetting Of Untrusted Software
    - Memory Image Forensics
    - Mobile/IoT Security
  - **brendan@ece.gatech.edu**
  - http://saltaformaggio.ece.gatech.edu
  - Office Hours: Tues. and Thur. 6:15 pm to 7:00 pm in CODA E1068B (or on the walk over), or any time by appointment

COURSE INFO

Course Website:

- https://saltaformaggio.ece.gatech.edu/teaching/fall2023/adv-topics-mlwr/
- General Course Info, Schedule, Syllabus

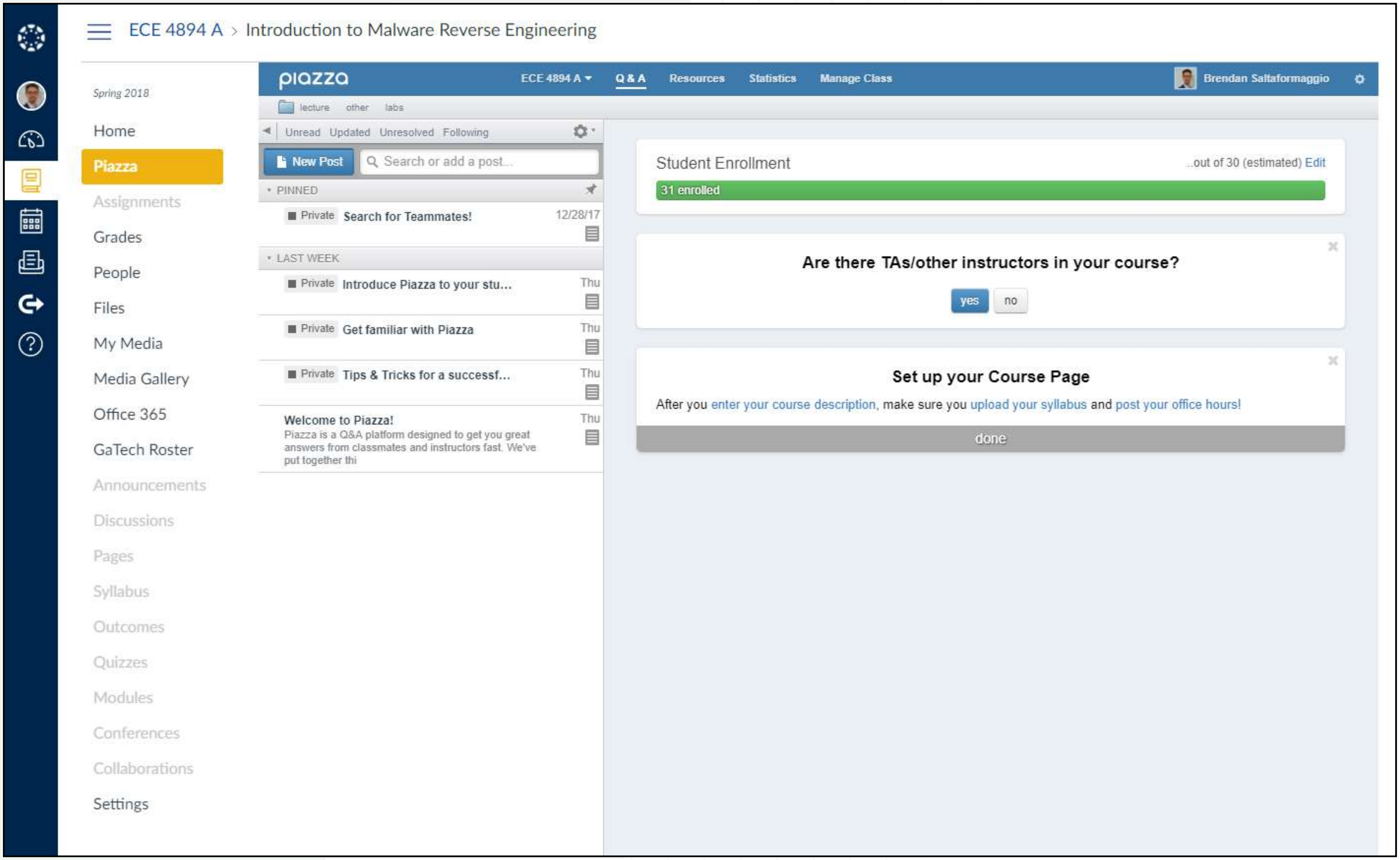
Canvas:

- https://canvas.gatech.edu
- Lecture Slides, Assignments, Grades
- I will post each new set of lecture slides a few days before we start them in class

Piazza:

- Link In Canvas
- Announcements, Discussion & Questions

PIAZZA IN CANVAS



ECE 4894 A > Introduction to Malware Reverse Engineering

PINNED

Private Search for Teammates! 12/28/17

LAST WEEK

Private Introduce Piazza to your stu... Thu

Private Get familiar with Piazza Thu

Private Tips & Tricks for a successf... Thu

Welcome to Piazza! Thu
Piazza is a Q&A platform designed to get you great answers from classmates and instructors fast. We've put together thi

Student Enrollment ..out of 30 (estimated) Edit

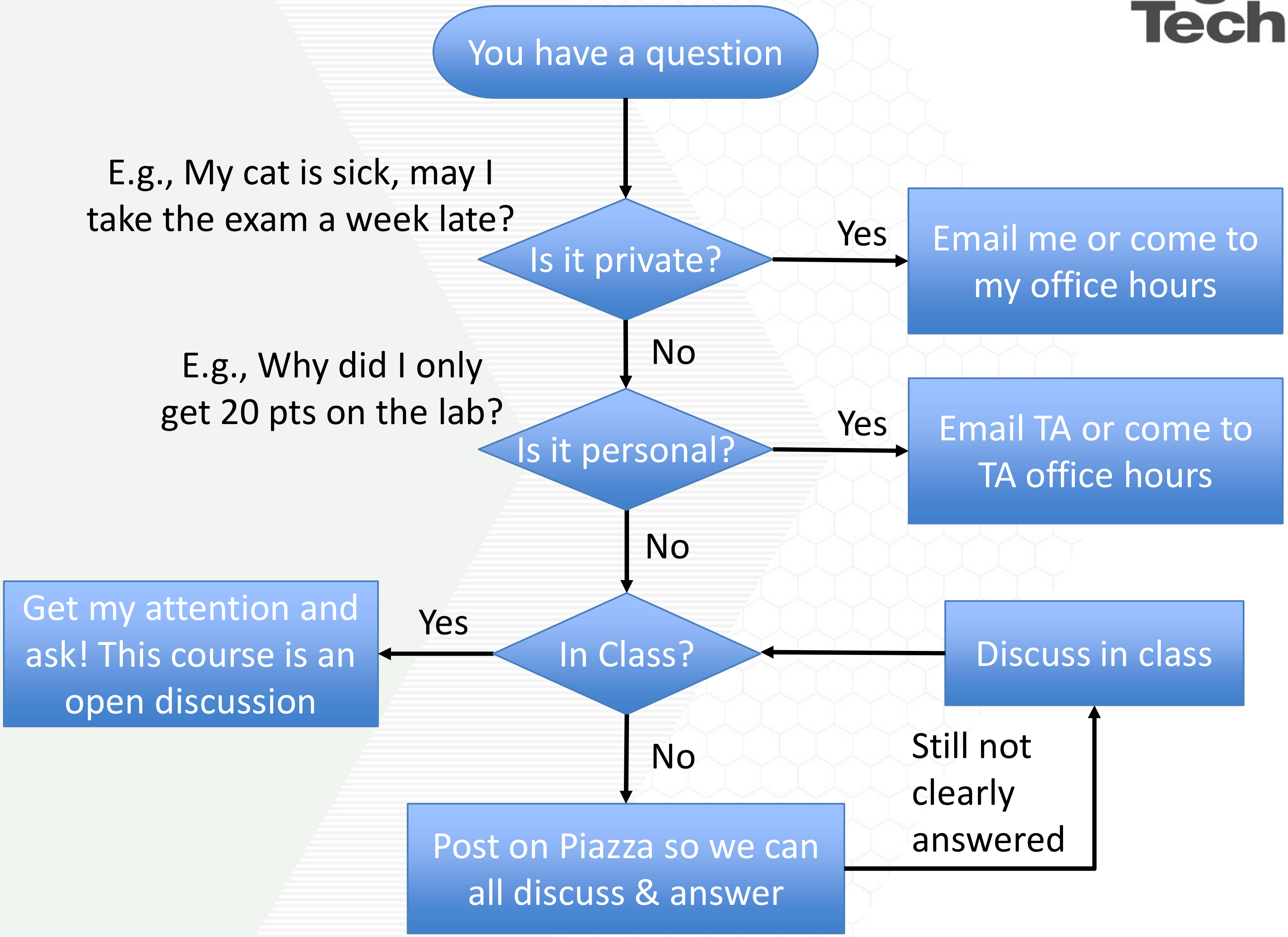
31 enrolled

Are there TAs/other instructors in your course?

Set up your Course Page

After you enter your course description, make sure you upload your syllabus and post your office hours!

CHAIN OF COMMAND



You have a question

E.g., My cat is sick, may I take the exam a week late?

Is it private?

Yes

Email me or come to my office hours

No

E.g., Why did I only get 20 pts on the lab?

Is it personal?

Yes

Email TA or come to TA office hours

No

In Class?

Yes

Get my attention and ask! This course is an open discussion

No

Post on Piazza so we can all discuss & answer

Still not clearly answered

Discuss in class

THIS COURSE IN ONE SLIDE

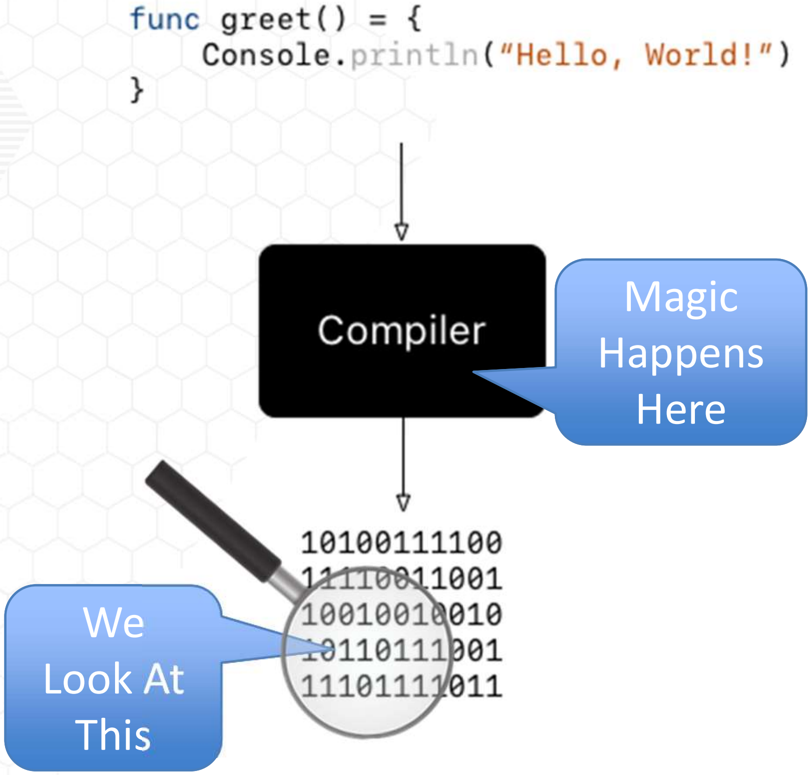
Advanced approaches for detecting vulnerabilities/malware within binary software

Software security is a rapidly changing field!

- NO textbook can keep up
- Instead, we will study published papers from top academic venues

There are a few principle techniques for software analysis

- We will cover these “building-blocks” in the lecture
- You will apply this knowledge in mini-projects



```
func greet() = {
    Console.println(“Hello, World!”)
}
```

```
10100111100
11110011001
10010010010
10110111001
11101111011
```

WARNING!

- This is a **research-focused** course! This is **not** a “requirement-filler”!
- You will be reading **many** research papers and proposing **new** research ideas!

- This course will require a significant amount of work!
  - To prepare you for high-quality PhD-level research in this field
- If you do not **LOVE** malware analysis and software security, it will be very hard!
  - Lots and lots of assembly language and C; You can try to learn assembly as we go

- There was a waitlist to join this course! So I expect you to earn your spot!

TESTIMONIALS

- “The class doesn't aim to mollycoddle you, and I appreciated that. It encouraged you to aspire for more and push your limits. Only in that extreme can one learn so much so well. “
- “The labs were long, and incredibly time consuming, but nothing we weren't fairly warned about. ”
- “One of the most rewarding and challenging courses I have taken at Georgia Tech.”
- “The amount of sleep I lost over this class was enormous, but we were warned so I can't complain about it. This course was great.”
- “Professor Brendan is a boss.”
- “Great professor great course Would malware again.”

COURSE AGENDA

Georgia Tech

The course will be divided into 2 modules:

The first 7 weeks:

- Binary program analysis principles (building blocks of this research field)
- Traditional lecture format
- You will complete 6 binary program analysis projects out of class
  - 4 will be static analysis with IDA Pro
  - https://www.hex-rays.com/products/ida/index.shtml
  - 2 will be dynamic analysis with Pin
  - https://software.intel.com/en-us/articles/pin-a-dynamic-binary-instrumentation-tool
  - Each project will require careful time allocation to complete on time!!
    - 1 or 2 week deadlines

The remainder of the course:

- How to conduct cutting-edge research in software security and cyber forensics
- Study published research papers
  - We (including myself) will take turns presenting these research papers during class
  - Presentations do not need to be great, simply convey the techniques and novelty to the class
- Large research project to identify and solve an open problem in these areas
  - The best among these will likely lead to publications (I will help this happen)
  - Team projects are great!
  - 1 Proposal presentation, 1 Results presentation
  - More on this later in the semester

CREATING THE NEXT®

GRADING

- Grades will be posted on Canvas
- 60% for the 6 mini-projects (10% each)
  - Grade based on the results produced by your tool
  - For some mini-projects, we will schedule demos during office hours
- 30% for the large research project
  - Grade based on **your understanding of the problem** --- not the success of your prototype
  - Large team projects should be larger in scope
- 10% for paper presentations & class participation

- No Midterm
- No Final Exam - You (your team) will submit a final report on your large research project

- Small extra credit assignments are likely to be announced in class

ZERO-TOLERANCE CHEATING

- Mini-projects are individual or teams of 2
  - Please discuss ideas with other students/teams
  - DO NOT share code (that includes comments in code!)

- I reserve the right to use MOSS to detect cases of substantial overlap
  - http://theory.stanford.edu/~aiken/moss/

- Zero tolerance towards violation of the GT honor code
  - http://www.honor.gatech.edu/

- If you are caught cheating:
  Zero on lab assignment + One grade drop + Report to dean (academic warning in file)

OUR GOALS FOR THIS SEMESTER

- Learn and apply the fundamental principles of dissecting malware, vulnerability finding/defense, and cyber attack triage
- Become aware of limitations of existing defense mechanisms and how to avoid them
- Read cutting-edge research publications on these topics
- Engage in critical discussion around key research topics in software security and forensics
- Propose solutions to open-ended research problems
  - Projects which align with your thesis research are encouraged as long as it still has an interesting security/forensics component
  - There is ample scope to publish in this area: If the results from your course project look promising, we can write a paper on it and I will fund your travel to go present it

PROGRAMMING REQUIREMENTS

- This course requires heavy programming
  - It is a 3-credit course but can feel like a 4-5 credit course
  - I said this before: Each project will require careful time allocation to complete on time!
- You MUST be proficient in C
  - You will be happier if you know some python and Assembler
    - It is ok if you do not
    - Everyone will be masters of them after this course …
- For the large semester project, you can use any language, system, thing you want
  - Must make a slide show ☺

PAPER PRESENTATIONS

- This is a research-focused course & you will have to conduct a research project
- You cannot do cutting-edge research without knowing where the edge is!

- To get on the cutting-edge, you must keep up with published papers
- Everyone (including me) must give paper presentations

- I expect **everyone** to read **every** paper
- 10% of your grade is based on class participation
- Class participation = discussing and proposing extensions to the papers in class & on Ed Discussion

SIGN UP FOR PAPER PRESENTATIONS ASAP!

https://docs.google.com/spreadsheets/d/1YRGkFEYmcD7e54QqInpN5cXkc1PCHdNGxNhKF8QJMR0/edit?usp=sharing

- The link to the spreadsheet is posted in Canvas
- The first presentation is next class!
- Read the instructions in the spreadsheet before signing up!
- At this time, please sign up for 1 time slot
- After everyone has signed up for one, we will start over and everyone will do a second presentation

PAPER PRESENTATIONS

- Each presentation should be ~15 minutes with 5 minutes for open discussion

- Your paper presentation must cover the following:
  1. The Problem
  2. Previous Solutions/Techniques
  3. Novel Solution Presented In This Paper
  4. Limitations Of Their Approach
  5. Future Research Opportunities

SEMESTER PROJECT

- You will have to propose & conduct a research project
- *There is ample scope to publish in this area*: If your project looks promising, we can write a paper on it and I will fund your travel to go present it

- Deadline for Team Project Proposal Approval
  - Discuss with me or the TA when your team has a project idea in mind
  - DO NOT start working on a project idea until it is approved by myself or the TA
  - I may have a few “kickstarter” ideas ;)

- Must give the TA or myself a mid-project update during office hours!
  - Deadline for Team Project Update
  - No mid-project update = 0 on the project!

- In Class Presentations at the end of the Semester
  - (See the Paper Presentation Sign Up Sheet)

QUESTIONS?

CREATING THE NEXT®