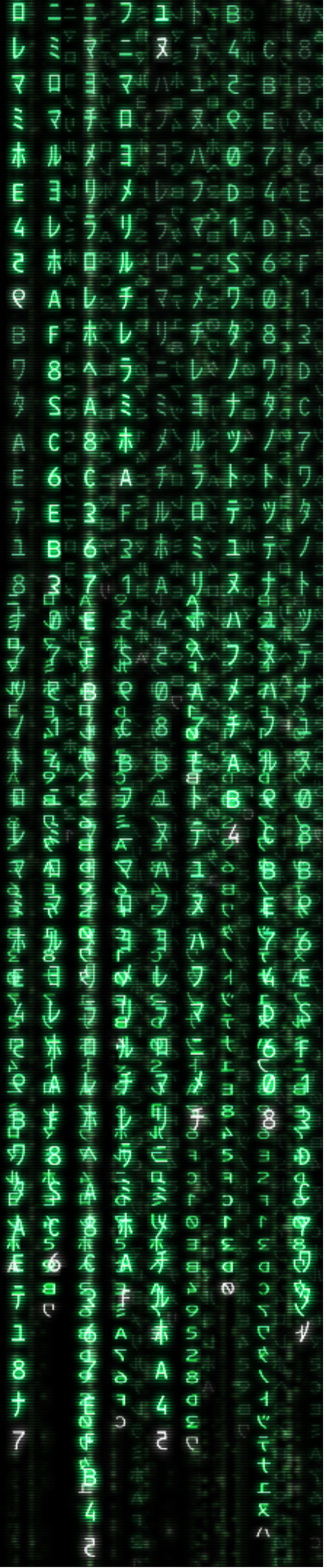


CSCI 8260 – Spring 2016

Computer Network Attacks and Defenses

Syllabus

Prof. Roberto Perdisci
perdisci@cs.uga.edu

Who is this course for?

- Open to graduate students only
- Students who complete this course successfully will receive 8000-level credit (4 credit hours)
- This is an advanced, research-oriented course
- Prerequisites
  - Operating Systems
  - Computer Networks
  - Programming (e.g., C/C++, Java, Python)
  - Basics of Computer Security + Crypto will help!

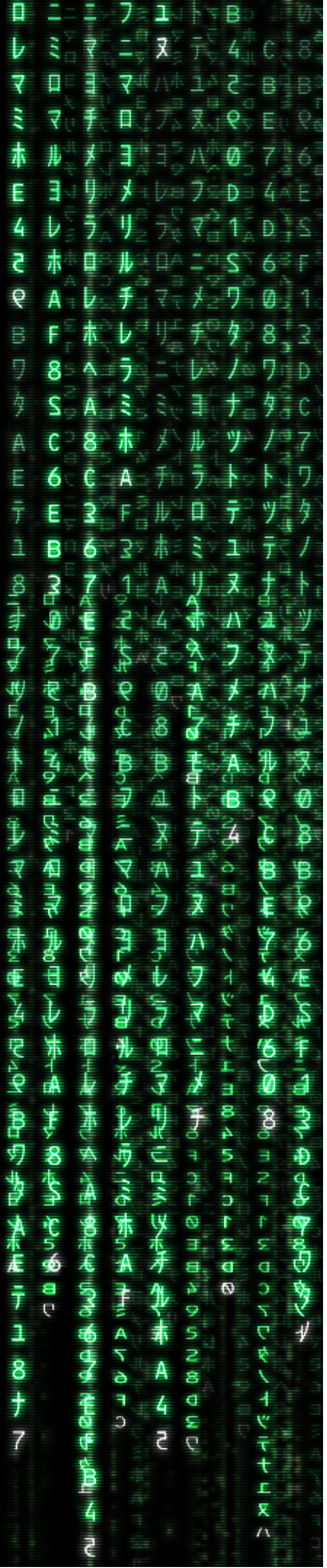
Goals of this course

- Analyze computer security systems
- Learn to identify vulnerabilities

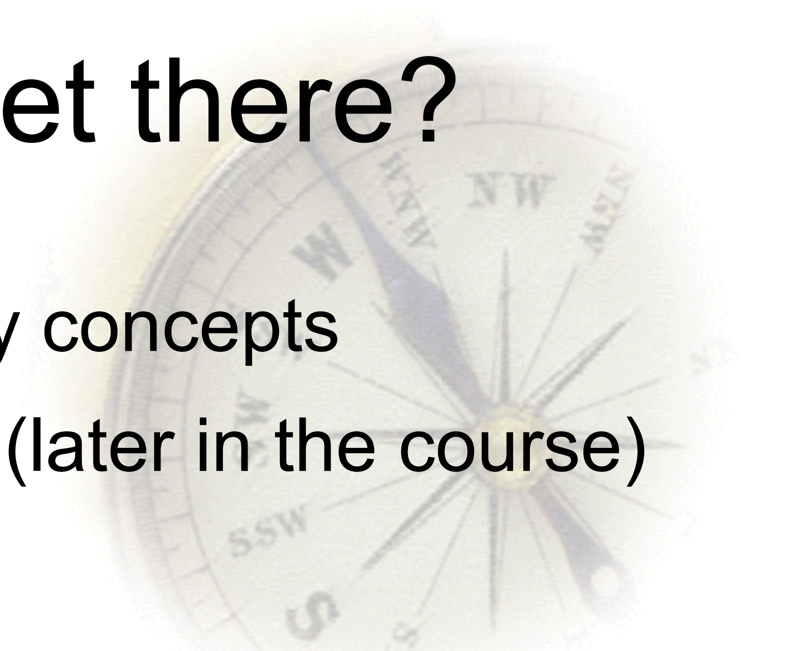
- Analyze recent attacks
- Learn to design better defenses

- Find and address open research problems

- Learn to read, analyze, and write academic papers



How will we get there?



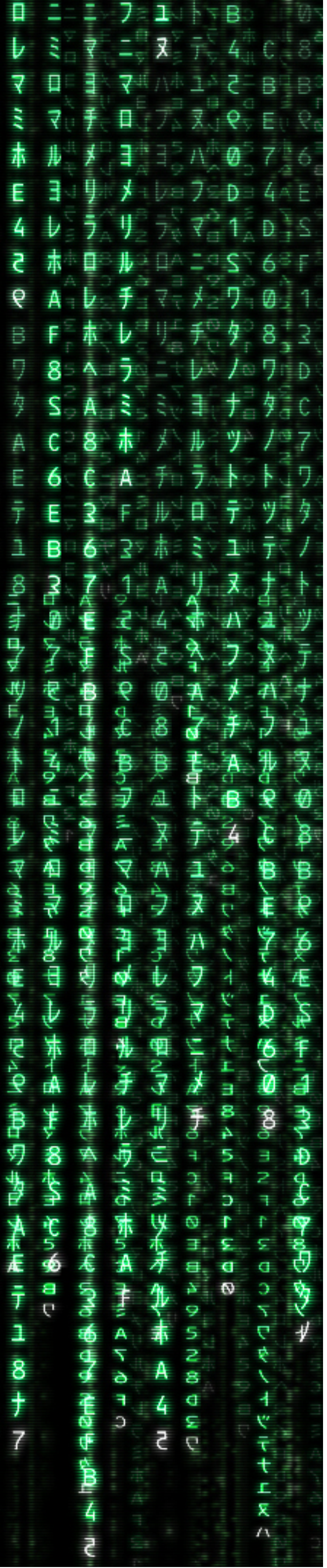
- Brief introduction to security concepts
- Quick intro to ML concepts (later in the course)
- Seminar-style lectures
- We'll read papers (mainly) from top security and systems conferences
  - IEEE S&P, USENIX Security, ACM CCS, NDSS, SIGCOMM, NSDI, etc...
- Papers will be assigned in advance
- Students are responsible for
  - Presenting one or more papers during the semester
  - Writing short reviews for some of the papers
  - Reading all assigned papers!

Topics

- Malware: analysis, packing/obfuscation, detection, behavioral clustering
- Worms: propagation and mitigation
- Botnets: measurement and detection
- Spam: content analysis, network-level spammer behavior
- Vulnerabilities: Buffer-overflows, *return-oriented* programming
- IDS: Anomaly detectors, evasion attacks

Topics

- Web Security: browser-side and server-side vulnerabilities
- Privacy: de-anonymizing data, self-destructive data
- DNS security: poisoning attacks, domain reputation and blacklisting
- Physical security: hardware-assisted security primitives, audio-visual attacks

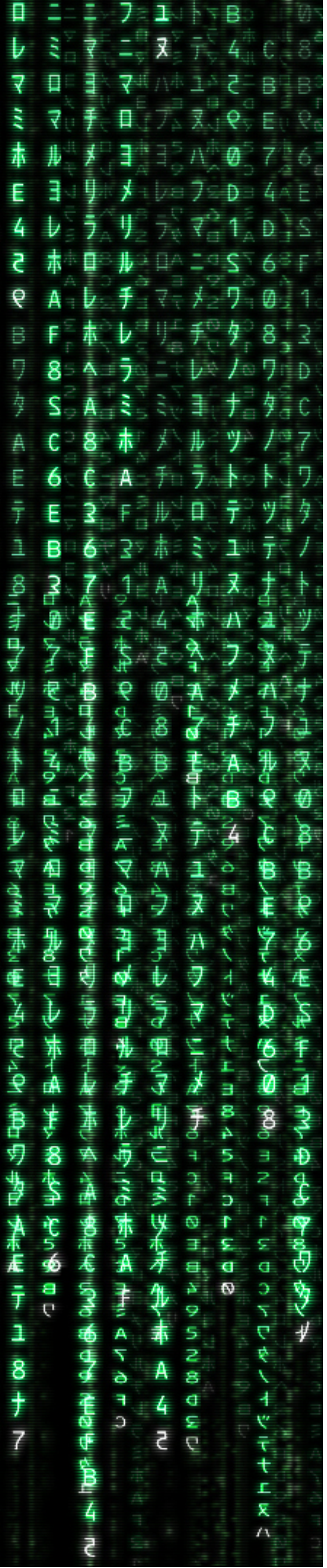


Grading

- 10% Class Participation
- 15% Paper Reviews
- 35% Paper Presentations
- 40% Research Project

Class Participation (10%)

- We will discuss one paper per lecture (refer to course schedule)
- You will need to **read all papers**, unless I indicated a paper is "optional"
- Reading the papers is fundamental to be able to actively participate to discussions during class



Paper Reviews (15%)

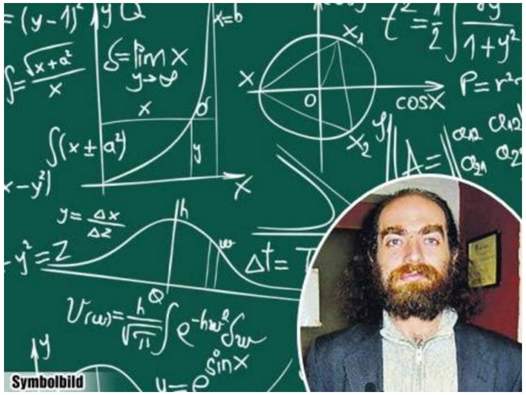
- You are responsible to write a short peer-style review for some of the papers (one paper per week, in average)
- I will indicate what papers you need to review
- Reviews need to be short (max 1 or 2 pages) and yet meaningful
  - What is the paper about?
  - What are the main contributions?
  - Are the contributions novel or incremental?
  - Is the paper technically correct
  - Is the experimental setup realistic?
  - What are the main experimental results?
  - Are they over-optimistic? Are they satisfying?
  - Pros/Cons and open problems

Paper Presentations (35%)

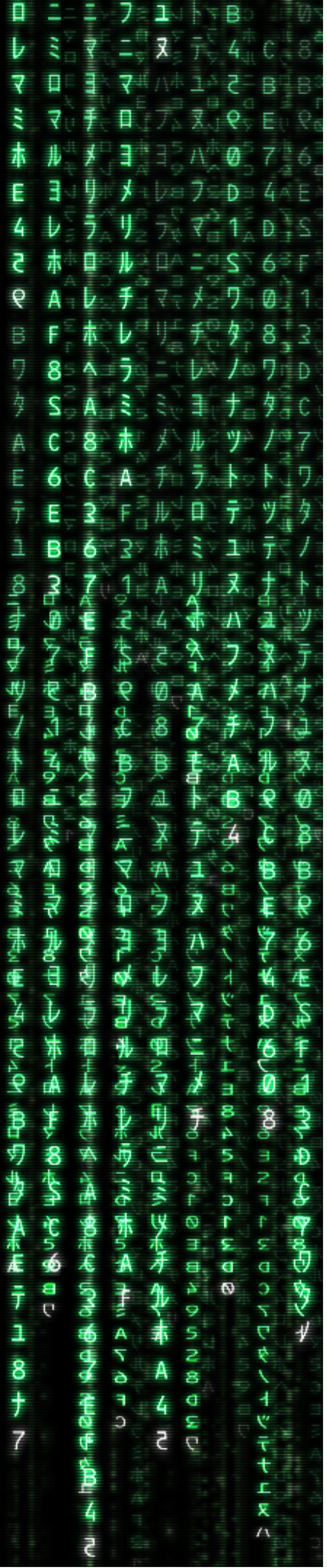
- You will be asked to present one or more papers during the semester
- Presentation guidelines
  - 40-50 min presentation + 15-20 min discussion
  - introduce the problem
  - explain motivations for the work
  - differences with previous work
  - describe approach
  - experimental setup/results
  - limitations
  - pros/cons and points for discussion

Research Project (40%)

- I will suggest possible projects, but feel free to propose your own **relevant topic**
- **Clearly state**
  - motivation, approach, results



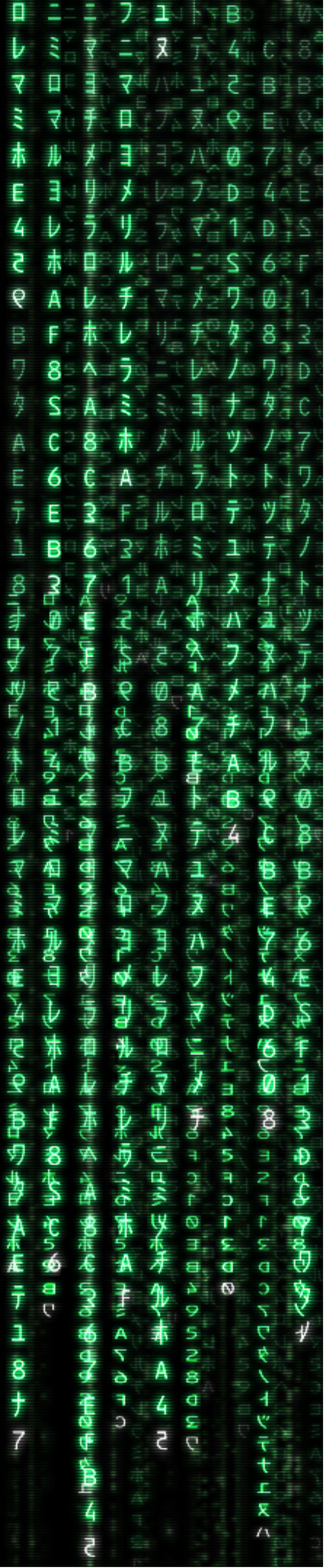
- Choose early!
- Be realistic!
  - Don't try to solve a *Millennium Prize Problem* in one semester!
- I prefer simplicity+completeness to nice ideas but incomplete results
  - unless you really have a **super cool** idea that has a chance to be published in IEEE S&P!



Research Project

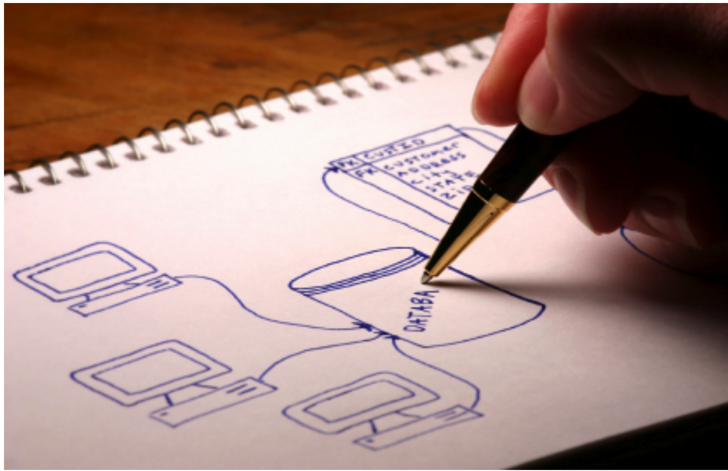
- it does not necessarily have to be related to your long-term research plans, but...
- try to find something that is close to your research area, if possible
  - You will likely enjoy it more!
  - You will probably do better!
  - e.g., if you do research in DBs, try to find something related to DB security
  - If you do research in mobile computing, choose something related to security in mobile devices
  - etc.

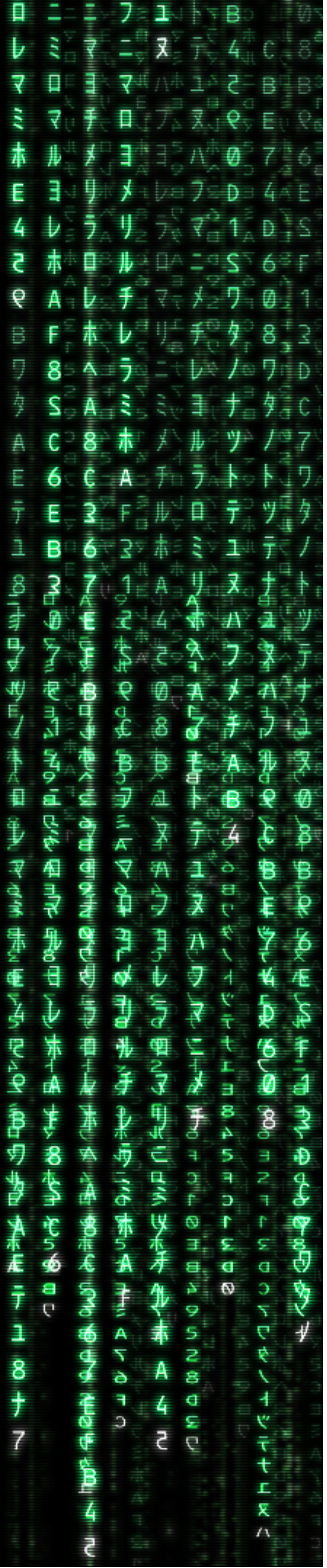
http://www.ixibo.co



Research Project

- Advice
  - read as many papers as you can on the topic you are interested in
  - make sure you are not re-inventing the wheel
  - can we overcome limitations of previous work?
  - look at the problem from a different angle
  - measurement papers are ok, in particular when you can draw unexpected or non-obvious conclusions



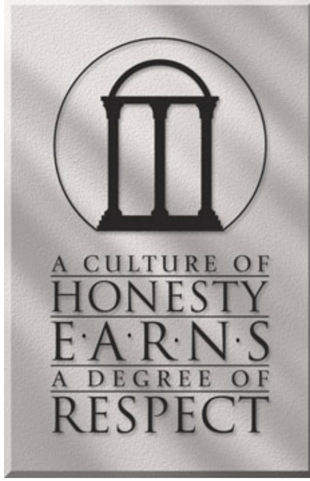


Research Project

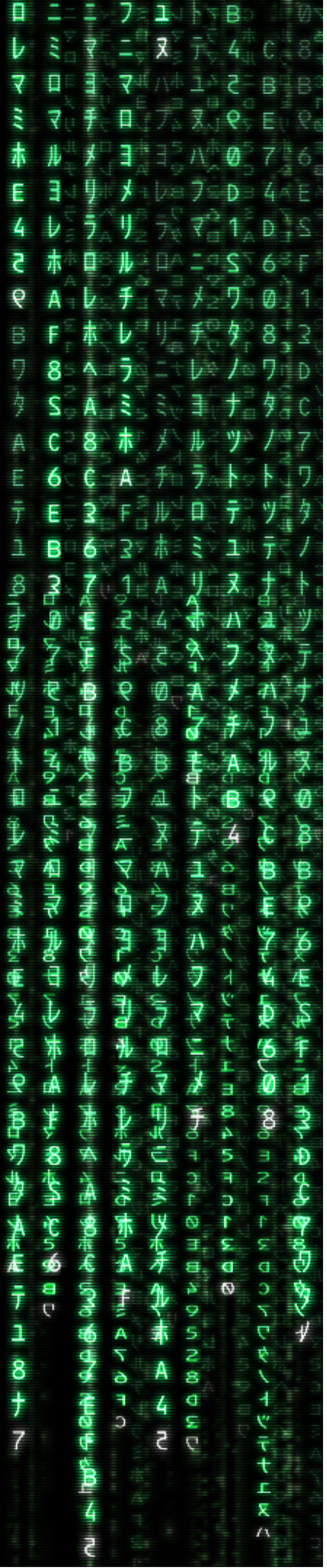
- Things to consider
  - data is fundamental!
  - what data have you got access to?
  - what data would you be able to get?
  - can you perform experiments on a meaningful amount of data?

- if you have doubts
  - talk to me...

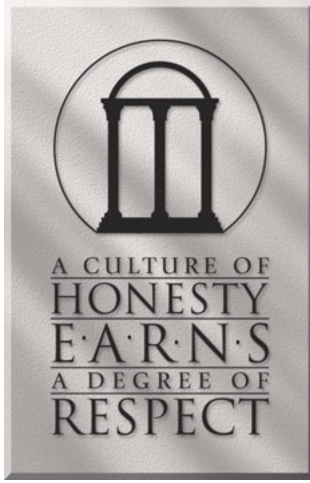
Academic Integrity



- Every student must abide by UGA's **academic honesty policy**
- Dishonest behavior including cheating, copying, or **forging experimental results** will not be tolerated!



Ethical Learning



- In this class we will learn about vulnerabilities in computer systems and attacks that may exploit them
- Such information must never be used for unethical purposes

First Assignment

- Learn LaTeX, please!

  http://en.wikibooks.org/wiki/LaTeX

  and plenty of other tutorials online...

Logistics

- Course website
  - http://www.cs.uga.edu/~perdisci/CSCI8260-S16/
  - official reference for all details regarding the course (check it regularly!)
- You can email me for questions
  - perdisci@cs.uga.edu
  - please use **[CSCI8260]** in the subject!
- If you need to talk to me
  - right after class
  - office hours (to be announced)

Next

- Introduction to Computer Security

- Brief overview of research topics in security

- Intro to ML

- Tips on how to choose a research project

- Tips on how to write a paper (maybe later in the course…)

- Start choosing what papers you would like to present (I will make a list available soon)

Before you leave...

- Questions?
- Introduce yourself and your research interests!