CSCI 6900

Computer Network Attacks and Defenses

Lecture 1: Introduction

Instructor: Prof. Roberto Perdisci

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 write academic papers

How will we get there?

- Seminar-style lectures
- We'll read papers (mainly) from top security and system conferences
  - IEEE S&P, USENIX Security, ACM CCS, NDSS, SIGCOMM, NSDI, etc...
- Papers will be assigned in advance
- Students are responsible for
  - Present one or more papers during the semester
  - Write short reviews for some of the papers
  - Read all assigned papers!

Topics

- Botnets: measurement and detection
- Worms: propagation and mitigation
- Malware: analysis, packing/obfuscation, detection, behavioral clustering
- Spam: content analysis, network-level spammer behavior

- Vulnerabilities: Buffer-overflows, *return-to-libc* attacks
- IDS: Anomaly detectors, evasion attacks

Topics

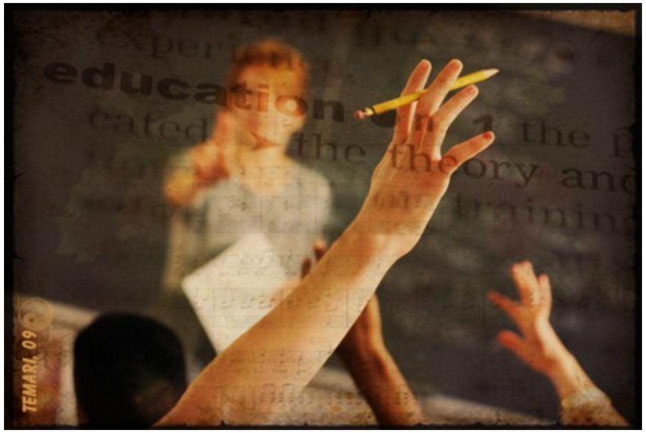
- Web Security: browser-side and server-side vulnerabilities
- Privacy: deanonymizing data, self-destructive data
- DNS security: poisoning attacks, domain reputation and blacklisting
- Physical security: cold-boot attack, audio-visual attacks

Grading

- 15% Class Participation
- 20% Paper Reviews
- 20% Paper Presentations
- 45% Research Project

Class Participation (15%)

- We will discuss one or two papers 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 (20%)

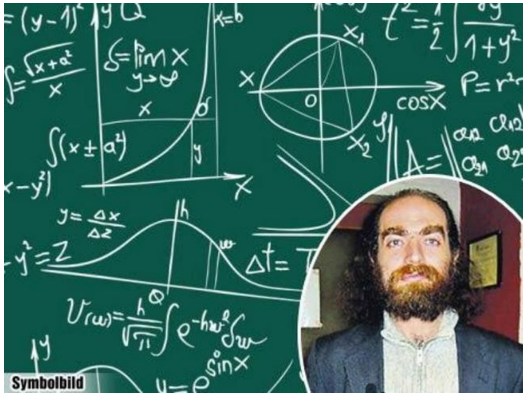
- You are responsible to write a short peer-style review for some of the papers
- I will indicate what papers you need to review
- Reviews need to be short (max 1 or 2 pages) and yet meaningful
  - What is the paper about?
  - What are the main contributions?
  - Are the contributions novel or incremental?
  - 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 (20%)

- 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
  - difference with previous work
  - describe approach
  - experimental setup/results
  - limitations
  - pros/cons and points for discussion

Research Project (45%)

- You are free to choose any **relevant** topic in computer and network security
- Conference-style paper
  - 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!

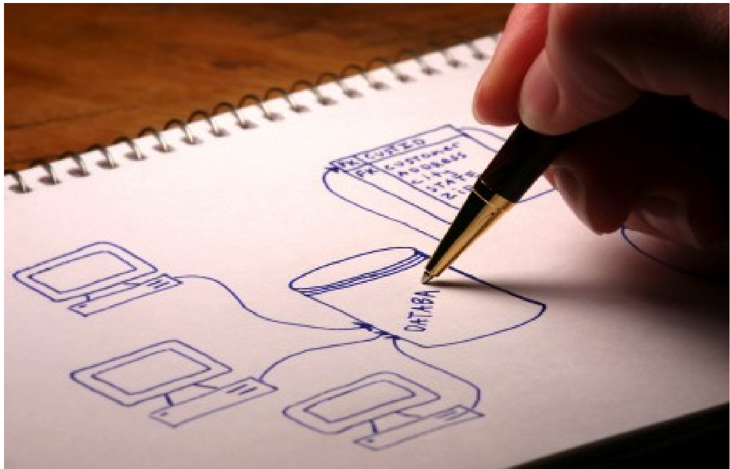
Research Project

- 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.izibo.c

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 **really** have trouble finding a suitable topic
  - talk to me...

Academic Integrity

A CULTURE OF HONESTY EARNS A DEGREE OF RESPECT

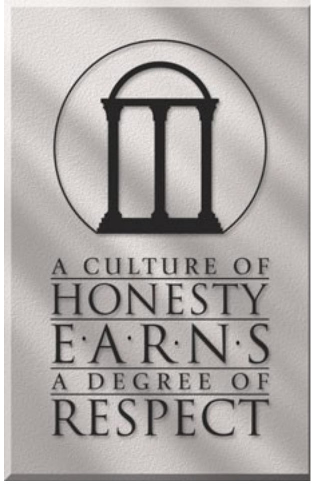
- Every student must abide by UGA's **academic honesty policy**

- Dishonest behavior including cheating, copying, or **forging experimental results** will not be tolerated!

- **Beware of the dawg,**

  he is watching you!

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

- **Beware of the dawg,**

  he is watching you!

First Assignment

- Write a summary of your research interests
  - what have you done so far?
  - what topics are you interested in for your future research?
  - why do you think those topics are relevant?
  - mention most important related work

First Assignment (cont...)

- LaTeX please!

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

  and plenty of other tutorials online...

- Deadline
  - 8/26/2010 11:59pm (hard deadline!)

$\LaTeX\,2_\varepsilon$

Logistics

- Course website
  - http://www.cs.uga.edu/~perdisci/CSCI6900-F10/
  - official reference for all details regarding the course (check it regularly!)

- You can email me for questions
  - perdisci@cs.uga.edu
  - please use **[CSCI6900]** in the subject!

- If you need to talk to me
  - right after class
  - send me an email to set up an appointment

Next Time

- Brief overview of research topics in security
- Tips on how to choose a research project
- Tips on how to write a paper (if we have time)
- Start choosing what papers you would like to present (I will make a list available tomorrow)

Before you leave...

- Questions?

- Please send me an email to introduce yourself
  - You name
  - PhD or Master's?
  - What year?
  - Your advisor (if you have one)
  - A link to a list of your publications (if any)