Announcements

• Assignment #1 due on Monday
  ▶ Submitted directly to Canvas.

• Be sure that you are registered!

• My student, Luis Vargas, will be serving as the TA for the semester.
  ▶ You will see him teach a lecture on occasion.
  ▶ His responsibilities will largely be grading assignments.
Reading papers …

- What is the purpose of reading papers?
- How do you read papers?
Understanding what you read

- Things you should be getting out of a paper
  - What is the central idea proposed/explored in the paper?
    - Abstract
    - Introduction
    - Conclusions

  These are the best areas to find an overview of the contribution

- How does this work fit into others in the area?
  - Related work - often a separate section, sometimes not, every paper should detail the relevant literature. Papers that do not do this or do a superficial job are almost sure to be bad ones.
  - An informed reader should be able to read the related work and understand the basic approaches in the area, and how they differ from the present work.
Understanding what you read

• What scientific devices are the authors using to communicate their point?

  ▷ Methodology - this is how they evaluate their solution.

  • Theoretical papers typically validate a model using mathematical arguments (e.g., proofs)

  • Experimental papers evaluate results based on test apparatus (e.g., measurements, data mining, synthetic workload simulation, trace-based simulation).

  • Empirical research evaluates by measurement.

  • Some papers have no evaluation at all, but argue the merits of the solution in prose (e.g., paper design papers)
Understanding what you read

• What do the authors claim?

  ▶ Results - statement of new scientific discovery.

  • Typically some abbreviated form of the results will be present in the abstract, introduction, and/or conclusions.

  • Note: just because a result was accepted into a conference or journal does necessarily not mean that it is true. Always be circumspect.

• What should you remember about this paper?

  ▶ Take away - what general lesson or fact should you take away from the paper:

  ▶ Note that really good papers will have take-aways that are more general than the paper topic.
Summarize Thompson Article

• Contribution
• Motivation
• Related work
• Methodology
• Results
• Take away
Reading a paper

• Everyone has a different way of reading a paper.

• Here are some guidelines I use:

  ➤ Always have a copy to mark-up. Your margin notes will serve as invaluable sign-posts when you come back to the paper (e.g., “here is the experimental setup” or “main result described here”)

  ➤ After reading, write a summary of the paper containing answers to the questions in the preceding slides. If you can’t answer (at least at a high level) these questions without referring to the paper, it may be worth scanning again.

• Over the semester, try different strategies for reading papers (e.g., Honeyman approach) and see which one is the most effective for you.
Reading a systems security paper

- What is the security model?
  - Who are the participants and adversaries
  - What are the assumptions of trust (trust model)
  - What are the relevant risks/threats

- What are the constraints?
  - What are the practical limitations of the environment
  - To what degree are the participants available

- What is the solution?
  - How are the threats reasonably addressed
  - How do they evaluate the solution

- What is the take away?
  - key idea/design, e.g., generalization (not solely engineering)

- Hint: I will ask these questions when evaluating course project.
Course Project

• The course project requires the student execute some limited research in security.
  – Demonstrate applied knowledge
  – Don’t try to learn some new non-security field
  – Be realistic about what can be accomplished in a single semester.
  – However, the work should reflect real thought and effort.

• The grade will be based on the following factors: novelty, depth, correctness, clarity of presentation, and effort.
Deliverables

• The chief product of the project will be a full size poster detailing your work. There will be several milestones:

  ▶ Project Choice
  ▶ Background and Related Work
  ▶ Abstract/Intro
  ▶ Final Poster Presentation

• This is a critical factor in your grade (25%) so you better take it seriously

  ▶ E.g., an exceptionally good (or poor) project may help (kill) grade
Project Choice

- Due on September 13th, in class
- Ordered list of projects
  - Choose three projects in order of interest
- Choose up to 2 collaborators
  - Optional
  - Get a sense of groupings
- I will choose your project and group
  - Hopefully, I can resolve the constraints implied
  - One group per project
  - A functional group
Topic Examples

- Web systems
  - Evaluate the security of a Web 2.0 application
  - Design a method of authenticating content (e.g., via Firefox ext.)
- Mobile Systems
  - Reverse engineer an important class of Android apps and say something meaningful about their security. (e.g., payment system)
- User Studies
  - Measure the effectiveness of passwords, card systems
- Network security
  - Develop an anonymity system more robust than Tor.

**Note**: picking a topic is very important, and should almost certainly involve an area that you know well.
Bad Ideas

- An encryption library for SMS.
  - Done... to death...
- A password wallet.
  - See SMS Encryption...
- Firewall rule checkers
- Steganographic schemes
- Anything that requires massive amounts of data that you can’t get your hands on...
  - Online Game trends that require snapshots of all users...
Good Luck

• This class is going to test you as a student.
  ▷ There will not be time to slow down this semester.
  ▷ Be sure that you are really ready for this.

• I will require you to do more than simply regurgitate facts.
  ▷ If you can not apply what you’ve learned, defend a position and argue against another, this will not be fun.

• Take this class for the right reasons.