CSCI 667: Concepts of Computer Security

Lecture 1

Prof. Adwait Nadkarni

Fall 2024

Derived from slides by William Enck

Some bad news

We are terrible at designing secure systems.

Designing secure systems is difficult.

Fundamental asymmetry between attacker and defender

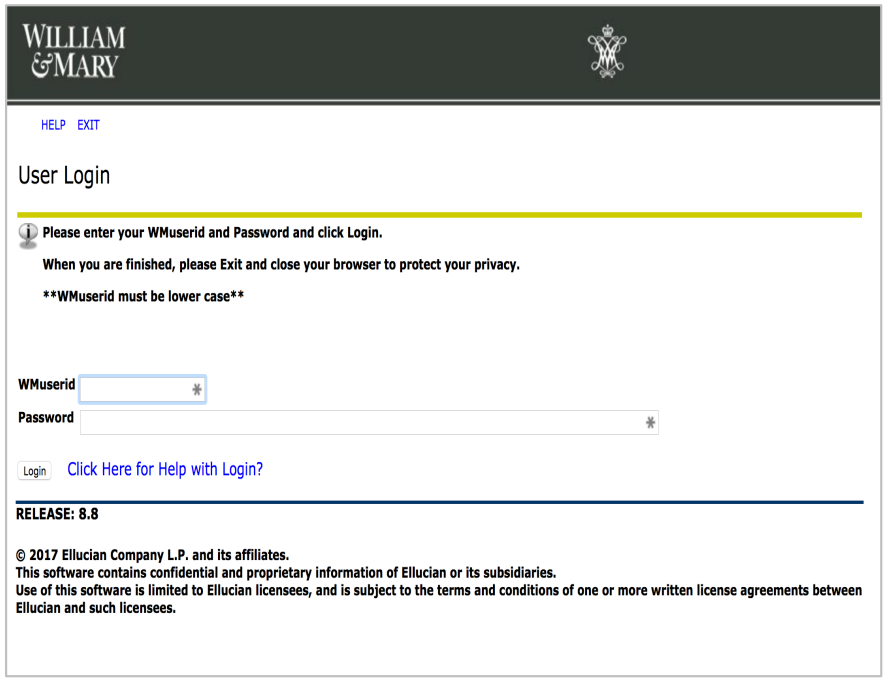
Functionality is easy to measure, but…

Airplane works

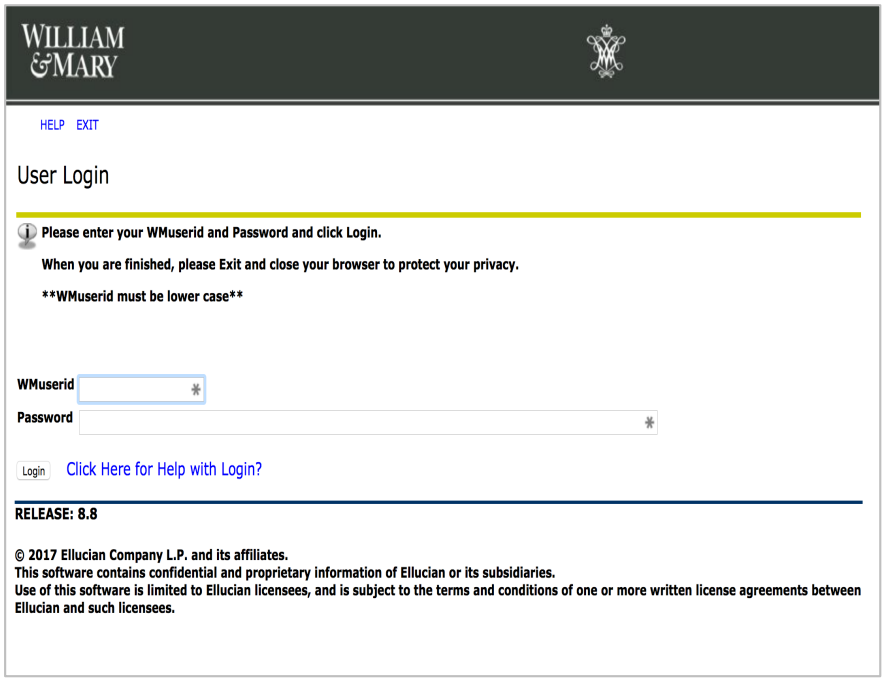
Airplane doesn't work

…*security* is almost impossible to measure

Web browser 0wned



Web browser not 0wned



Some good news

Computer security is a growth area.

Goals

- My goal: *to provide you with the tools to understand, evaluate and apply research in computer security*.
  - Basic technologies
  - Engineering/research trade-offs
  - How to read/write/present security research papers
- *This is a hard course.* The key to success is sustained effort.
  - Do the readings
  - Participate in the class
- Pay-off: security competence is a rare, valuable skill

Non Goals

- Familiarization with the latest tools
- Professional Security Certification

Course Topics

- High-level Topics:
  - Basics of crypto *(this isn't a crypto course)*
  - Host vulnerabilities
  - Host defenses
  - Network malware
  - Network defenses
  - Web security
  - IoT security
- Check the syllabus!
- **Note:** I reserve the right to adapt the syllabus throughout the semester; *I will give at least one week's notice of any changes*

Prerequisites

- No prerequisite courses, but…
  - IP Networks
  - Modern Operating Systems (Linux/UNIX)
  - Discrete Mathematics
  - Basics of systems theory and implementation
    - E.g., file systems, distributed systems, networking, operating systems, …
  - laugh at my jokes

Course policies, expectations, and other fun bureaucratic goodness

This is the most important slide in this deck!

Course Website:

https://www.adwaitnadkarni.com/teaching/csci667

- **Piazza** for discussions and announcements: https://piazza.com/wm/fall2024/csci667
- **Blackboard** for assignment submission: https://blackboard.wm.edu

Office Hours

- T/Th: 9: 20 AM – 10:50 AM
  - and by appointment

Textbook

- This course has *no required textbook*. However,
  - **Readings** from seminal papers, online book chapters, and other sources
  - Useful **online books**:
    - Security Engineering, Ross Anderson (Available online: http://www.cl.cam.ac.uk/~rja14/book.html)
    - Operating System Security, Trent Jaeger (*Available online via* https://libraries.wm.edu/)
    - Handbook of Applied Cryptography (Available online: http://cacr.uwaterloo.ca/hac/index.html)

Things that are not your readings

WIKIPEDIA
The Free Encyclopedia

Slashdot

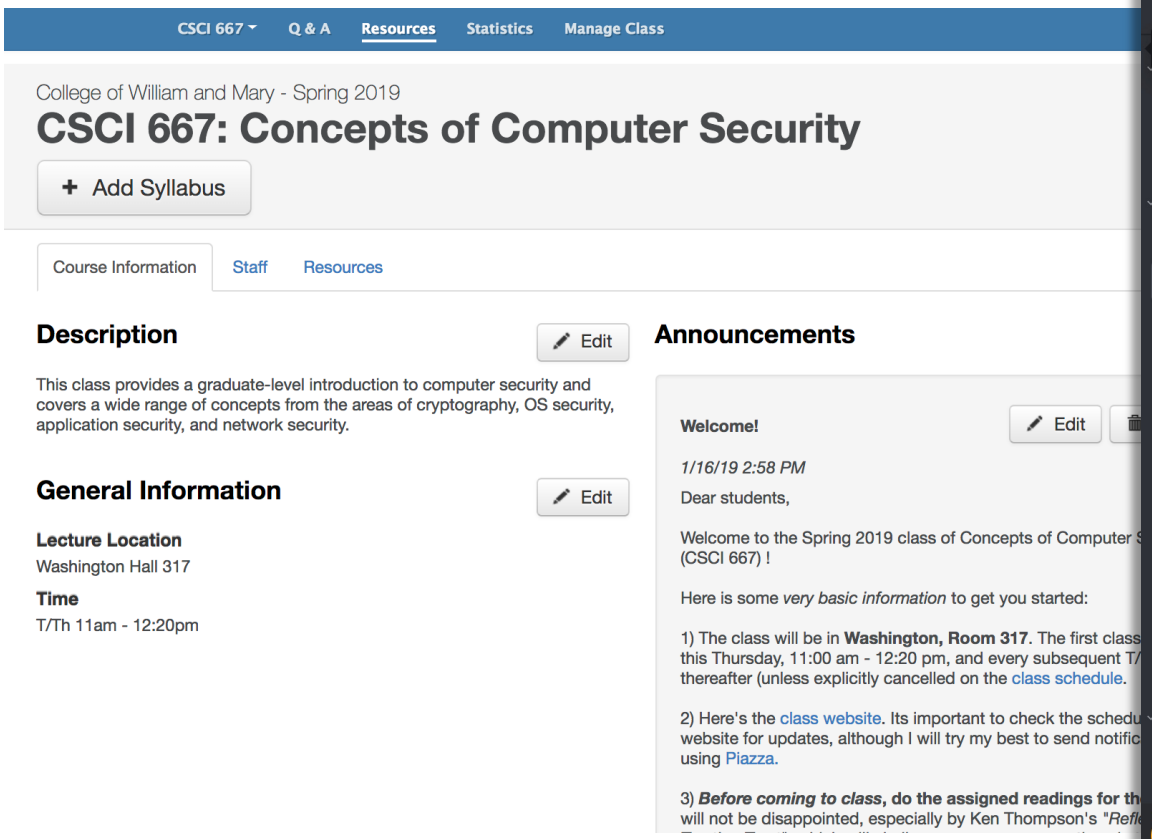
News for Nerds. Stuff that matters.

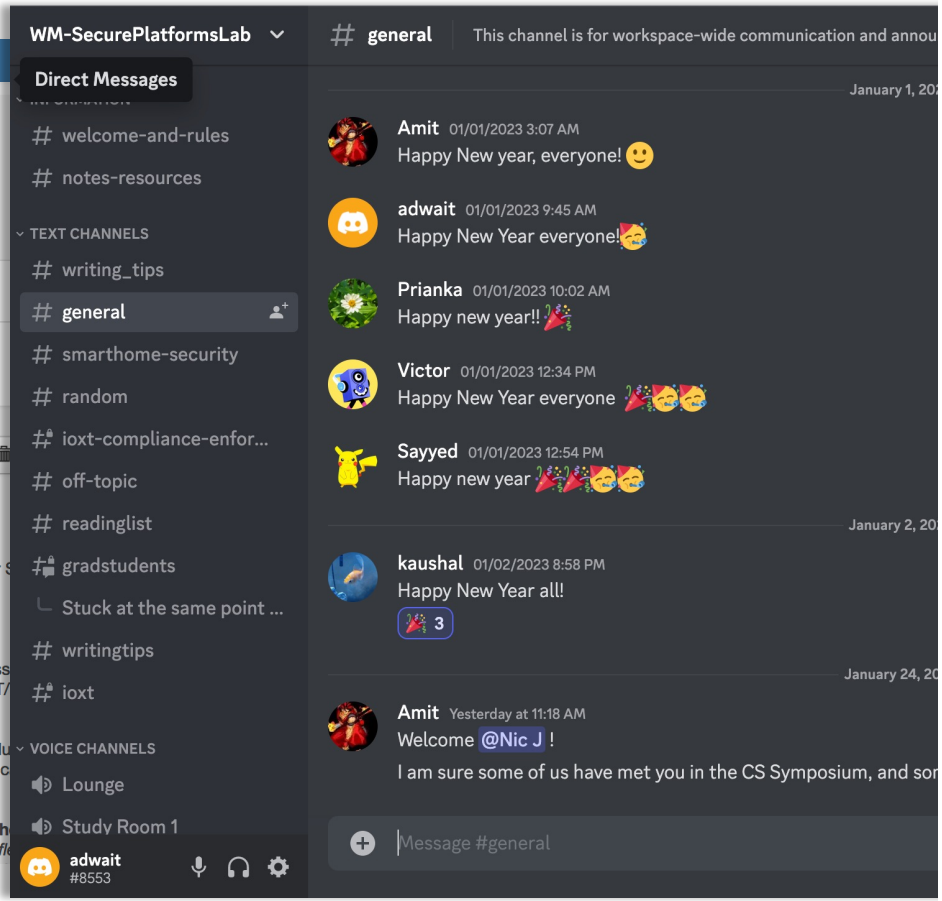
digg

engadget

Online Course Discussion

- **Extensive** class discussions and announcements via Piazza.
  - VOTE: **PIAZZA or DISCORD for discussions?**
- You are expected to read each and every posting
- You are expected to participate.

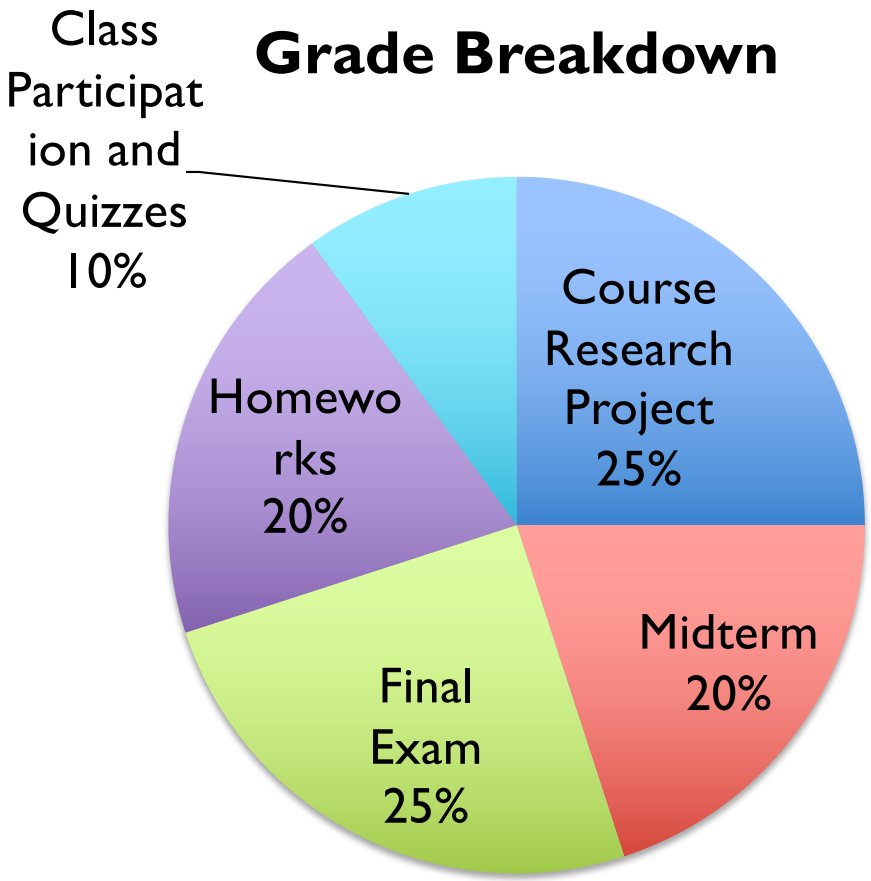




Online Course Discussion

- **Do** post to Piazza if…
  - …you have a question about the class subject matter (slides, lectures, etc.)
  - …you need a clarification on a homework
  - …you have a general question about network security
  - …you have a question regarding a class policy
- If you send any of the above to me directly, I'll ask you to post it on Piazza
- ***Don't:***
  - Give away solutions to assignments
  - Start flamewars
- *Do* be respectful of others

Grading



- Course project is a major emphasis of the class
- There are 4 homework assignments
  - *Conceptual and short: Mostly question based*
  - 25% penalty for late homeworks within 24 hrs, 100% penalty thereafter.
  - *Can discuss, provided you:*
    - *Write your own answers*
    - *Name your collaborators*
  - **Extra credit:** hw5

Course Project

- End Result: *Research* Paper (8-10 page conference-style paper)
  - Motivation for an Experiment
  - Background
  - Related Work
  - Experimental Approach
  - Experimental Evaluation
- Start with an Existing System/Approach
  - ***Break It***
- See a problem? ***Fix it***
  - Aim for a Research-Quality Result
- Have an interesting observation? ***Measure it!***
- Reproduce prior results of a category (not just *one paper*)

Project Milestones

- The course project is 25% of your grade
- Milestones (see web page for details)
  - Project Proposal – 5 points
  - Related Work – 20 points
  - Research Plan – 60 points
  - Abstract/Intro – 15 points
  - Final written paper – 100 points

Submitted together

- Unless otherwise specified, all project related assignments must be created in **LaTeX**

Exams

- Midterm and Final
- Exams
  - Conceptual Questions (Basic and Complex)
  - Constructions
  - Precise Answers

Class Participation and Quizzes

- ***Participation***
  - Start from 0/10
  - Points increase as you participate on Piazza/in-class
  - Ample opportunities to participate
- Quizzes/ ***Paper Reviews***
  - Quick quizzes on the previous lecture and readings
  - Quizzes on *readings* may require:
    - Define Concepts
    - Comparison with Other Approaches
    - Details of Approach
  - In lieu of quizzes, I may ask you to do paper reviews (*rarely)*
  - *There will be a quiz after every class if I have 10 minutes left*

Other Policies

- Please turn off cell phones during class.
- I will do my best to respond to emails within 24 hours. You will receive faster answers if you post to Piazza/Discord.
- Students may appeal to the instructor for reconsideration of a grade, but the appeal must be in writing (i.e., email), and must be sent within 3 weeks (or the close of the semester, whichever is sooner) of receiving the graded assignment.
- Behave civilly: don't be late for class; don't read newspapers/blogs/etc. during class; don't solve Sudoku puzzles during class; don't struggle with crossword puzzles during class; respect others' opinions, even if they are clearly wrong.
- Adhere to good scientific principles and practices, and uphold the W&M Student Code of Conduct.

Cheating policy

- Cheating is not allowed
- We run tools
- If you cheat, you will probably get caught
- If you get caught, you will get a
  ...ment
  ...rse (not
  ...e caught
  ...cheating)
- **I REFER ALL ACADEMIC DISHONESTY INCIDENTS TO THE OFFICE OF STUDENT CONDUCT, WITHOUT EXCEPTION**
- If you don't cheat and **work hard**, you will always do better than if you cheated

This includes the course project!

All text and figures should be your own.

Course credo:

Think like an attacker,
but behave like a responsible adult.

W&M's computer usage policies apply to this class.

Security course != permission to disrupt or cause harm

Ethics Statement

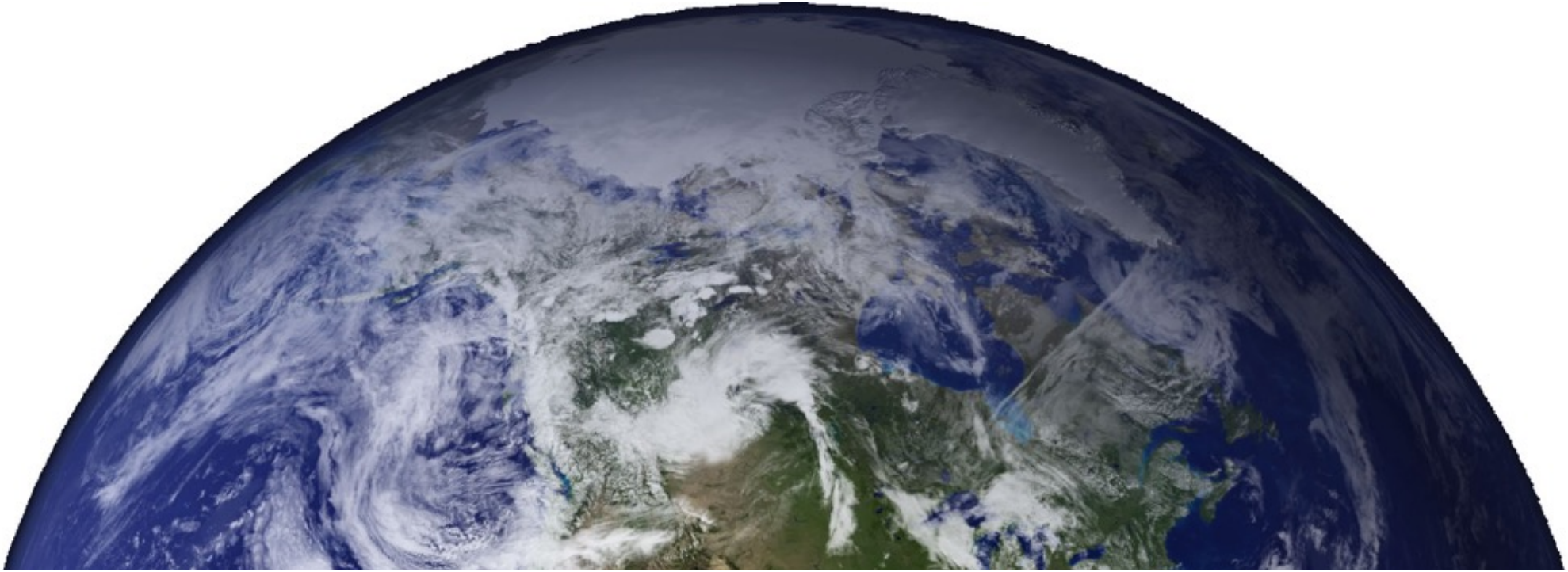
- This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class and or institution.
- When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor Nadkarni.

Readings

- There are a large amount of readings in this course covering various topics. These assignments are intended to:
  - Support the lectures in the course (provide clarity)
  - Augment the lectures and provide a broader exposure to security topics.
- Students are ***required*** to do the reading!
  - *About 10-20% of questions on the tests (and most of the quizzes) will be off the reading on topics that were not covered in class*. You better do the reading or you are going to be in deep trouble when it comes to grades.

Lecture notes

- Slides will be released on the schedule page *after each class*.
- I like trees.



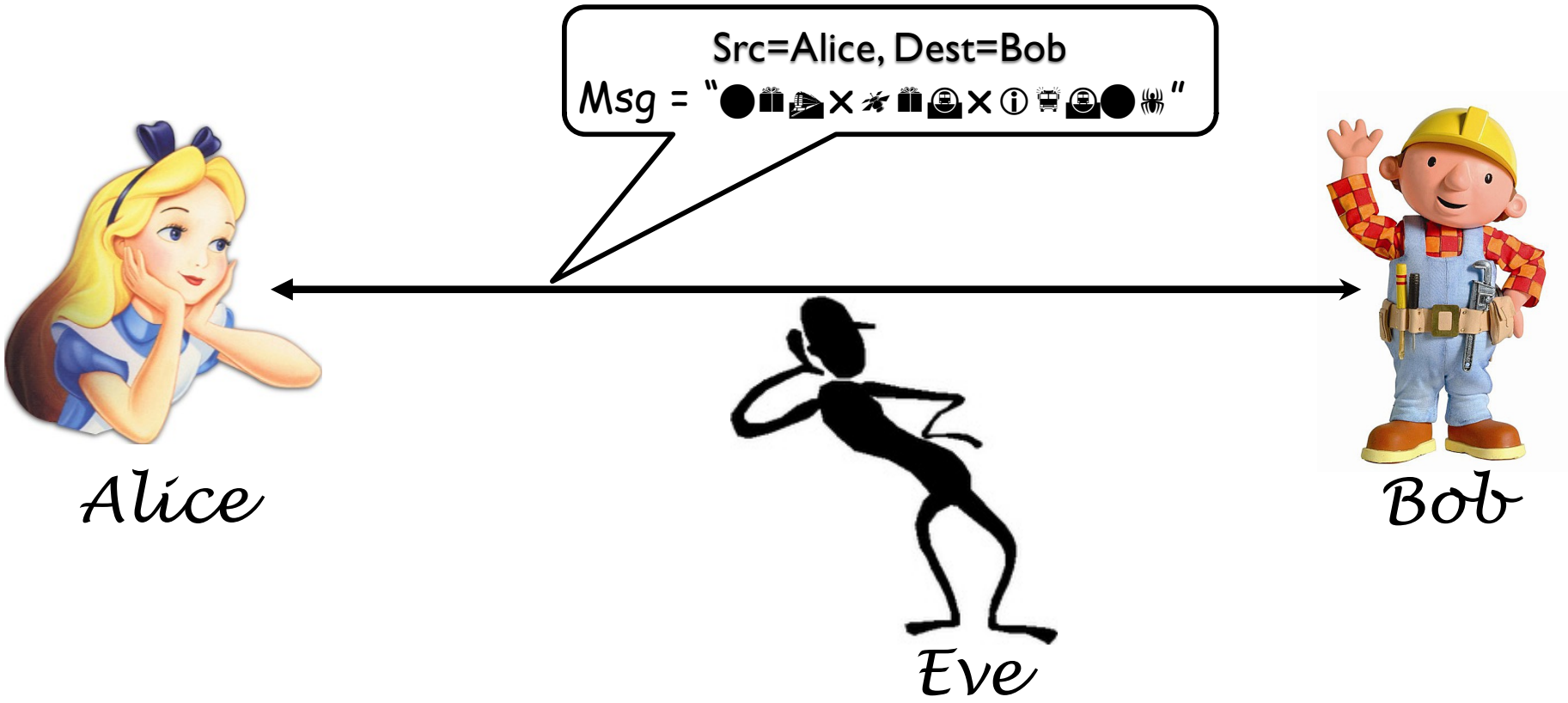
Homework 1 assigned today

- Learn to use LaTeX
- Introduce yourself
- Agree to the ethics statement
  - Required to pass the class
- Due: **September 5, 11:59PM**

Meet the players.

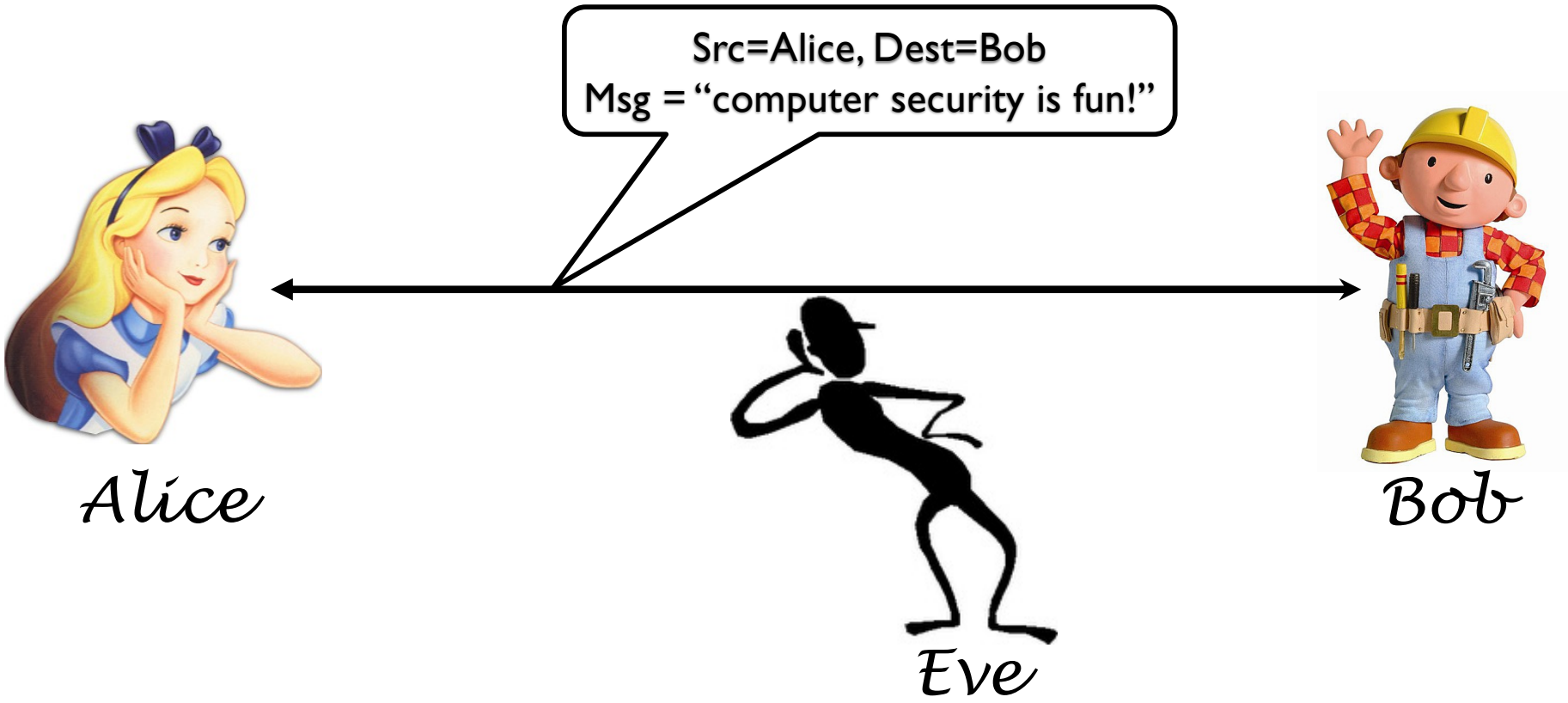
Let's look at some potentially desirable properties of a secure network system...

Confidentiality



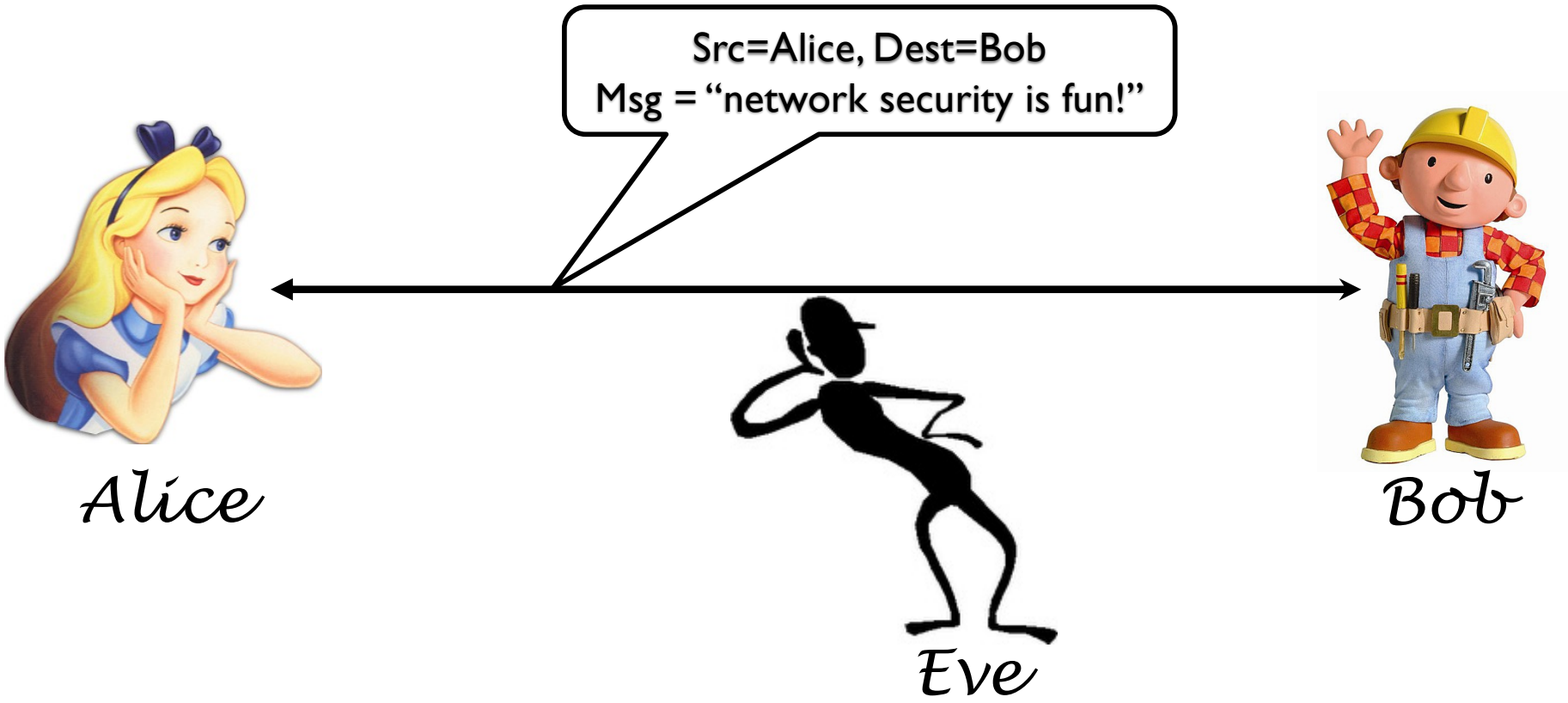
Alice and Bob want to communicate privately, preventing Eve from learning the contents of their communication

Integrity



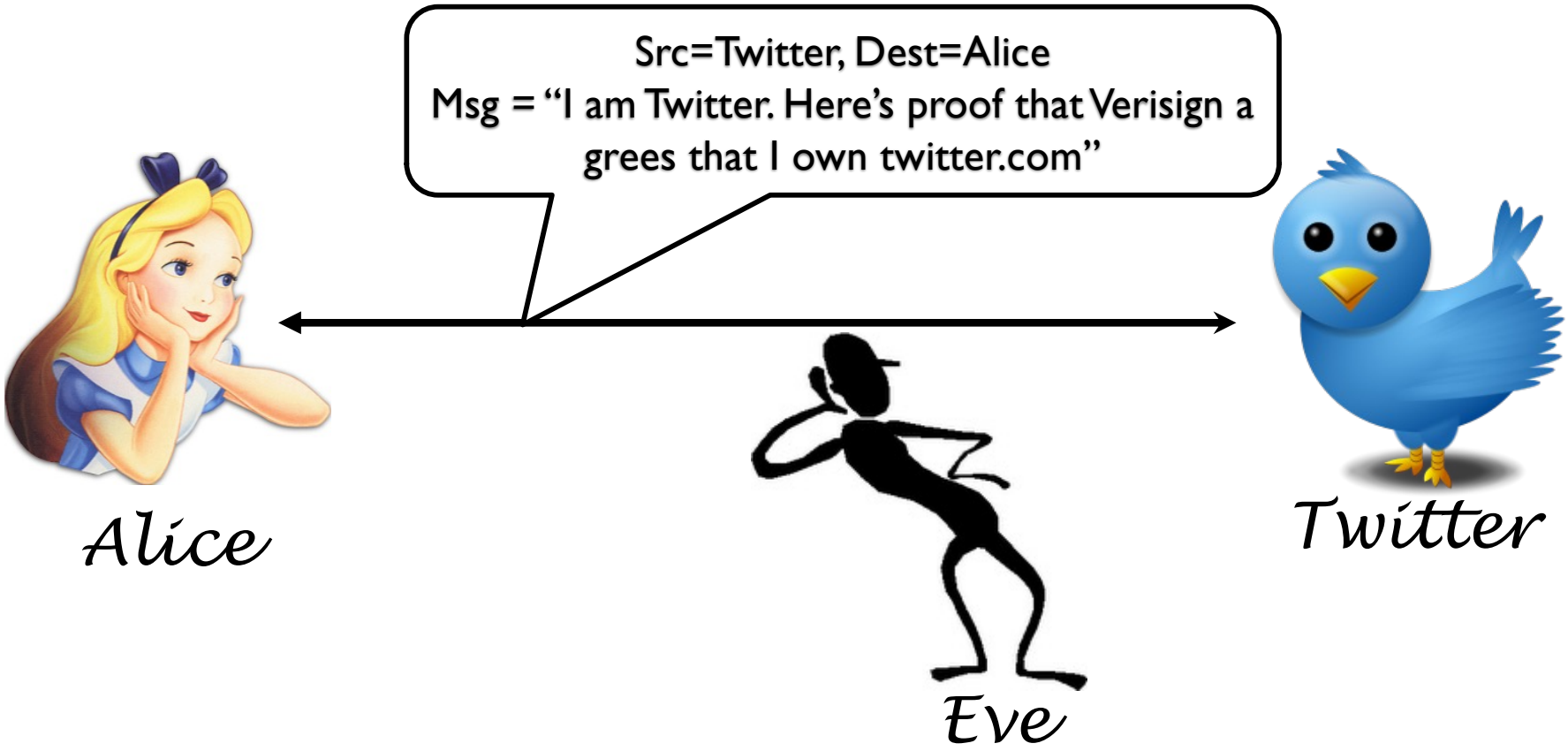
Bob wants to verify that the message hasn't been altered in transit.

Authentication



Bob wants to verify that the message is actually from Alice.

Server authentication

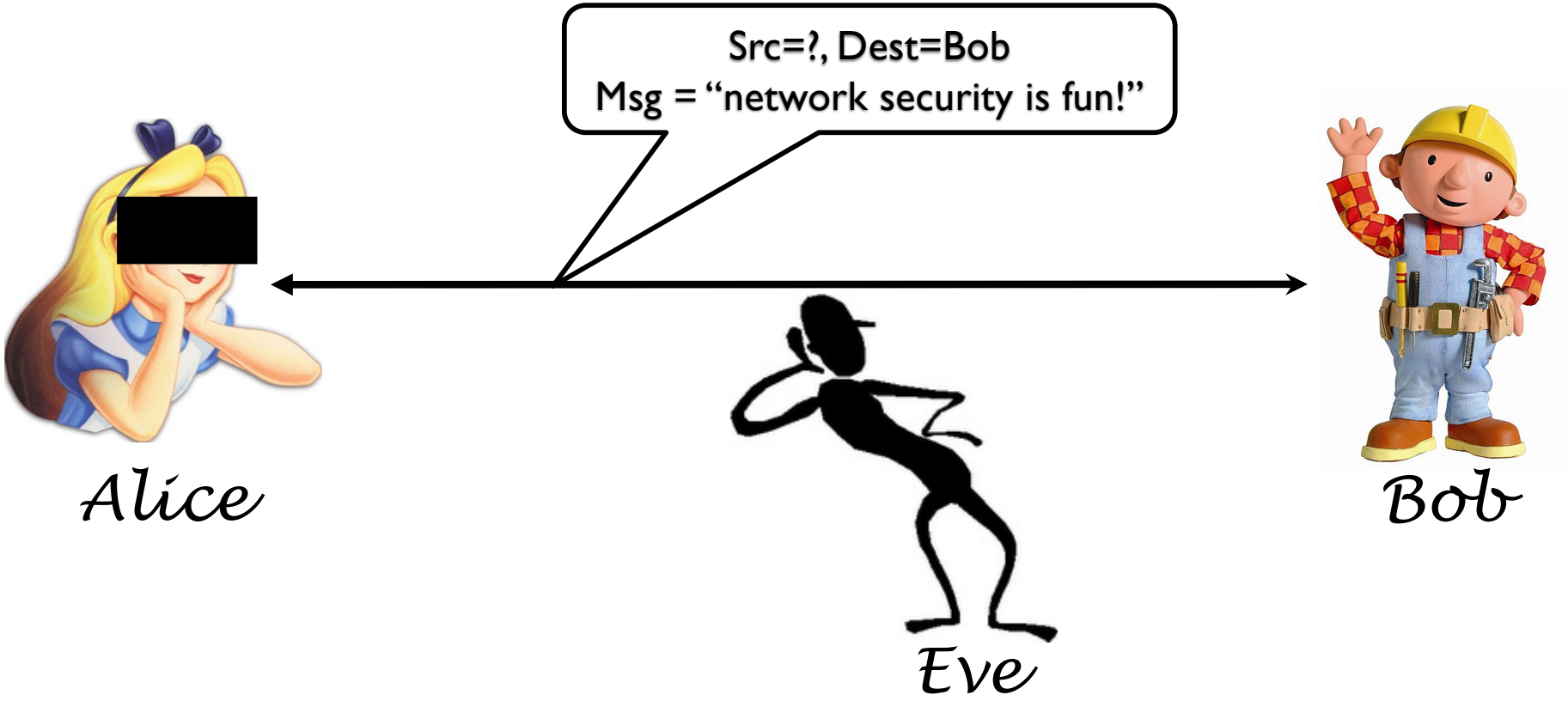


The service wants to prove its identity to Alice.

Client authentication

Alice wants to prove her identity to the service.

Anonymous communication



Alice wants to communicate anonymously to Bob (sender anonymity)

Security Research Methods I

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
    - Conclusion

    } *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 (cont.)

- 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., design papers)

Understanding what you read (cont.)

- What did they find?
  - 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.

The best papers are the ones that teach you something

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.

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")
    - Digitally: Zotero, Mendeley
  - 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 and see which one is the most effective for you.

Class Exercise

- Summarize the Thompson Article:
  - Contribution
  - Motivation
  - Related work
  - Methodology
  - Results
  - Take away

A Sample Summary

- Contribution: Ken Thompson shows how hard it is to trust the security of software in this paper. He describes an approach whereby he can embed a Trojan horse in a compiler that can insert malicious code on a trigger (e.g., recognizing a login program).
- Motivation: People need to recognize the security limitations of programming.
- Related Work: This approach is an example of a Trojan horse program. A Trojan horse is a program that serves a legitimate purpose on the surface, but includes malicious code that will be executed with it. Examples include the Sony/BMG rootkit: the program provided music legitimately, but also installed spyware.
- Methodology: The approach works by generating a malicious binary that is used to compile compilers. Since the compiler code looks OK and the malice is in the binary compiler compiler, it is difficult to detect.
- Results: The system identifies construction of login programs and miscompiles the command to accept a particular password known to the attacker.
- Take away: Thompson states the "obvious" moral that "you cannot trust code that you did not totally create yourself." We all depend on code, but constructing a basis for trusting it is very hard, even today.

Back to the Course Project

- The course project requires the student execute some limited research in security.
  - Demonstrate applied knowledge
  - Be realistic and practical about what can be accomplished in a single semester.
    - Don't try to learn some new *non-security field* *(e.g., if you do not know NLP, then…)*
    - Don't rely on external resources you don't have *(devices, servers, data)*
  - 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***.
- Talk to me if you want to do something related to your research

Project Choice

- *Create a Project Proposal and submit it to Blackboard (**Deadline: September 24rd***

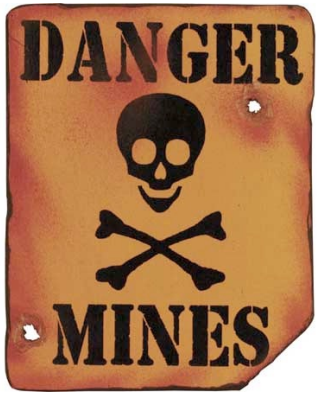
1. Ordered list of projects
   - Propose at least five unique projects in order of interest
2. Choose groups of 1, 2 (or 3 with approval)
3. A list of 2-3 meeting slots to meet with me to finalize the project *(Office Hours + by appointment)*
      - *Meeting with me prior to the deadline is recommended*

- I have the end say on your project and group
  - Hopefully, I can resolve the constraints implied
  - One functional group per project

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 or IoT Systems
  - Design and build an Android security extension.
  - Evaluate the security of a specific *class of Android apps* via systematic analysis (e.g., IoT managers)
- *Defenses for attacks seen elsewhere (Slashdot, BlackHat, DefCon, …)*
- ***Reproducibility study**: Reproduce the results of a set of recent top conf papers **(only if the source+dependencies are available).***
- Note: picking a topic is very important, and should almost certainly involve an area that you know well

Bad Ideas



- An encryption library for IM/SMS.
  - Done... to death...
- 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...
- Anything that requires source code access to proprietary software

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.