



WILLIAM & MARY

CHARTERED 1693

CSCI 445: Mobile Application Security

Lecture I

Prof. Adwait Nadkarni

First things first

- Make a **Nametag**

Why did you take this class?



Sub-\$100 Smartphone



Roll over image to zoom in

BLU Advance L5 -Unlocked Dual Sim, 16GB -Black

[Visit the BLU Store](#)

★★★★☆ 620 ratings | 67 answered questions

Best Seller

Price: **\$39.99** ✓prime & FREE Returns

Get 5% back (\$1.99 in rewards) on the amount charged to your Amazon Prime Rewards Visa Signature Card.

Model Name	Advance L5
Wireless Carrier	Unlocked for All Carriers
Brand	BLU
Form Factor	Smartphone
Memory Storage Capacity	16 GB
Operating System	Android 8.1

✓ [See more](#)

About this item

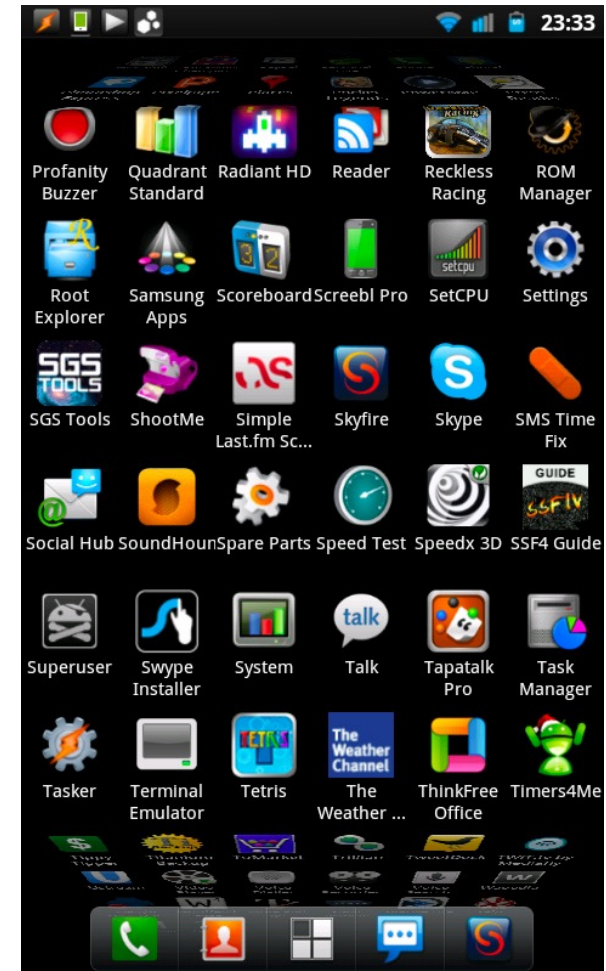
- Unlocked Dual SIM smartphone, Android 8.1 Oreo (Go Edition)
- 4.0" Touchscreen Display
- 5MP Main Camera with flash + 2MP Selfie Camera
- 16GB Internal memory 512MB RAM Micro SD up to 64GB, 1.3GHz Quadcore processor with Mali-400 GPU
- GSM Quad band, 3G (850/1900/2100) US compatibility with GSM Networks including, T-Mobile, Metro PCS, and others. (Not compatible with new AT&T or Cricket activations or with CDMA Networks like Verizon, Sprint, and Boost Mobile)

🗨 [Report incorrect product information.](#)

https://www.amazon.com/Advance-A390L-Unlocked-Phone-Camera/dp/B07Z6Q9NCZ/ref=sr_1_4?dchild=1&keywords=blu+smartphone&qid=1630539203&refinements=p_36%3A14674872011&rnid=14674871011&s=wireless&sr=1-4

Smartphones = Apps

- A smartphone is a cellular phone that allows the user to download and install *third-party applications*
- App = software
- App \approx **Web page**
- An app ...
 - is an interface to a service (e.g., Facebook, Google Maps)
 - brings content to users (e.g., Kindle, Netflix)
 - provides a specific utility (e.g., compass, document scanning)
 - ... *is a conceptualization of computing for users*

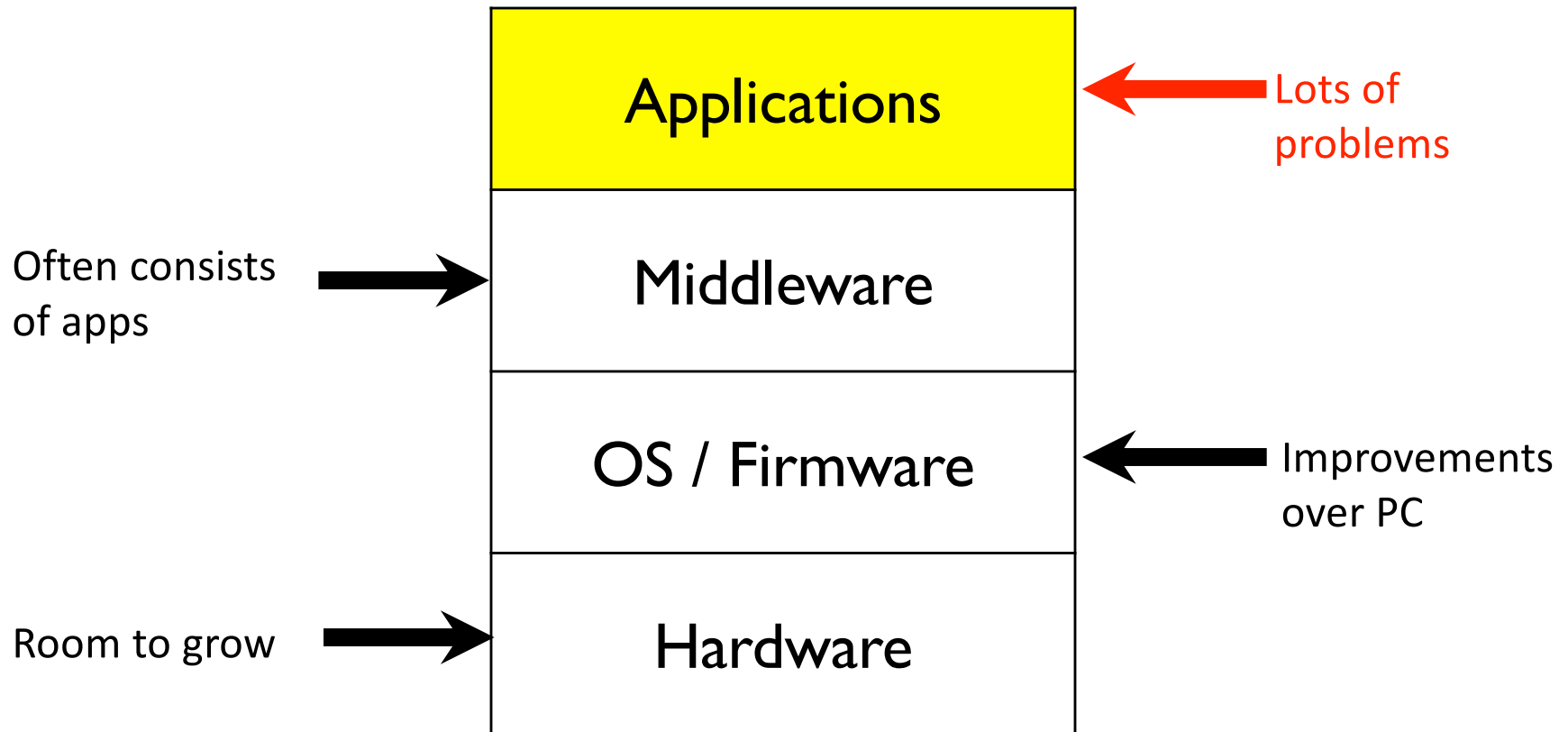


Mobile Application Design Characteristics

- In simple terms, an application is a program.
- What does a program do?:
 - Transform inputs → outputs
- What are these inputs/outputs?
 - Network
 - Storage
 - User Interface
 - Sensors/Camera/Mic
 - Other applications
 - ...?



Security at Different Layers



The new “modern” operating systems



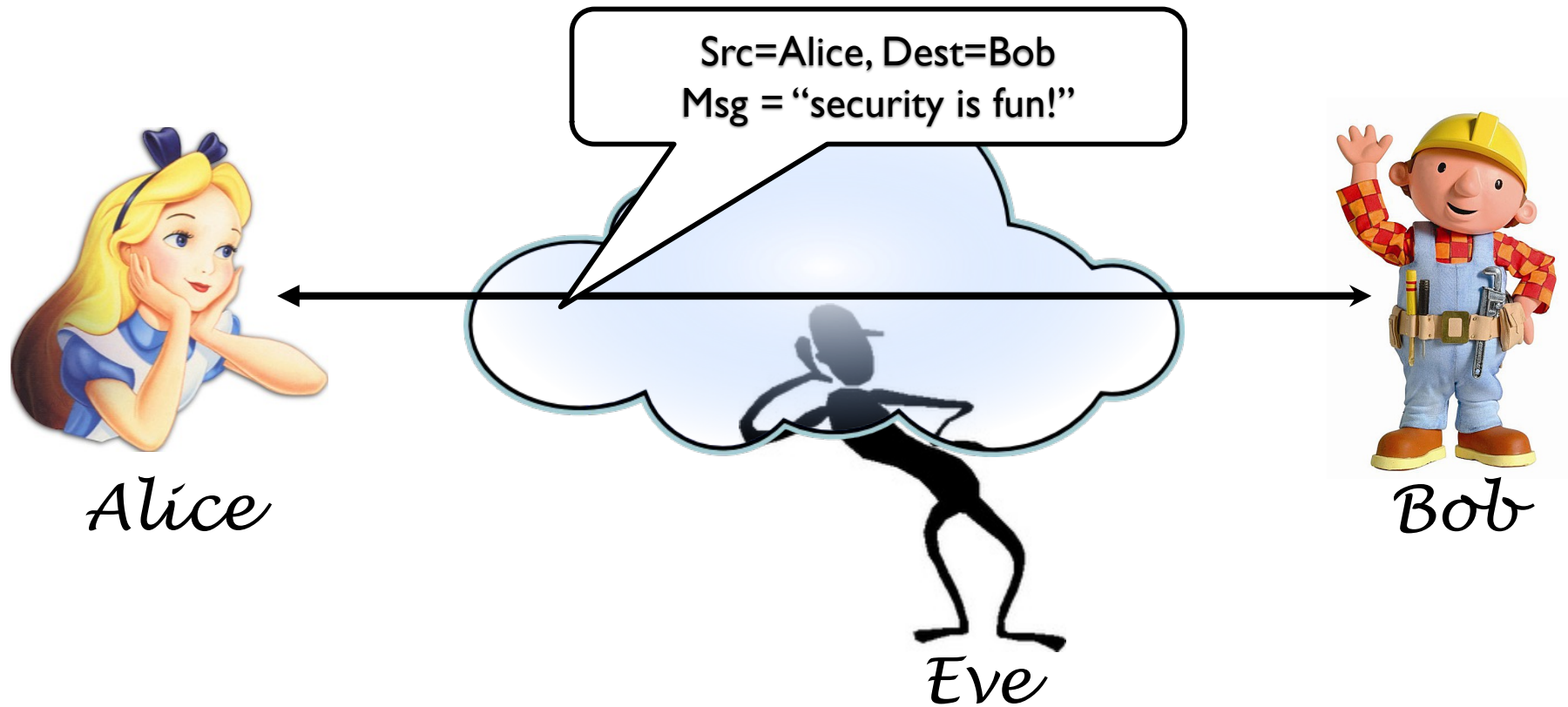
- Applications are *security principals*

Mobile application security

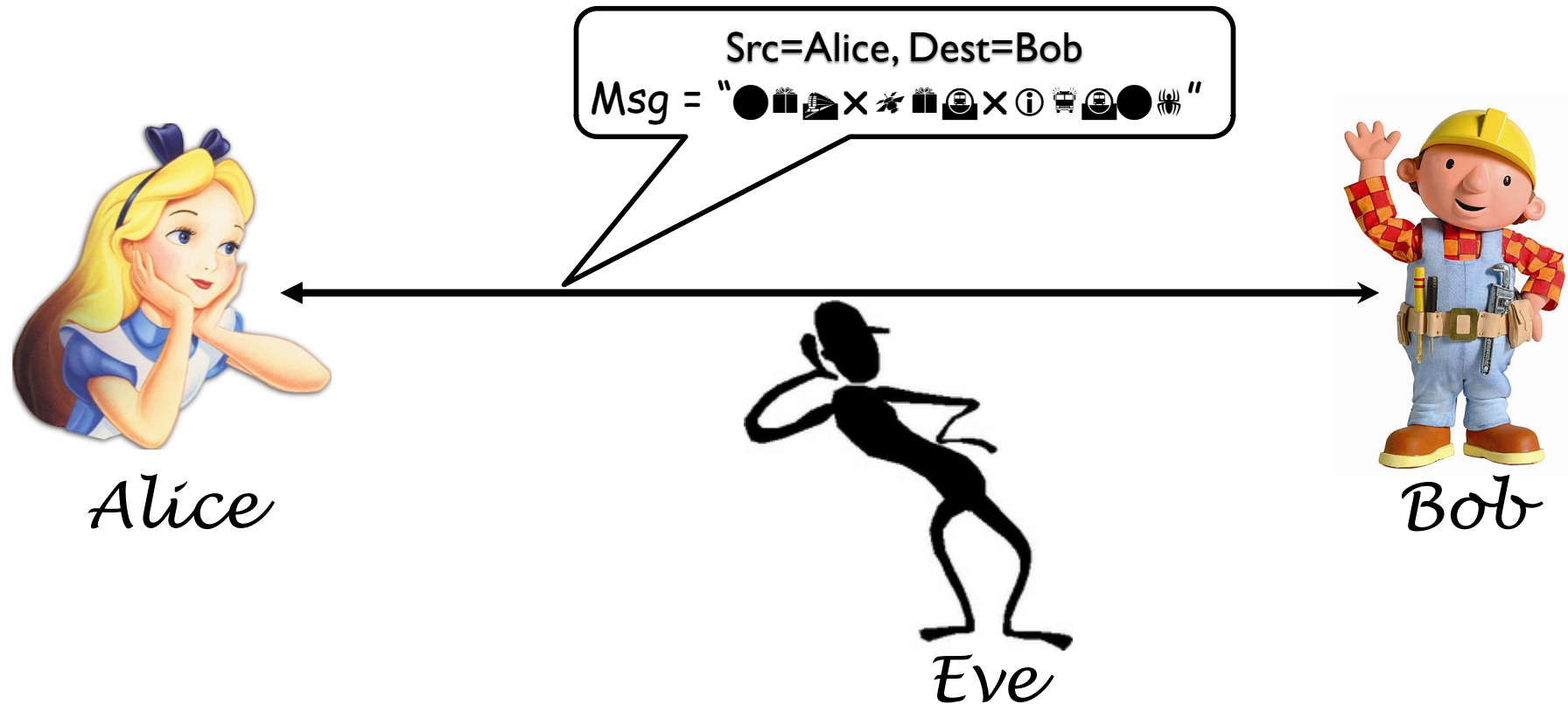
- Is about protecting what? (e.g., consider Gmail)
 - Users
 - App Interfaces
 - Data at Rest
 - Data in Transit
 - Intellectual Property
or Digital media (e.g., Netflix)
 - ...
 - What does *secure* mean?
- Inputs/Outputs:
 - Network
 - Storage
 - User Interface
 - Sensors/Camera/Mic
 - Other applications
 - ...?

**Let's look at some potentially
desirable properties...**

Meet the players.



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.

Client authentication



Alice wants to prove her identity to the service.

Server authentication



The service wants to prove its identity to Alice.

Mobile Application Security

- Is about protecting:
 - Users
 - App Interfaces
 - Data at Rest
 - Data in Transit
 - Intellectual Property
 - ...
- What does *secure* mean?
 - Confidentiality, integrity, authenticity, privacy

Designing *secure* systems is hard



Designing secure apps is hard

- Lots of work to be done!
- Major findings from prior research:
 - Apps *leak private user data*
 - Apps have *unprotected network connections*
 - Apps have *unprotected interfaces*
 - Apps ask for *user credentials*
 - Apps are *overprivileged*
 - Apps are sometimes even *malicious*
 - ...
- **Therefore**, prior research focuses on designing secure apps and analyzing apps for detecting unwanted behavior.

Goals

- My goal: *to provide you with*
 1. *an understanding of the security implications of application design choices,*
 2. *tools to grasp, evaluate and apply research in mobile application security.*
- Security pitfalls/ best-practices/ trade-offs
- Application security analysis
- *This is a hard course.* The key to success is sustained effort.
 - Do the readings and assignments
 - Participate in the class, including **extra credit opportunities**
- **Pay-off:** security competence is a rare, valuable skill

Non-Goals

- Familiarization with the latest tools
- Android/iOS application development
- Professional Security Certification

Course Topics

- High-level Topics:
 - Basics of crypto *(this isn't a crypto course)*
 - Basics of access control
 - Communicating over the network
 - Storage access
 - Inter-app communication
 - WebViews/ Protecting against Injection
 - User Privacy
 - Static/Dynamic/other analysis
- 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

- Software Development (CSCI 301)
- Programming experience: You will need to code, a lot!
 - *Most of the homeworks/project milestones require programming*
 - Experience with Java (and Android specifically) is a plus
- Familiarity with
 - IP Networks
 - Modern Operating Systems (Linux/UNIX)
 - Discrete Mathematics
- 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.adwaitnadhkarni.com/teaching/csci445>

- **Piazza** for discussions and announcements:
<https://piazza.com/wm/spring2022/csci445/home>
- **Blackboard** for assignment submission, grades:
<https://blackboard.wm.edu>
- **Slack** for in-class Q&A and project discussions
- **Zoom** for lectures if I fall sick

Office Hours

- Time: T/Th, 10:50 AM – 12:20 PM
 - and by appointment
- Place: ~~McGlothlin Street Hall, 104c~~
 - Zoom (Office hours room, invite shared on Blackboard and Piazza)

Textbook

- This course has *no required textbook*. However,
 - 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/>)

Readings

- **Readings** from published papers, online book chapters, and other sources
- **Important:** Published work can contain **mistakes** too
 - Trivial: Grammar, typos
 - Non-trivial:
 - Unrealistic/incorrect assumptions (e.g., about systems, human behavior) → example: *fire sprinkler “apps”*
 - Faulty arguments (e.g., due to an incorrect understanding of the premise, or just bad logic)
 - Incorrect math
 - Excessive claims (e.g., claims of generality not backed by the evaluation).

Readings

- **Readings** from published papers, online book chapters, and other sources
- **Important:** Published work can contain **mistakes** too
- *Each student owes Prof. Nadkarni **2 bugs** from published papers assigned in class (2.5 pt each, **5 course points total**)*
- The bugs must be
 - Non-trivial/substantial
 - New (*first to report*)
 - Correct/valid, and you must be able to *tell me why*
- I decide all if a bug is valid, i.e., satisfied the 3 criteria.
- You do not need expertise in mobile app security to do this; but only *critical thinking*

Things that are not your readings



WIKIPEDIA
The Free Encyclopedia

Slashdot

News for Nerds. Stuff that matters.



engadget

Online Course Discussion

- **Extensive** class discussions and announcements via Piazza.
- You are expected to read each and every posting
- You are expected to participate: **10 Points for class participation**
- Try not to post anonymous unless necessary (can't grade otherwise)

CSCI 445 ▾ Setup Q & A Resources Statistics ▾ Manage Class

College of William and Mary - Fall 2021

CSCI 445: Mobile Application Security

+ Add Syllabus

Course Information

Staff

Resources

Description

Edit

This course is a senior-level introduction to mobile application security. Students successfully completing this class will be able to understand and apply the various security best-practices in designing mobile applications, and will also develop a background in the research and practices in performing security analysis of mobile applications.

The course will introduce the fundamental concepts in security and privacy (e.g., confidentiality, threat models, crypto basics, SSL/TLS, access control) and demonstrate how these concepts apply to secure mobile application development. Students will also learn the various techniques used in

Announcements

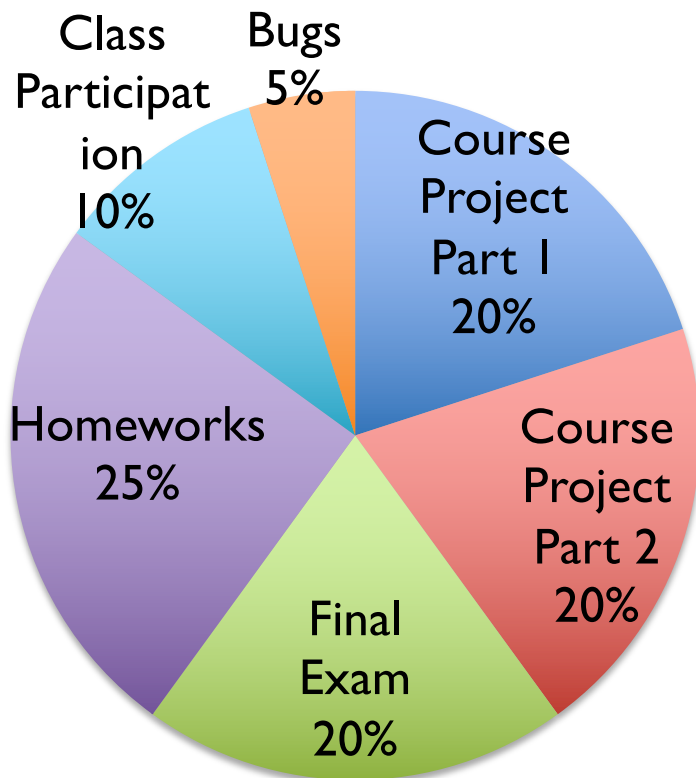
Add an Announcement
Click the Add button to add an announcement.

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 mobile 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

Grade Breakdown



- Course project is a major emphasis of the class
- 5 homework assignments (25%)
 - Question based: Conceptual and short, *OR*,
 - Programming: App development and analysis
 - Can discuss → Write your own answers/code + let me know who you discussed with.
 - 25% penalty for late homeworks within 24 hrs, 100% penalty thereafter.

Homework 1, Assigned today

- **Part 1:** Learn to use LaTeX
 - Introduce yourself
 - Agree to the ethics statement
 - Required to pass the class
- **Part 2:** Programming
 - Make a “Hello World” Android application
 - “Hello World” *notification* every 30 seconds
- **Due: September 6th, 11:59PM**


Course Project

Phases

Phase 1: Secure Mobile App Development
20% grade, or 100 points

Phase 2: Mobile Application Security Analysis
20% grade, or 100 points

Milestones

1. Project Proposal (10 points)
2. App design and implementation (90 points)
3. Analysis Plan (40 points)
4. Analysis Report (60 points)
5. Project Presentation (≤ 5 extra credit on course grade) 

09/01

10/18

12/08

Exams and Quizzes

- Final (20% Grade)
 - Conceptual Questions (Basic and Complex)
 - Constructions
 - Precise Answers
- Quizzes (Included in class participation)
 - Quick quizzes on the previous lecture and readings
 - **A quiz after every class**
 - *If I have ~10 minutes to spare.*
 - Quizzes on *readings* may require:
 - Define Concepts
 - Comparison with Other Approaches
 - Details of Approach

Other Policies

- Please turn off cell phones during class.
- I will do my best to respond to emails (Subject: CSCI445) within 24 hours. You will receive faster answers if you post to Piazza.
- 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.
- Be civil: 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

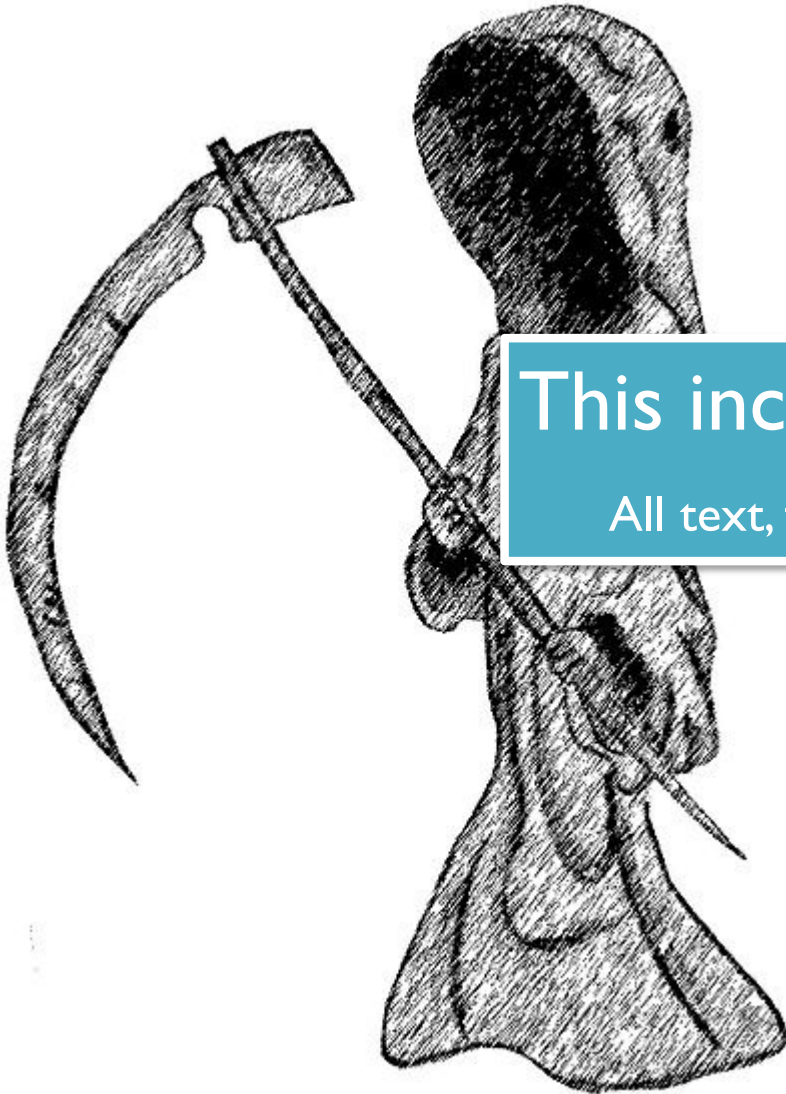
If you get caught, you will get a *negative* grade on an **F** on you

This includes the course project!

All text, figures and code should be your own.

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



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

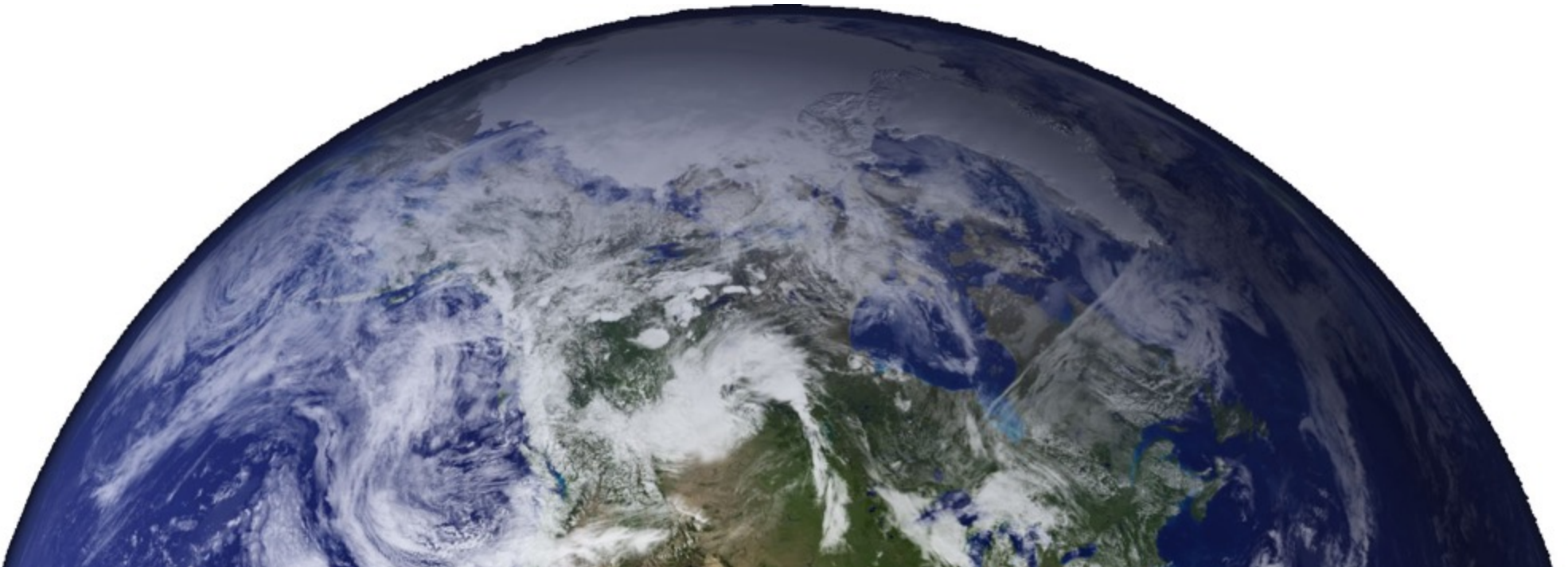
- This course considers topics involving personal and public privacy and security. **As part of this investigation we will cover technologies whose abuse may infringe on the rights of others.** As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention 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.



Recall: Project Proposal

- *Deadline: September 13, 11:59 PM (Tuesday)*
 - At least **five unique** application ideas in order of interest
 - Each possessing at least *4 characteristics (i.e., network, storage, inter-app communication, permissions, Webviews, etc.)*.
 - Part of one or more real features.
 - Names of **up to 4 group members**.
- **IMPORTANT:** Immediately after submitting the proposal to Blackboard, ***schedule a 30 minute meeting with me***
- I have the final say on your project and group

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.

