CMSC 426
Principles of Computer Security

Introduction

Today's Topics

- Course Information and Syllabus
  - Grading Scheme
  - Academic Integrity

- Security Objectives
  - CIA Triad
- Avenues of Attack

Introductions

- Dr. Katherine Gibson
  - Education
    - BS in Computer Science, UMBC
    - MS & PhD in CS, University of Pennsylvania
  - Likes
    - Dogs
    - Video Games
    - Nail polish
  - Favorite CS topics:
    - Pointers
    - Makefiles
    - Why Java sucks

What the Course is About

- Principles of Computer Security
  - A broad overview of a variety of security topics
    - Threat, attack, and adversary models
    - Essentials of cryptography
    - Computing security models
    - Network and database security
    - Malware
    - Secure programming
    - OS security
    - Legal and ethical issues

Course Resources

- Blackboard
  - For announcements, turning in assignments, receiving grades
  - Has link to website and Piazza on sidebar
- Website
  - Has information on schedule, assignments, exam info, office hours
  - Where lecture slides will be posted
- Piazza
  - For asking/answering questions, forming groups, etc.

Grading Scheme

- This class has
  - 4 Labs (100 points each)
    - Large, hands-on assignments
  - 5 Homeworks (20 points each)
    - Small, theory and application-based assignments
  - 5 Papers (10 points each)
    - Short papers done in small groups
    - Response papers, summary papers, etc.
  - 3 Exams (150 points each)
    - Non-comprehensive exams

Submission and Late Policy

- Most assignments will be submitted via Blackboard

- Assignments are due Wednesdays at midnight (11:59:59 PM)
- Late assignments receive a ***<u>zero</u>***
- In other words, there are no late assignments

- Extensions may be granted, but only for <u>actual</u> emergencies
  - Submit early, submit often

Academic Integrity

General Rules

- Don’t copy someone else’s work
- Don’t leave your work unprotected
- Don’t post your code online
- Don’t pay someone else to do your work
  - Automatic F in the course

- Come to office hours or Piazza for help

- Don’t be stupid (please)

Using Online Resources

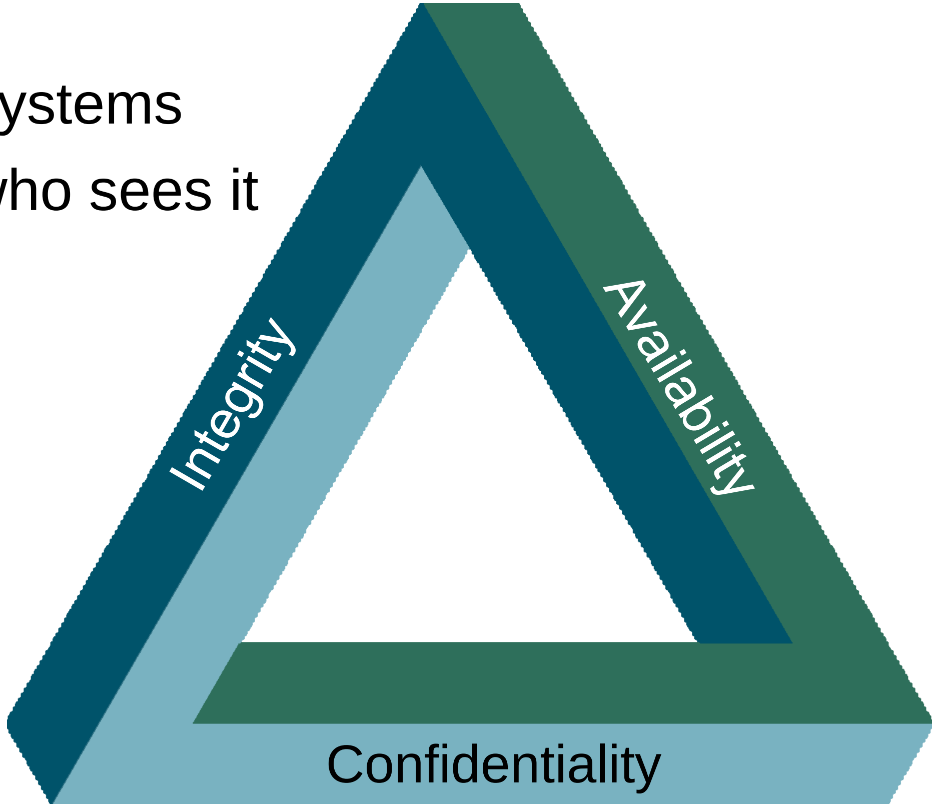
- You’re allowed to use Google, Stack Overflow, etc.
  - Provided it does ***not*** comprise a significant portion of your submission

- If you use resources (outside of the course slides/book), you ***must*** cite their use:
  - Where you found the information
  - What the code does/how the explanation applies/etc.
  - Whether it was copied, adapted, or only provided inspiration

Introduction to Security

Security Objectives: The CIA Triad

- There are three key objectives in computer security:
  - Confidentiality
    - Data is not available to unauthorized persons/systems
    - Users have control over their information and who sees it
  - Integrity
    - Accuracy and completeness of data is assured
    - System performs functions unimpeded
  - Availability
    - System, information, and means of access are kept in working order and function correctly



Additional Objectives

- Authenticity
  - Users and data can be verified to be genuine and therefore trusted
- Accountability
  - Actions (like security breaches and false data) can be traced to their source or origin → Why does this matter?
- Non-repudiation
  - Users cannot deny their involvement in sending/receiving data
  - Legal term; encompasses the system as a whole

Accountability for an Imperfect World

- ~~Security protocols and systems can fail and be breached~~
- Security protocols and systems will fail and be breached

- Need to be able to trace failures and breaches to their source
  - Origins and destinations of sent data
  - Which users access what data and when

- Ideally, detect and report intrusion when it happens (instead of when someone notices a problem later)

Avenues of Attack

- Computer systems have multiple avenues of attack
  - Software
  - Hardware
  - Networks
  - Physical
  - Human/Social
  - Insider attack
  - Passive attack

"Acoustic Side-Channel Attacks on Printers"

Phishing emails, phone scams, oversharing

Exercise: Security Examples

- How do each of the following examples measure up in terms of confidentiality, integrity, and availability?
- What avenues of attack are applicable for each?

Walls

Wax seals

Burner phones

Credit cards

Daily Security Tidbit

- DEFCON Voting Machine Hacking Village
  - 25 (paperless electronic) voting machines and 13 imitation websites were made available for physical probing and hacking attempts
  - Problems: plain text password storage, expired certificates, easily-breakable physical locks, “password” as a password, etc.

  - 11-year-olds hacked the Florida website in under 15 minutes
  - A 17-year-old took down the entire website by writing down the IP address and googling MySQL commands for five minutes
  - Another hacker played gifs and music by uploading a Linux OS

Announcements

- We will be meeting on Tuesday
  - Enjoy the long weekend!

- Course website will update with a more detailed schedule of topics and assignment due dates

Image Sources

- Penrose triangle (adapted from):
  - https://pixabay.com/en/optical-illusion-illusion-triangle-154081/
- Hadrian's wall (adapted from):
  - https://commons.wikimedia.org/wiki/File:Hadrian%27s_wall_at_Greenhead_Lough.jpg
- Wax seal:
  - https://www.flickr.com/photos/artistmam/4245651173/
- Burner phone:
  - https://pixabay.com/en/nokia-1280-cell-phone-mobile-1502601/
- Credit card:
  - http://www.freestockphotos.biz/stockphoto/8210