CMSC 414 — Computer and Network Security

Introduction

Dr. Michael Marsh

August 28, 2017

Course Goal

- What is security?
- What kinds of things can go wrong?
- How do we prevent things from going wrong?
- How do we assess the security of a system?
- How can we address things beyond our control?

Logistics

You **must** come to class, or provide a valid excuse (in advance, if possible)

Things to bring:

- Clicker or device with TurningPoint app
- Laptop for short programming exercises

No required text, see course webpage for reading assignments

- I expect you to have done the readings before lecture
- We will not cover the assigned material in detail

See ELMS for assignments

- Check frequently — new assignments will be posted after the 3:30 lecture

Logistics

Grading (*will be curved*):

	Percentage of Final Grade
In-class assignments	*5*
Preliminary assignments	*5*
Reinforcing assignments/projects	40
In-class exams (2)	30
Final exam (cumulative)	20

Teaching Staff:

Instructor

- Dr. Marsh

Graduate TAs

- Soumya Indela
- Akhil Koul

Undergraduate TAs

- Rachel Baylor
- Kevin Jordan
- Vinay Viswanadha

Question 1

You've just learned about a cool exploit. Where might you try this out for yourself?

A. A virtual machine on your computer

B. A random website

C. The CS Department's grades server

D. Your roommate's computer

Tools and Resources

See the course webpage

- Virtual Machine $\Leftarrow$ Use it!
- GDB
- C, Python, Bash
- Git $\Leftarrow$ How you'll get some of your assignments!
- Piazza
- ELMS $\Leftarrow$ Check it frequently!

Your Responsibilities

- **Code of Academic Integrity**
- **Do not** violate any laws or anyone's privacy
- Do all the readings **before** class
- Do *not* skip *any* assignments
  - 2 assignments for each lecture: 1 before, 1 after
- Attend *all* lectures (unless you have a valid excuse)
  - Quizzes every class are part of your grade

Question 2

You've got a big project due in another class, so you figure you'll just blow off the CMSC 414 assignment that's due. What is the result of this?

A. You get no credit on it, and put in extra effort on the remaining assignments.

B. You had a friend do it for you, so you're good.

C. You explain the situation to the instructor, and get an extension.

D. You fail the class.

Security

It's a big topic, spanning:

- Biology (bitterness, toxins, genetic "altruism", etc.)
- Society (law enforcement, armies, insurance, etc.)
- Technology (locks, fences, encryption, etc.)

We can't hope to cover everything, much less in depth

- Even limiting ourselves to computer technology
- Have to trade off how much we cover with depth of coverage

Survey:

- Programming errors, exploiting them, and preventing them
- Cryptography and its applications
- Network protocol vulnerabilities and defenses
- User-driven security

Group Exercise 1

What does security mean to you?

Discuss at your table (1 minute), 1-5 word phrases

Terminology

Coherent discussion requires some standardization of language

Systems, and parts thereof

- Protocols/designs
- Software implementations
- Hardware
- Infrastructure
- People

Security Properties

Subjects/Principals/Identities

- Who/what participates in the system
- Aggregates like **groups** and **roles**

Trust/Trustworthiness

Vulnerability/Threat/Exploit

Security Properties

Can't design or evaluate a system without knowing what properties we want

Allows us to define a **security model** and **threat model**

What we want to guarantee, against what sort of **adversary**

Question 3

Which of the following is *not* a security property?

A. Anonymity

B. Complexity

C. Integrity

D. Privacy

Confidentiality and Integrity

Confidentiality Protecting data from unauthorized access

Integrity Assuring that data has not been modified

Authenticity Integrity plus *freshness*

Techniques:

- Encryption/Encoding/Encipherment
- Digital Signatures
- Hashes/Checksums

Location:

- In motion ("on the wire")
- At rest ("on disk")

What we need depends on **what we're doing with the data** and **what we need to protect** $\Rightarrow$ security/threat models

Privacy, Anonymity, and Availability

Relatively recent as security properties

Security used to be about institutions, not users

For most people, the Internet started in the late '90s

Privacy	Control over your own *data*
Anonymity	Control over your own *metadata*
Availability	Ability for *legitimate users* to access a system

metadata $\equiv$ **data**

Group Exercise 2

What are some examples of threats?

Discuss at your table (1 minute)

Types of Threat Actors

- Nation States
- Criminal Organizations
- “Hactivists”
- Glory Hounds/Bored Hackers
- “Script Kiddies”
- **Insiders** $\Leftarrow$ #1 Threat!

Types of Vulnerabilities

- Programming Errors
- Improper Use of Cryptography
- Misplaced Trust
- Imbalanced Economic Motivations
- Incorrect Assumptions

Question 4

Which of the following is a *subject*?

A. The door of a bank vault

B. Bob from Accounting

C. Alice's private key

D. System administrators

System Participants

Broadly speaking:

Subject	*Who*
Principal	*Who* or *What*
Identity	Are *A* and *B* the same *principal*?
Group	A set of *principals*
Role	A set of functions/permissions

Often, a *subject* participates **indirectly** in a system through another *principal*

Alice's private key **speaks for** *Alice*

You will have first-hand experience with this on `gizmonic.cs.umd.edu`

Roles

Allows consistent control/configuration for a potentially fluid *group*

Every role has access to *something*

Some examples:

- Supervisor
- Auditor
- Developer
- System Administrator
- Student
- Janitor

Question 5

What do you call the property that something has not been modified?

A. Authenticity

B. Availability

C. Confidentiality

D. Integrity

The Rest of this Course...

1. Common programming errors (starting with **buffer overflows**)
2. Cryptography and related topics
3. Applications of Cryptography
4. Network Security
5. Censorship
6. Economics/Human Behavior

Group Exercise 3

To finish out today's class, take a look at some of the blogs and news sites on the course page. **How do some of the recent stories relate to the high-level concepts we've covered today?**

Discuss at your table