# Course Overview



CS 458: Information Security

Kevin Jin

# Outline

- Administrative Issues
- Class Overview
- Introduction to Computer Security
  - What is computer security?
  - Why computer security?
  - Computer security components

# This Course

- is instructed by Kevin Jin
  - dong.jin@iit.edu
  - Xiaoliang Wu (xwu64@hawk.iit.edu)
- comes with FREE office hours:
  - Monday 3:15 pm – 4:15 pm or by appointment
- has a course website
  - https://sites.google.com/view/cs458-fall-2020/
  - Lecture slides, class schedule, syllabus, no-grading homework
- has a piazza discussion forum
  - https://piazza.com/iit/fall2020/cs458/home
- has a blackboard
  - Live classes and office hours; watch class videos
  - Submit labs, quizzes

# Who am I?

- CS faculty, Ph.D., University of Illinois at Urbana-Champaign (UIUC), http://cs.iit.edu/~djin/
- Research: cyber-security, networking, cyber-physical system security, simulation & modeling
- Industrial experience at Los Alamos National Lab, IBM, Motorola
- I like designing/building/deploying large-scale software systems that are grounded in strong theoretical principles

# Course Overview - Textbook

- Textbook (Recommended)
  - Computer Security: Principles and Practice by William Stallings and Lawrie Brown, second edition
  - Computer & Internet Security: A Hands-on Approach by Wenliang Du, Second Edition
- Additional Readings (useful but not required)
  - Computer Security: Art and Science by Matt Bishop
  - Applied Cryptography by Bruce Schneier
  - Information Security Risk Analysis by Thomas Peltier
  - Threat Modeling by Frank Swiderski
  - Security in Computing by Charles P. Fleeger
  - Security Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson
  - Network Security—Private Communication in a Public World, 2nd Edition (2002), by Charlie Kaufman, Radia Perlman, and Mike Speciner

# Course Overview - Syllabus

- Introduction to the major topics in computer security
  - human factors in security policy
  - cryptography
  - key and identity management, authentication, access control
  - network and system security
  - software security, database security
  - malware
  - cyber-physical system security
  - more …

# Course Overview - Syllabus

- Objective: to provide a basic understanding of the problems of information assurance and the solutions that exist to secure information on computers and networks
- The very first security class, to explore more about cyber security
  - Master of cyber-security degree
    - https://www.iit.edu/academics/programs/cybersecurity-mas
    - Red team/blue team exercises, data protection and privacy, IoT, software, network, system, AI …
  - Available for co-terminal students as well

# Course Overview - Lectures

- Lecture Slides - Disclaimer
  - Not intended to be self sufficient
  - Going through lecture slides will NOT be enough to master course materials
- Occasionally, we may have
  - Pre-recorded lectures
  - e.g., this coming Wednesday, 8/26

# Course Overview - Grading

| | |
|---|---|
| Labs | 60% |
| Self-Evaluation Quizzes | 10% |
| Final Exam | 30% |
| Piazza Posting (Good Q&A) | 5% (bonus) |

## Homework

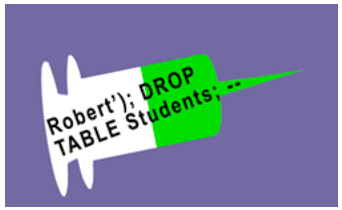
- About 10 homework
- **NOT** be graded (no submission required), but strongly advised for doing well in the exam and quizzes

## No extra project for extra credits

# Course Overview - Labs

- 4 Labs
  - MD5 Collision Attack
  - RSA Encryption and Signature
  - SQL Injection Attack
  - TCP Attacks
- Release and submit via Blackboard
- Download and install VM
  - use the Ubuntu 16.04 VM
  - https://seedsecuritylabs.org/lab_env.html






# Academic Honesty

## IIT has a strict academic honesty policy

- The misrepresentation of any work submitted for credit as the product of a student's sole independent effort, such as using the ideas of others without attribution and other forms of plagiarism.
- The use of any unauthorized assistance in taking quizzes, tests or examinations.
- The acquisition, without permission, of tests, answer sheets, problem solutions or other academic material when such material has been withheld from distribution by the instructor.
- Deliberate harmful obstruction of the studies, research or academic work of any member of the IIT community.
- Making a material misrepresentation in any submission to or through any office of the university to a potential employer, professional society, meeting or organization.
- The intentional assistance of others in the violation of the standards of academic honesty.

You can read the entire policy at

http://www.iit.edu/student_affairs/handbook/information_and_regulations/code_of_academic_honesty.shtml

# Acknowledgement

Some class materials borrowed from Dr. Susan Hinrichs, Dr. David Nicol, Dr. Rakesh Bobba, Dr. Mark Stamp, and Dr. Wenliang Du.

# Rest of Today

- Introduction to computer security

# Security is not a Point Product

# Computer Systems to Protect

- Operating Systems
- Networks
- Software Applications
- Smart Phones
- Embedded Systems
- Cyber Physical Systems
- …

We will not event attempt to be exhaustive

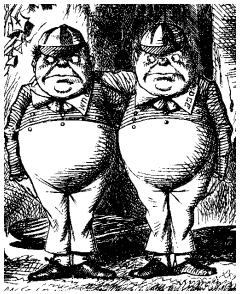
# Adversaries

- Mischief makers (script kiddies)
- Hackers
- Criminals
- Hacktivists
- Nation states
- Ourselves (sometimes) ☺
- ….

# The Cast of Characters

- Alice and Bob are the **good guys**

- Eve is the **bad "guy"** →



- Eve is our generic "intruder"

# Alice opens Alice's Online Bank (AOB)

- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice's and Bob's concerns similar? How are they different?
- How does Eve view the situation?

# Computer Security Goal: CIA

- **Confidentiality**
  - Keeping data and resources hidden
  - Privacy
- **Integrity**
  - Data integrity (integrity)
  - Origin integrity (authentication)
- **Availability**
  - Enabling access to data and resources

# CIA

- AOB must prevent Eve from learning Bob's account balance
- **Confidentiality:** prevent unauthorized *reading* of information
  - Cryptography used for confidentiality

# CIA

- Eve must not be able to change Bob's account balance
- Bob must not be able to improperly change his own account balance
- **Integrity:** detect unauthorized *writing* of information
  - Cryptography used for integrity

# CIA

- AOB's information must be available whenever it's needed
- Alice must be able to make transaction
  - If not, she'll take her business elsewhere
- **Availability:** Data is available in a timely manner when needed
- Availability is a "new" security concern
  - Denial of service (DoS) attacks

# Beyond CIA: Crypto

- How does Bob's computer know that "Bob" is really Bob and not Eve?
- Bob's password must be verified
  - This requires some clever **cryptography**
- What are security concerns of passwords?
- Are there alternatives to passwords?

# Beyond CIA: Protocols

- When Bob logs into AOB, how does AOB know that "Bob" is really Bob?
- As before, Bob's password is verified
- Unlike the previous case, **network** security issues arise
- How do we secure network transactions?
  - **Protocols** are critically important
  - Crypto plays critical role in protocols

# Beyond CIA: Access Control

- Once Bob is *authenticated* by AOB, then AOB must restrict actions of Bob
  - Bob can't view Charlie's account info
  - Bob can't install new software, etc.
- Enforcing these restrictions: *authorization*
- **Access control** includes both authentication and authorization

# Beyond CIA: Software

- Cryptography, protocols, and access control are implemented in **software**
  - Software is foundation on which security rests
- What are security issues of software?
  - Real world software is complex and buggy
  - Software flaws lead to security flaws
  - How does Eve attack software?
  - How to reduce flaws in software development?
  - And what about malware?

# Some Terminology

- **Threat** – Set of circumstances that has the potential to cause loss or harm.
- **Vulnerability** – Weakness in the system that could be exploited to cause loss or harm
- **Attack** – When an entity exploits a vulnerability on system
- **Control or Countermeasure** – A means to prevent a vulnerability from being exploited
- **Adversary** – threat agent

# Classes of Threats

- **Disclosure** – Unauthorized access to information
- **Deception** – Acceptance of false data
- **Disruption** – Interruption or prevention of correct operation
- **Usurpation** – Unauthorized control of some part of a system

What security goal (CIA) does each class violate?

# Things to cover in CS458

# Cryptography

- Classic cryptography
- Symmetric ciphers
- Public key cryptography
- Hash functions
- Advanced cryptanalysis

# Access Control

- Authentication
  - Passwords
  - Digital certificate
  - Other methods of authentication
- Authorization
  - Access Control
    - Lists/Capabilities
    - Role-Based Access Control
    - Mandatory Access Control
  - Multilevel security (MLS), inference control
  - Firewalls, intrusion detection systems (IDS)

# Protocols

- "Simple" authentication protocols
  - Focus on basics of security protocols
  - Lots of applied cryptography in protocols
- Attacks on network protocols
  - TCP/IP, UDP, ICMP, DNS …
- Real-world security protocols
  - SSL, IPSec, Kerberos

# Software

- Security-critical flaws in software
  - Buffer overflow
- Malware
  - Viruses, worms, botnets
  - Prevention and detection
- Software reverse engineering (SRE)
  - How hackers "dissect" software

# Software

- Software is a BIG security topic
  - Lots of material to cover
    - e.g., Database security, Buffer overflow
  - Lots of security problems to consider
  - But not nearly enough time available…

# Key Points

- Must look at the big picture when securing a system
- Main components of security
  - Confidentiality
  - Integrity
  - Availability
- Differentiating Threats, Vulnerabilities, Attacks and Controls

# Reminder

- Course website
  - https://sites.google.com/view/cs458-fall-2020/
  - Lecture slides, class schedule, syllabus, no-grading homework
- Piazza discussion forum
  - https://piazza.com/iit/fall2020/cs458/home
  - sign-up link https://piazza.com/iit/fall2020/cs458

- Upcoming Wednesday' class will be pre-recorded on blackboard