Introduction to Information Security
14-741/18-631 Fall 2021
Unit 1: Lecture 1: Introduction

Limin Jia liminjia@andrew

Hanan Hibshi hhibshi@andrew

Limin Jia (Units 1,2,4,5)

Contact Info
liminjia@cmu.edu

- **Brief Bio**
  - B.E. in CSE from Univ. of Sci. & Tech. of China
  - PhD in CS from Princeton University
  - Associate Research Professor at ECE
- **Research**
  - Applying formal methods to analyze systems, and to build provably secure software systems
- **Courses**
  - 14-741/18-631 Intro to Info Security
  - 14-828/18-636 Browser Security
  - 18240 Structure and Design of Digital Systems

Hanan Hibshi (Units 2, 3, 5, 6)

- **Brief Bio**
  - B.S. in CS, KAU, Saudi Arabia
  - INI alumna, MSISTM (now MSIS)
  - PhD in Societal Computing, SCS@CMU
  - Assistant Teaching Professor at the INI
- **Research**
  - Usable security and privacy
  - Cybersecurity education
  - Security decision-support and Security Requirement Engineering
- **Courses**
  - 14-741/18-631 Intro to Info Security
  - 14-828/18-636 Browser Security
  - 14-735 Secure Coding

Contact Info
hhibshi@cmu.edu

ini
Carnegie Mellon University
Information Networking Institute

CyLab
Security and Privacy Institute

Today's agenda

- Introductions
- Syllabus overview
- Course objectives
- Course overview
- Course policies

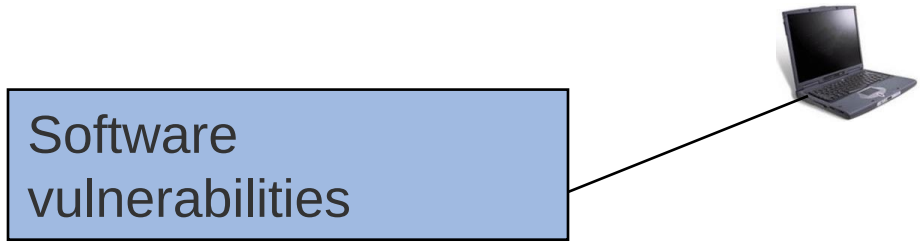
- What is security

Syllabus overview

- **Four major themes, grouped in six scheduling units:**
  - Foundations & crypto (Units 1 and 2)
  - Software security (Unit 3)
  - Network and web security (Unit 4)
  - Crypto applications (Unit 5)
  - Human and socio-economic factors (Unit 6)

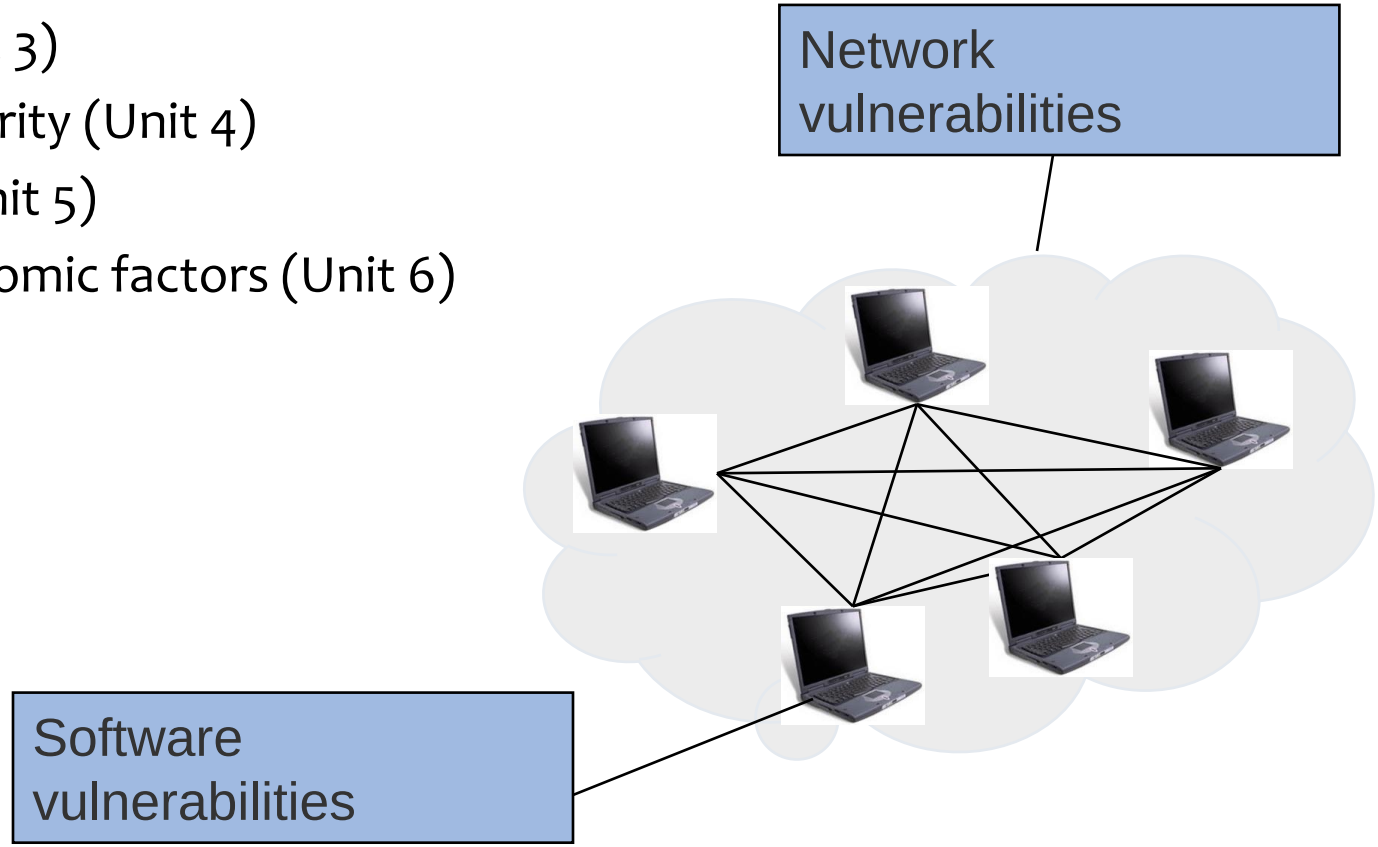
Syllabus overview

- **Four major themes, grouped in six scheduling units:**
  - Foundations & crypto (Units 1 and 2)
  - Software security (Unit 3)
  - Network and web security (Unit 4)
  - Crypto applications (Unit 5)
  - Human and socio-economic factors (Unit 6)



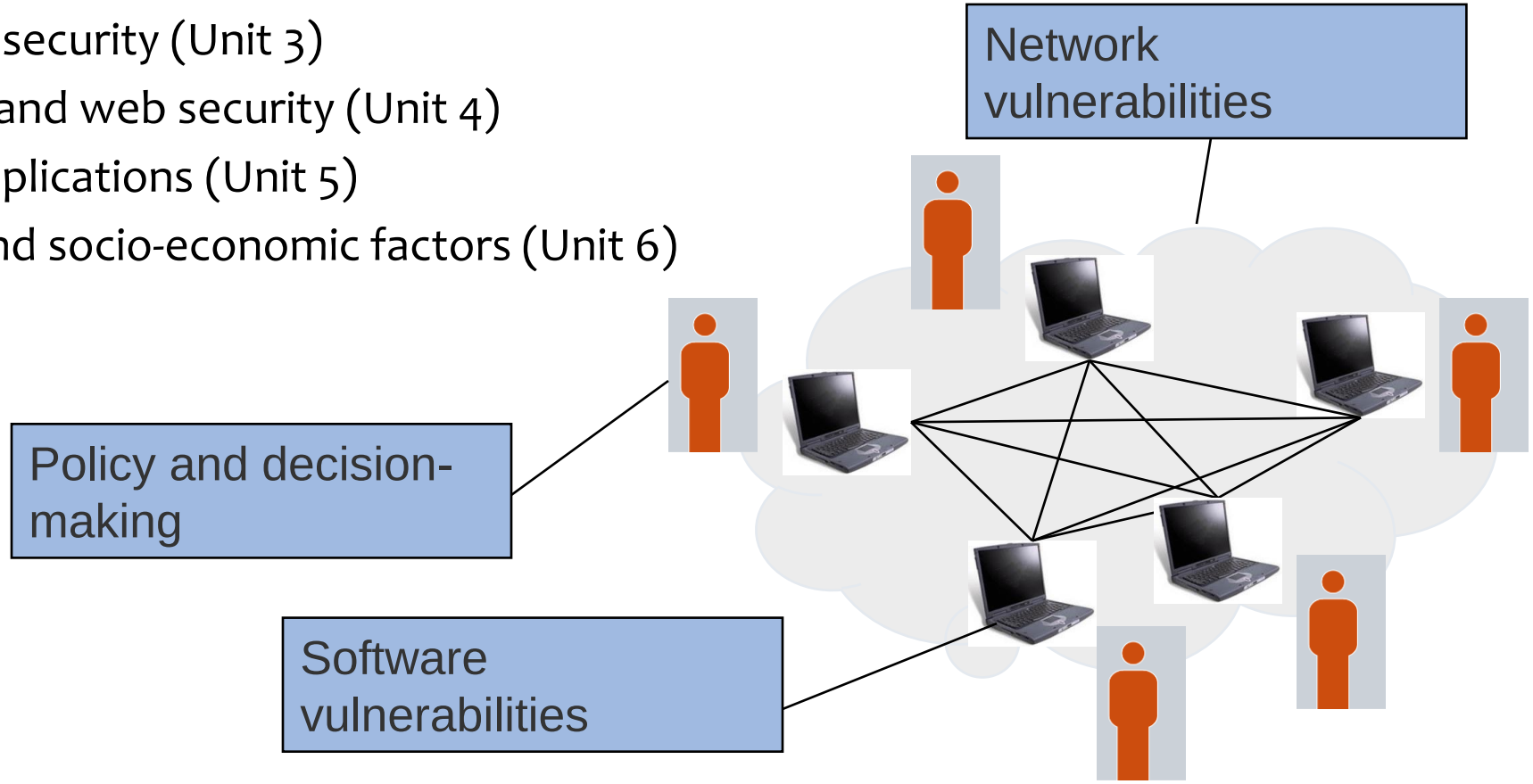
Syllabus overview

- **Four major themes, grouped in six scheduling units:**
  - Foundations & crypto (Units 1 and 2)
  - Software security (Unit 3)
  - Network and web security (Unit 4)
  - Crypto applications (Unit 5)
  - Human and socio-economic factors (Unit 6)



Syllabus overview

- **Four major themes, grouped in six scheduling units:**
  - Foundations & crypto (Units 1 and 2)
  - Software security (Unit 3)
  - Network and web security (Unit 4)
  - Crypto applications (Unit 5)
  - Human and socio-economic factors (Unit 6)



Course objectives

- **Provide a good understanding of security concerns in information systems**
  - Host level — Software vulnerabilities and defenses
  - Network level — Network vulnerabilities
  - Societal level — Policy and decision-making
- **Provide necessary background for more advanced security courses and electives**
  - Network security
  - Security for software engineers/systems
  - Security architecture and analysis
  - Privacy courses

More on course objectives

- **By the time you complete this course, you should be able to…**
  - Analyze security requirements of a system
  - Judge merit of security solutions

Boss: I want to go into mobile banking business!

Boss: PureNoise is selling us their security solutions: "Uses 128 rounds of a ridiculously strong 3072 bit paranoid encryption that far exceeds even military standards!"

Further more on course objectives

- **By the time you complete this course, you should be able to…**
  - Identify problems within context and find solutions

Boss: I want to go into mobile banking business!

  - Explain and discuss topics related to security
    - At work: to your team members and manager
    - After work: to your friends and family
      - What about this ransomware thing that is everywhere, should I be worried?
  - Engage in life-long learning process

Expectations

- **Two distinct components: theory + practice**
  - Lectures: high-level concepts
  - Assignments: hands-on exercises
  - Tests are on concepts covered in lectures
  - Recitations cover some of tools/practical skills needed for assignments
- **Less hand-holding than undergrad class**
  - We will try the best we can to accommodate everyone with different background
  - Expect students to learn on their own and search for resources to resolve issues
    - Remember to cite resources!

How to do well in this class

- **Not all about getting "A"s**
- **Knowledge**
  - Easy to read up and know the facts
- **Know how to apply knowledge and your analytical skills to solve problems**
  - Hard, but necessary to be successful later in your career
- **If you can do both well, you are guaranteed to get an "A"**
- **To do well in the class**
  - Aim for understanding the problem and the solution
  - Blindly pattern matching texts on the slides to answer exam questions is a very bad idea
  - Requires some background in linux and programming
    - Additional learning is needed if you lack this background
- **Time and stress management (university resources on syllabus)**

Course overview: instructors and TAs

- **Instructor**

Section	**Units 1,2,4,5**	**Units 2,3,5,6**
name	Limin Jia	Hanan Hibshi
Office hour	On canvas zoom	On canvas zoom
Office	CIC 2216	INI 123
email	liminjia@andrew	hhibshi@andrew

- **Teaching assistants**
  - 10 TAs (information on syllabus)
  - Grade assignments, answer questions, hold office hours, and recitations
- **Meeting time:**
  - Section A/SV: T/Th 3:05 pm Eastern Time
  - Section B/C: T/Th 10:10 am Eastern Time
- **Recitation on Fridays :**
  - Section A/SV: 3:35pm Eastern Time
  - Section B/C: 12:20pm Eastern Time

Course overview: resources

- **Websites**
  - Canvas: https://canvas.cmu.edu/
  - Piazza: https://piazza.com/cmu/fall2021/1474118631
  - Gradescope: https://www.gradescope.com/

- **Optional textbooks**
  - Security Engineering: A Guide to Building Dependable Systems, by Ross J. Anderson
  - Cryptography & Network Security: Principles and Practices, by William Stallings
  - The Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
  - Computer Security: A Hands-On Approach, by Wenliang Du.
  - Computer Security: Art and Science, by Matt Bishop.

Course overview: grades

- **Grading (more on later slides)**
  - Participation (quizzes) 10%
  - Homework assignments 50%
  - Midterm 20%
  - Final 20%

Course policies: Late submissions

- **Homework must be turned in by earliest class time (1:30PM Eastern) on the due date**
- **Three grace days for the entire semester**
  - You can use each grace day at your convenience to extend a homework deadline by 24 hours
  - Automatically deducted based on the timestamp of your submission
- **When you run out of grace days, you incur a penalty of 25% per day your homework is late**
- **We will not accept homework more than three days late**

Course policies: Plagiarism

- **Homework assignments**
  - Your fellow students are your best resource for advice, discussions…
  - But all solutions presented must be your own work
  - Don't copy from any source (web, other students, …)
  - Short citations are ok, if properly quoted and referenced
- **Tests**
  - No collaboration of any kind is allowed
  - Laptops and cell phones can't be used (if in class, we may administer tests over gradescope)
  - Books, research papers are allowed in exams
- **Cheating will be dealt with in the severest manner**
  - Don't do it: you will get caught and it is not worth it

Talk to us (instructor or TAs) if you are unsure whether a form of collaboration is appropriate

What is high-level discussion

- **Mentioning/explaining GENERAL syntax.**
  - For example, how to "pipe" between C and python
- **Explaining general Unix/Linux commands**
- **How to install software, get it to work, etc.**
- **Mentioning/explaining a good tool for debugging**
- **Explaining the content from the book/lecture**
- **Providing websites for tutorials or general information that would enhance everyone understanding**
- **Sharing hints that originally came from TAs**
- **TAs share hints in recitations, office hours or piazza**

What is NOT high-level discussion

- Sharing code to be used for the solution
- Sharing detailed “how to’s” for solutions
- Providing specific details about what to write and what to change in the code
- Looking at each other’s code (in-person, online, etc.)
- Discussing solutions to the specific syntax level

Course policies: Other

- **Materials are copyrighted, please do not upload them or redistribute them without instructor's permission**
- **Turn off or silence your phones (and other alarms)**
  - We will subtract points!
- **Please read the syllabus!**

Class format: lecture

Pre-lecture:

- **For most lectures:**
  - Approx 20-page reading assignment (on average)
- **For some lectures:**
  - Short instruction video and canvas quiz to complete

Class time:

- Active participation is expected

Class format: assignments

- **Eight homework assignments (labs/problem sets)**
  - Deposit electronic version in Gradescope
  - PDF only: Use andrewid-hw-n.pdf (e.g. liminjia-hw-1.pdf)
  - Each problem should begin on a new page
  - More on canvas
- **3 grace days that you can take for any assignments**
- **50% of your total grade**

Class format: tests

- **Midterm: 20% of your grade**
- **Final exam: 20% of your grade**

Class format: quiz

- **Associated with specific lecture activities**
- **Offline quiz**
  - Can be taken on canvas offline during a time window of a couple of days
  - Typically, graded for completion, not correctness
- **Online quiz**
  - Must be taken during class time
- **The participation grade (10%) depends on these quizzes**
- **Allowed to miss 2 quizzes without incurring penalty to your grade**

Recitation

- **On Fridays (start on Sept. 17th after the first homework is out)**
- **TAs will discuss material/questions related to homework**
- **Will be recorded**
- **Most times TAs will lead the recitation from CIC1201**
- **In-person attendance for recitations is optional**
- **Time conflict**
  - Due to space constraints, please do not physically attend the section that you did not register for
  - Please use the recording instead

Office hours

- **Each OH lasts 2 hour**
- **5 sessions per week**
- **Some will be over zoom**
  - Guidelines on the zoom OH on canvas
  - 3 TAs are in silicon valley campus
- **Some will be in person**

Optional homework teams

- **Goal:**
  - get to know your classmates,
  - have someone to bounce ideas off while working on homework assignments
- **Team assignment:**
  - Up to you (e.g., via piazza)
- **Team work expected:**
  - Only on problems explicitly marked at "team assignment"
  - Still must write your own answer/code for each homework assignment
  - Can discuss with team member
  - In the write up, each team list all members.
    - If two students' answers look the same, but no team members are listed, will be processed as academic violation

Security

What is security?

- “Building systems to remain dependable in the face of malice, error or mischance” (Ross Anderson)
- “Ensuring systems operate properly and remain secure from outside intrusion” (US Air Force)
- “The state or process of protecting and recovering networks, devices and programs from any type of cyberattack.” (Norton)
- “A set of techniques used to protect the integrity of an organization’s security architecture and safeguard its data against attack, damage or unauthorized access.” (Palo Alto Networks)

Security properties and objectives

- Confidentiality, privacy, secrecy
- Integrity
- Availability
- …(more in lecture 3)

Security analysis

- **Consider computer systems at your doctor's office**
- **What is the target system?**
  - Enumerate assets and their value
  - Operating value, replacement cost
- **Who are the adversaries?**
  - Identify attackers
  - Estimate attacker's resources
  - Probability of attack (risk assessment)
- **What are the security requirements?**
  - Confidentiality? Integrity? Authenticity?
- **What security approaches are effective?**
  - Technological effectiveness vs. cost effectiveness

Approaches to security

- **Social norms**
  - We don't go around killing other people b/c we know it is not socially acceptable behavior
- **Legal enforcement**
  - We don't go around killing other people b/c we don't want to rot in jail for the rest of our lives
- **Economics**
  - Make the attack too costly to carry out
  - Not necessarily just monetary costs

Technological approaches

- **There will always be bad people around, keeping the bad people at bay**
- **Strong lines of defense**
  - Cryptography, firewall
- **Redundancy**
  - Approach taken by Internet routing mechanisms
  - Multiple paths to same destination – makes it much harder for an attacker to prevent communication
- **Detection**
  - Can be used as a feed to legal system
- **Preemptive strike**
  - E.g., Peer-to-peer file sharing network poisoning
- **Recovery**
  - Back-ups, insurance

Security engineering

- **“Security is a process, not a product” (Schneier)**
  - Not something you can buy
    - Be wary of security consultants
    - Even though some of you may later choose that line of work
  - Something you have to build/engineer into a system
  - Preferably at system design time
    - Retrofitting security usually produces poor results
    - See: most operating systems, the Internet…

How to become a security engineer?

- **"We're in here talking about practice […] practice […] practice […] practice […] practice […] practice […] practice […]" (Allen Iverson, who didn't realize he was talking about security engineering)**
- **You don't become a security expert by taking a class or getting a certification (CISSP or other)**
  - Although hopefully this class will help get you started on the right track
- **You become a security expert by living, breathing and thinking about security all the time**

[From http://blogs.technet.com/h/rhalbheer/archive/2011/01/14/real-physical-security.aspx]

"An impressive résumé, General, but remember—department-store security is different from national security."

Published in: New Yorker (8/15/1993)

Takeaways

- **Security: important but difficult**
- **"Security" is not absolute**
  - Attacker
  - Properties
  - Cost
- **Security is about managing risk in the presence of an adversary**

Next time

- **Read "Why Cryptosystems Fail"**
- **If you don't have access to Canvas**
  - Google the paper title to download a copy
  - Google "STRIDE analysis" to read about that