Why do we want to study Security?

- It is important
- There is never a dull day!
- It is fun!

Security is Important

- An increasing part of our business, social, and personal life involves internet-connected computer systems
  - Web, email, social networks, entertainment, . . .
  - Mobile computing
  - Cyber-physical systems
  - Internet of things
- Protecting the security and privacy of our digital interactions is critical
  - Most of them involve networked systems and applications
There is never a dull day!

- Every day, we hear news of yet another high-profile hack, data theft, etc.
- New vulnerabilities surface all the time, and we have to find new solutions
- High-stakes game where attackers and defenders innovate constantly in order to stay ahead of each other
An Unprecedented Look at Stuxnet, the World’s First Digital Weapon

How A Coffee Machine Infected Factory Computers with Ransomware

It’s no surprise that the Internet of Things (IoT) devices are highly vulnerable to cyber attacks but who would know a time would come when these devices will become a security threat to institutions?

A few months ago researchers exposed life threatening vulnerabilities in IoT (Industrial Internet of Things) devices specifically industrial robots. In their findings, robots could be hacked, but in this case, the threat was severe.

Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

But the deeper aspects of your personality remain hard to detect.
System Security: It is fun!

- System security brings together all of the fun CS topics we have learned through other courses
  - Architecture
  - Operating Systems
  - Networks
  - Compilers and Programming Languages
  - Algorithms
  - AI

- System security helps us make connections between these topics, helping us to understand them and remember them better.
**What is security**

**Wikipedia:**
Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.

---

**What is computer security?**

- **Everyone has their own definition**
  - No single one is perfect
- **Computer security deals with protecting data, programs, and systems against intelligent adversaries.**
- **Safety vs Security**
  - What's the difference between the two?
  - Do they interact?

---

**CIA**

Security is about CIA

**Confidentiality:** Keeping data and resources hidden or protected from unauthorized disclosure

**Integrity:** Data and Programs are modified in specified and authorized ways. Data integrity and origin integrity.

**Availability:** Systems and networks are available for use by legitimate users
Why is it hard?

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
- Implementations are buggy
  - Buffer overflows have been the “vulnerability of the decade” for multiple decades!
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
  - Phishing, social engineering, etc.

Why is it hard?

- It is hard to get security right because:
  - Security is hard to test for
    - Testing correctness versus security
  - It requires a deep understanding of all technologies involved in the design and implementation of a system
    - Really hard in large real systems
  - Users are typically the weakest link
  - Asymmetry between attack and defense

Course Focus

- Introduction to a wide range of topics in computer system and software security
  - vulnerabilities, exploit and mitigation techniques
  - malware trends and defenses against untrusted code
  - binary analysis, reverse engineering and forensics
  - software vulnerability scanning techniques and tools
- Cultivate the “security mindset”
  - Understand the modus operandi of attackers: find vulnerabilities, subvert protections, bypass defenses, ... 
- Hands-on assignments in exploit development and mitigation
- Get a taste of security research through a project (may be optional)
Ethics and Legal Considerations

- Play Fair
- Cannot teach defense without offense, but:

**Breaking into systems is illegal!**
**Unauthorized data access is illegal!**

- Computer Fraud and Abuse Act (CFAA)
- Practice on your own systems or controlled environment
- Scanning/penetration testing/etc. of third-party systems may be allowed only after getting permission by their owner

Course Logistics

- Lectures: Mon/Wed: 4:00PM to 5:20PM
- Grade breakdown (subject to some changes):
  - 10 to 12% Homework quizzes (scaled up by 33
  - 20 to 30% Mid-term exam(s)
  - 20 to 30% Programming projects
  - 30 to 35% Final exam
- Blackboard will be used for assignments and grading
- Piazza for discussions
- Static information on the course web page:
  [http://seclab.cs.stonybrook.edu/sekar/cse509](http://seclab.cs.stonybrook.edu/sekar/cse509)

Code of Conduct

- The work that you present as your own *should be your own*
- Cite the resources that you used (other people’s code, documents, etc.)
- Don’t allow your code/paper summaries to be copied
- Don’t copy other people’s code or paper summaries
- Anything short of the above, will be grounds for immediate “F” grade and further disciplinary action
Some slide contents in this lecture and future ones are courtesy of Nick Nikiforakis and Michalis Polychronakis