Today’s agenda

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

- What is security
Course overview: Introductions

- **Instructor**
  
  Limin Jia

  Thursday 3:00-4:00pm or by appt.

  CIC 2216

  liminjia@cmu.edu

- **Teaching assistants**
  
  - 3 PhD TAs, 3 MS TAs
  - Grade assignments, answer questions, hold office hours

- **Websites**
  
  https://www.cmu.edu/blackboard/  
  https://piazza.com/cmu/fall2015/1474118631

- **Meeting time:**
  
  - PIT M/W 2:30pm Eastern Time CIC 1201 (SV B23 212)
Course overview: Textbook and grades

- **Optional textbooks**
  - The Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone

- **Grading**
  - Homework assignments 25%
  - Midterm (in class) 25%
  - Final exam (in class) 40%
  - Class participation (Quality vs. quantity) 5%
  - Reading critiques 5%
    - Reading critiques counted, and randomly sampled for grading
Homework must be turned in by class time on the due date

Two grace credits for the entire semester
- You can use each grace credit at your convenience to extend a homework deadline by 24 hours

When you run out of grace credits, you incur a penalty of 25% per day your homework is late

We will not accept homework late by more than three days
Course policies: Plagiarism

- **Homework assignments (including reading critiques)**
  - 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

- **In-class exams or quizzes**
  - No collaboration of any kind is allowed
  - Books, research papers are allowed
  - Laptops and cell phones can’t be used

- **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
Course policies: Other

- Please turn off/mute your cell phones (or put them on vibrate – and don’t pick up!)
  - Penalty on participation grade for frequent offenders (see handout)

- Laptops OK, but
  - Please refrain from reading the news, being on Facebook, or checking email in class
  - Even though it may not necessarily disrupt the lecture, it is rude!
  - You probably do not need to have your laptop with you in class
  - Please avoid using backchannels (Twitter, IRC, instant messaging) with other students
  - Instead, share your comments with the rest of the class

- Materials are copyrighted, please do not upload them or redistribute them without instructor’s permission
Class format

- **For each lecture**
  - Approx 20-page reading assignment (on average), hand in summary before lecture
  - Deposit electronic version in Assignments prior to the start of the lecture
  - PDF only
  - Use andrewid-date.pdf (e.g. liminjia-0825.pdf)
  - Active participation is expected
    - Please do ask questions and make constructive comments during lectures…
    - You participation grade depends on it
  - Be on time! (important announcements are made at beginning of lecture)
  - Slides available on Blackboard; usually after the lecture (because I make extensive use of annotations), but policy may change over the semester

- **Four homework assignments (labs/problem sets)**
  - Deposit electronic version in Assignments (BB) prior to the start of the lecture
  - PDF only
  - Use andrewid-hw-n.pdf (e.g. liminjia-hw-1.pdf)

- **1 in-class midterm**

- **1 in-class final exam**

- **We reserve the right to have some random quizzes**
  - Which wouldn’t count for much, to be honest – they would be included in the participation grade
Objectives

Make sure you read the required readings
Make you think about the material

Please keep reading critique short (1 page or less)
Summarize the paper in 2-3 sentences
Identify the three points you think are the most important and valid in the paper (say why)

DO NOT PARAPHRASE THE PAPER, have a critical, independent view

“Property A that the paper describes is important, because another study (Y) has shown that systems satisfying A are more resilient to spoofing” (Good!)

“Property B is important for securing the system” (WHY???)

“The paper is well written which makes it easy to read for me” (WEAK - argue on the contents, not the form)

Identify one point that you either
disagree with (say why), or that
you would like to have seen addressed in the paper (say why)
Four major themes, grouped in five scheduling units:

- Foundations & crypto (Units 1 and 2)
- Host security (Unit 3)
- Communications/network security (Unit 4)
- Human and socio-economic factors (Unit 5)
Four major themes, grouped in five scheduling units:

- Foundations & crypto (Units 1 and 2)
- Host security (Unit 3)
- Communications/network security (Unit 4)
- Human and socio-economic factors (Unit 5)
Four major themes, grouped in five scheduling units:

- Foundations & crypto (Units 1 and 2)
- Host security (Unit 3)
- Communications/network security (Unit 4)
- Human and socio-economic factors (Unit 5)
Syllabus overview

- Four major themes, grouped in five scheduling units:
  - Foundations & crypto (Units 1 and 2)
  - host security (Unit 3)
  - communications/network security (Unit 4)
  - human and socio-economic factors (Unit 5)
# Tentative schedule

<table>
<thead>
<tr>
<th>Unit</th>
<th>Date</th>
<th>Topic</th>
<th>Readings</th>
<th>Homeworks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mon, Aug 31</td>
<td>Introduction</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Sep 2</td>
<td>Threat models</td>
<td>Anderson(*)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Sep 7</td>
<td>Labor day: no class</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Sep 9</td>
<td>Physical security (Guest lecture)</td>
<td>Tobias</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Sep 14</td>
<td>Basic security properties</td>
<td>HAC Chapter 1 (1.1, 1.2, 1.4, 1.6, 1.7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Sep 16</td>
<td>Basic policy overview</td>
<td>Anderson chap. 24</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit 1: Foundations</td>
<td>Mon, Sep 21</td>
<td>Cryptography I: history, private key algorithms</td>
<td>HAC Chapter 1 (everything), Stallings chapter 2 and 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Sep 23</td>
<td>Cryptography II: public key algorithms</td>
<td>Stallings chapter 9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Sep 28</td>
<td>Cryptography III: unkeyed algorithms, hashes</td>
<td>Lamport (*)</td>
<td>HW1 out</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Sep 30</td>
<td>PKI</td>
<td>KPS chap. 15, PGP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit 2: Cryptography basics</td>
<td>Mon, Oct 5</td>
<td>Access control I: Operating Systems</td>
<td>Saltzer-Schroeder(*)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Oct 7</td>
<td>Access control II: Multilevel and multilateral security</td>
<td>Anderson chap. 8 and 9</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Oct 12</td>
<td>Buffer overflows/basic software vulnerabilities</td>
<td>AlephOne, Cowan</td>
<td>HW1 due</td>
</tr>
<tr>
<td></td>
<td>Wed, Oct 14</td>
<td>Software/hardware issues (TCG, Rowhammer)</td>
<td>Parno et al., Kim et al.(*)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Oct 19</td>
<td>Midterm review</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Oct 21</td>
<td>MIDTERM EXAM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Oct 26</td>
<td>Security protocols</td>
<td>Abadi-Needham</td>
<td>HW2 out</td>
</tr>
<tr>
<td></td>
<td>Wed, Oct 28</td>
<td>Security protocols (cont'd), SSL</td>
<td>Anderson-Needham(*)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Nov 2</td>
<td>Networks I: TCP vulnerabilities</td>
<td>TBD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Nov 4</td>
<td>Networks II: DDoS attacks</td>
<td>Mirkovic-Reiher refs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Nov 9</td>
<td>Web security</td>
<td>TBD</td>
<td>HW2 due, HW3 out</td>
</tr>
<tr>
<td></td>
<td>Wed, Nov 11</td>
<td>Networks III: Anonymity</td>
<td>Dingledine(*), Chaum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Nov 16</td>
<td>Cryptocurrencies</td>
<td>Nakamoto, Bonneau et al. (*)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Nov 18</td>
<td>Security economics / psychological aspects</td>
<td>CEVG (*)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Nov 23</td>
<td>Online crime</td>
<td>Thomas et al.</td>
<td>HW3 due, HW4 out</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Nov 25</td>
<td>Thanksgiving, no class</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Nov 30</td>
<td>Usable security</td>
<td>WT(*)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wed, Dec 2</td>
<td>Management and assurance</td>
<td>Anderson chap. 22 and 23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mon, Dec 7</td>
<td>Final review</td>
<td></td>
<td>HW4 due</td>
</tr>
<tr>
<td></td>
<td>Wed, Dec 9</td>
<td>FINAL EXAM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 in the INI/ECE programs
  - 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
Sample security statements

- PureNoise
  “Uses 128 rounds of a ridiculously strong 3072 bit paranoid encryption that far exceeds even military standards!”

- ICS
  - “99.99% of the people out there use math to encode and they use math to 'break' the code. Since we don't really use math, it would be quite hard to break.”
  - “Tree Encoded Files Can Be ‘Zipped.’”
Both landed in Bruce Schneier’s Crypto-gram’s Doghouse column (http://www.schneier.com/crypto-gram.html)

- PureNoise in March 2003
  - Larger keys/number of rounds are not necessary indicative of better security (and in fact, rarely are, when used as advertisement material)
- ICS in July 2004
  - Encryption is really nothing more than a mathematical transform applied to text; hard to do “without math”
  - Properly encrypted file would actually be very random, and, as a result, would be quite hard to compress
  - Side note: this “company” doesn’t even exist anymore
  - Optionally, read Schneier’s full commentary – it’s really a treat
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
What is security?

- “Building systems to remain dependable in the face of malice, error or mischance” (Ross Anderson)
- “Managing a malicious adversary [and] guaranteeing properties even if a malicious adversary tries to attack” (Adrian Perrig)
Security properties and objectives

- Confidentiality, privacy
- Integrity
- Authentication, identification
  (entity authentication vs. message authentication)
- Anonymity
- Certification
- Non-repudiation
- Timestamping
Security analysis

- What is the target system?
  - Enumerate assets and their value
  - Operating value, replacement cost

- Who are the adversaries?
  - Identify attackers
  - Estimate attackers 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 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 [...]” (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
Takeaways

- Security: important but difficult
- “Security” is not absolute
  - Attacker
  - Properties
  - Cost
- Security is about managing risk in the presence of an adversary
Getting immersed in security

- **Mailing lists**
  - CERT mailing lists
    - [https://www.us-cert.gov/cas/signup.html](https://www.us-cert.gov/cas/signup.html)
  - Bugtraq ([http://online.securityfocus.com/](http://online.securityfocus.com/))
    - You can sign up for their mailing list at [http://online.securityfocus.com/archive](http://online.securityfocus.com/archive)
  - Dave Farber’s Interesting People list at [http://www.interesting-people.org](http://www.interesting-people.org)

- **Blogs**
  - Freedom to Tinker (Ed Felten’s blog on technology and policy) [http://www.freedom-to-tinker.com](http://www.freedom-to-tinker.com)
  - Declan McCullagh’s Politech list at [http://www.politechbot.com](http://www.politechbot.com)

- **Twitter is also a good source of pointers**
Next time

- Read “Why Cryptosystems Fail”
- Reading critiques are required
- If you don’t have access to blackboard
  - Download paper at
  - http://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf