**Course Syllabus**

**18-631/14-741:** *Introduction to Information Security*

**Fall 2018**

**Instructor (Section A):** Limin Jia

**Office Location:** CIC 2216

**Email Address:** liminjia@cmu.edu

**Office Hours:** TBA

**Instructor (Section B/SV):** Martin Carlisle

**Office Location:** 4616 Henry 125

**Email Address:** carlislem@cmu.edu

**Office Hours:** TBA

**Teaching Assistants: Darion Cassel**

darionc@andrew.cmu.edu

**Era Vuksani**

evuksani@andrew.cmu.edu

**Rintaro Fujita**

frintaro@andrew.cmu.edu

**Irene Lin**

iwl@andrew.cmu.edu

**Jason Yu**

jyu@cmu.edu

**Rongzhi Wan**

rwan@andrew.cmu.edu

**Wai Tuck Wong**

waituck@cmu.edu

**Xinchen Wang**

xinchenw@andrew.cmu.edu

**Office Hours:** See piazza (Resources -> Staff)

**Course Management Assistant:** Michelle Mahouski

**Email Address:** mmahousk@andrew.cmu.edu

**Office Location**: HH 1112

**Course Canvas:** <https://cmu.instructure.com/>

**Class Lecture:**

*Section A Monday and Wednesday, 7:30pm – 8:50pm* CIC 1201

*Section B Monday and Wednesday, 2:30pm – 3:50pm* CIC 1201

*Section SV* *Monday and Wednesday, 11:30am – 12:50pm* B23 212

**Optional Textbooks:**

This course does not have a required textbook. The following books are useful references, especially the ﬁrst book:

*Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd edition, by Ross Anderson. Publisher: John Wiley and Sons (2008), New York

*(ISBN: 0-470-06852-3).*

Also available for free online at: <http://www.cl.cam.ac.uk/~rja14/book.html>

*Computer Security: A Hands-On Approach*, by Wenliang Du. Publisher: CreateSpace (2017). (*ISBN-13: 978-1548367947)*

*Computer Security: Art and Science*, 2nd edition, by Matt Bishop. Publisher: Addison Wesley (2018), *(ISBN: 0321712331)*

*Cryptography and Network Security: Principles and Practice*, 6th edition, by William Stallings. Publisher: Prentice Hall (2013), New Jersey *(ISBN: 0133354695)*

*The Handbook of Applied Cryptography*, by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone Publisher: CRC Press (1996) *(ISBN: 0849385237)*.

Also available for free online: <http://www.cacr.math.uwaterloo.ca/hac/>.

**Take Care of Yourself:**

Do your best to maintain a healthy lifestyle this semester by eating well, exercising, avoiding drugs and alcohol, getting enough sleep and taking some time to relax. This will help you achieve your goals and cope with stress.

All of us benefit from support during times of struggle. You are not alone. There are many helpful resources available on campus and an important part of the college experience is learning how to ask for help. Asking for support sooner rather than later is often helpful.

If you or anyone you know experiences any academic stress, difficult life events, or feelings like anxiety or depression, we strongly encourage you to seek support. Counseling and Psychological Services (CaPS) is here to help: call 412-268-2922 and visit their website at http://www.cmu.edu/counseling/. Consider reaching out to a friend, faculty or family member you trust for help getting connected to the support that can help.

**Course Description:**

Our growing reliance on information systems for daily activities, ranging from remote communications to financial exchanges, has made information security a central issue of our critical infrastructure. The course introduces the technical and policy foundations of information security. The main objective of the course is to enable students to reason about information systems from a security engineering perspective, taking into account technical, economic and policy factors. Topics covered in the course include elementary cryptography; access control; common software vulnerabilities; common network vulnerabilities; policy and export control laws, in the U.S., Japan, and elsewhere; privacy; management and assurance; economics of security; and special topics in information security. Prerequisites: The course assumes a basic working knowledge of computers, networks, C and UNIX programming, as well as an elementary mathematics background, but does not assume any prior exposure to topics in computer or communications security. Students lacking technical background (e.g., students without any prior exposure to programming) are expected to catch up through self-study.

**Number of Units:** 12

**Graduate Course Area:** Software Systems and Computer Networking

**Course Wiki:**

Students are encouraged to use the ECE wiki to provide feedback about the course at:

<http://wiki.ece.cmu.edu/index.php>.

**Course Objectives**:

This course primarily aims at providing a level of literacy in information security adequate enough to understand the security implications on a number of diverse domains including software engineering; networking; privacy; and policy.

A secondary objective is to provide a working knowledge of topics such as cryptography, privacy, network security, and infrastructure management, so that students can acquire the necessary background for more advanced security courses.

By the end of this course, students will be able to reason about systems from the perspective of a security engineer. That is, they should be able to deﬁne the system to protect; determine the security properties that are desired for this system; identify the possible threats to these security properties, and their likelihood of occurrence; and consider possible mitigations against these threats.

More specifically, the course will fulfill the following education objectives in relationship to the program objectives.

1. *Technical skills in building secure information systems.*  
   Students will be able to apply abstract mathematical and scientific concepts such as cryptography to enforce security properties. Students will be able to use concrete engineering techniques and tools such as state of the art security mechanisms, defenses and tools to build secure systems.
2. *Technical skills in analyzing security of information systems.*  
   Students will be able to design and conduct experiments, as well as to analyze and interpret data to infer security threats and effectiveness of possible mitigations.
3. *Analytical and creative skills in identifying problems within context and find solutions.*
4. Students will be able to design a system, component, or process to meet desired security requirements within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability.
5. Students will be able to identify, formulate, and solve simple security issues in modern computer and information systems.
6. Students will be able to understand the impact of engineering solutions in a global, economic, environmental, and societal context. Students will be able to see how information security is not only an engineering necessity, but how it affects non-technical fields, such as management and risk analysis.
7. Student will gain knowledge of contemporary issues and will be aware of the current pressing information security challenges.
8. *Skills in functioning within a larger work environment.*
9. Students will be able to converse about security issues both with engineering teams and with management to function on multi-disciplinary teams.
10. Students will be exposed to ethical and legal ramifications of information security to obtain an understanding of professional and ethical responsibility.
11. Students will be able to develop principled arguments to justify secure system design so they can communicate effectively to future team members, managements, and clients.
12. *Recognition for the need for, and an ability to engage in life-long learning.*

Students will be equipped with fundamental knowledge that will allow them to further their study of information security and adapt to the frequently changing information security landscape, independent of the specific tools in use.

**Grading:**

|  |  |
| --- | --- |
| 35% | Homework |
| 25% | Midterm Exam |
| 40% | Final Exam |

Class participation is measured by both frequency and pertinence of the insights. That is someone who constantly makes trivial remarks would not necessarily get higher marks than somebody who more infrequently makes a judicious observation or asks insightful questions.

Quizzes will be assigned at the beginning of class and will consist of a small set (no more than five) multiple choice questions on the reading(s) of the day. Not every class will have a quiz, and quizzes will not necessarily be on the same readings for both sections. The lowest grade from all quizzes will not be counted.

**Tentative Course Calendar:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Unit** | **A/B/SV** | **Class Activity** | **Readings** | **HW** |
| **1: Basics** | Mon, Aug 27 | 1: Classes Begin / Introduction | Thompson |  |
| Wed, Aug 29 | 2: Threat Models | Anderson  <https://www.scmagazine.com/feds-charge-14-with-making-atm-cashouts-appear-like-one/article/543295/>  <https://krebsonsecurity.com/2014/10/chip-pin-vs-chip-signature/>  <https://www.s21sec.com/en/blog/2017/01/alice-simplicity-for-atm-jackpotting/>  Abomhara et al (STRIDE) |  |
| Mon, Sep 3 | **Labor Day: No Class** | | |
| Wed, Sep 5 | 3: Basic Security Properties | [HAC Ch 1 (1.1, 1.2, 1.4, 1.6, 1.7)](http://cacr.uwaterloo.ca/hac/about/chap1.pdf) |  |
| **2: Cryptography** | Mon, Sep 10 | 1: Cryptography I: history, private key algorithms | [HAC Ch 1 (everything),](http://cacr.uwaterloo.ca/hac/about/chap1.pdf) Stallings Chapter 2 and 3 |  |
| Wed, Sep 12 | 2: Cryptography II: public key algorithms | Stallings Chapter 9  <https://eprint.iacr.org/2015/1018.pdf> | HW1 Out |
| Mon, Sep 17 | 3: Cryptography III: unkeyed algorithms, hashes | Lamport  <https://www.theregister.co.uk/2017/02/23/google_first_sha1_collision/> |  |
| Wed, Sep 19 | 4: Cryptography IV: PKI | KPS Ch. 15, PGP, <https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning> | Recitation on Sept. 21st |
| Mon, Sep 24 | 5: Basic Policy Overview | [Anderson Ch. 24](http://www.cl.cam.ac.uk/~rja14/book.html)  Keys Under the Doormats (sections 1 and 2) <https://dspace.mit.edu/handle/1721.1/97690>  History of crypto wars: <http://www.dailydot.com/layer8/encryption-crypto-wars-backdoors-timeline-security-privacy/> |  |
| **3: Software Security** | Wed, Sep 26 | 1: Access control I: Operating Systems | Saltzer-Schroeder | HW 1 Due HW 2 Out |
| Mon, Oct 1 | 2: Access control II: Multilevel and multilateral security | [Anderson Chapters 8 and 9](http://www.cl.cam.ac.uk/~rja14/book.html) |  |
| Wed, Oct 3 | 3: Buffer overflows/basic software vulnerabilities | AlephOne, Cowan |  |
| Mon, Oct 8 | 4: Software vulnerability defenses | Abadi et al, Shacham et al.  <https://crypto.stanford.edu/cs155/lectures/02a-ctrl-hijacking.pdf>  <https://www.blackhat.com/docs/us-15/materials/us-15-Yason-Understanding-The-Attack-Surface-And-Attack-Resilience-Of-Project-Spartans-New-EdgeHTML-Rendering-Engine-wp.pdf> (esp Section 4) |  |
| Wed, Oct 10 | 5: Software/hardware issues (TCG, Rowhammer) | Parno et al., Kim et al.  <https://media.blackhat.com/us-13/US-13-Butterworth-BIOS-Security-WP.pdf> | Recitation on Oct. 12 |
|  | Mon, Oct 15 | Midterm Review |  | HW2 Due |
|  | Wed, Oct 17 | MIDTERM EXAM |  |  |
| **4: Network and Web Security** | Mon, Oct 22 | 1: Security protocols | Abadi-Needham | HW 3 Out |
| Wed, Oct 24 | 2: Security protocols (cont'd), SSL | Anderson-Needham |  |
| Mon, Oct 29 | 3: Networks I: TCP vulnerabilities | Bellovin |  |
| Wed, Oct 31 | 4: Networks II: DDoS attacks | Mirkovic-Reiher |  |
| Mon, Nov 5 | 5: Networks III: Web security | OWASP  <https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29> |  |
| Wed, Nov 7 | 6: Networks IV: Anonymity | Dingledine, Chaum, Corrigan et al, Hooff et al. | Recitation on Nov. 9 |
| **5: Human Factors and Economics** | Mon, Nov 12 | 1: Cryptocurrencies | Nakamoto, Bonneau et al. | HW3 Due HW4 Out |
| Wed, Nov 14 | 2: Adversarial machine learning | <https://www.ece.cmu.edu/~lbauer/papers/2016/ccs2016-face-recognition.pdf> | Recitation on Nov. 16 |
| Mon, Nov 19 | 3: Security economics / psychological aspects | Herley (<http://www.nspw.org/papers/2009/nspw2009-herley.pdf>) |  |
| Wed, Nov 21 | **Thanksgiving Break; No Classes** |  |  |
| Mon, Nov 26 | 4: Online crime | Thomas et. Al |  |
| Wed, Nov 28 | 5: Usable security | Whitten-Tyger, Christin et al. | HW4 Due |
| Mon, Dec 3 | 6: Management and Assurance | Anderson Ch 22 & 23 |  |
|  | Wed, Dec 5 | Final review |  |  |
|  |  | **FINAL EXAM PERIOD** |  |  |

**Course Policies:**

*Language*

This course is entirely taught in English, and all materials submitted by the students, including homeworks, exams, assignments, and quizzes, must be submitted in English. In-class oral participation must also be in English.

**Please do not worry about making grammatical or vocabulary mistakes. We will never penalize you for using improper grammar or vocabulary, as long as your statements remain clear and unambiguous.**

Homeworks, quizzes or exams submitted in a language other than English will not be graded.

*Lectures*

We will not check attendance, but it is really in your best interest to attend each lecture. In-class participation is encouraged and expected (see “grading”). In other words, please do ask questions and make constructive comments during lectures.

*Auditors & Non-degree Students*

Auditors are expected to attend lectures, but cannot submit homeworks, hand in tests, or take exams. Auditors only get a record of audit at the end of the semester. On the other hand, non-degree students are subject to the same rules and expectations as degree students.

*Cell Phone and Wi-Fi*

Please remember to turn off or silence your phones (and other alarms) before each class meeting. We will subtract *i* points from your total grade the *i*-th time your phone/alarm/pager rings in class during the semester. No exceptions.

As a matter of courtesy to the instructor and other students, please refrain from reading the news, participating in social networks, or checking your email using your wi-ﬁ connection during lectures. It is most likely the case you do not need a laptop when you come to class.

*Late Homework Submission Policy*

For full credit, homeworks must be turned in by class time on the due date. You have two “grace days” that you can use at any time during the semester for late homework. That is, you can turn in a total of two homework assignments a day late (“a day late” is deﬁned as any delay between 0 and 24 hours after the deadline), one homework two days late, etc. You must notify the instructor and T.A.s prior to using (a) grace day(s). Assignments turned in late without “grace credit” will be penalized by 25% per day. Homework late by more than three days will not be graded. Exceptions require either prior arrangement or doctor-validated medical excuse.

*Collaboration Policy*

Students are encouraged to talk to each other, to the T.A.(s), to the instructor, or to anyone else about any of the homework assignments. **Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. Each student must write out his or her own solutions to the homeworks. Consulting another student’s solution is prohibited, and submitted solutions may not be copied from any source. These and any other form of collaboration on assignments constitute cheating.** Any form of collaboration is strictly prohibited on the exams and is considered cheating. If you have any question about whether some activity would constitute cheating, please feel free to ask.

Cheating on an assignment/exam will result in failure of the course, and the university administration (department, college) will be notiﬁed per the appropriate procedures.

Simply stated, feel free to discuss problems with each other, but do not cheat. It is not worth it, and you will get caught.

*Copyright Policy*

All teaching materials in this class, including course slides, homeworks, assignments, practice exams and quizzes, are copyrighted; reproduction, redistribution and other rights solely belong to the instructor (Limin Jia and Martin Carlisle). **In particular, it is not permissible to upload any or part of these materials to public or private websites without the instructor’s explicit consent.** Violating this copyright policy will be considered as an academic integrity violation, with the consequences discussed above.

Reading materials are also copyrighted by their respective publishers and cannot be reposted or distributed without prior authorization from the publisher.

**ECE Academic Integrity Policy   
(**<http://www.ece.cmu.edu/programs-admissions/masters/academic-integrity.html>)**:**

The Department of Electrical and Computer Engineering adheres to the academic integrity policies set forth by Carnegie Mellon University and by the College of Engineering. ECE students should review fully and carefully Carnegie Mellon University's policies regarding Cheating and Plagiarism; Undergraduate Academic Discipline; and Graduate Academic Discipline. ECE graduate student should further review the Penalties for Graduate Student Academic Integrity Violations in CIT outlined in the CIT Policy on Graduate Student Academic Integrity Violations. In addition to the above university and college-level policies, it is ECE's policy that an ECE graduate student may not drop a course in which a disciplinary action is assessed or pending without the course instructor's explicit approval. Further, an ECE course instructor may set his/her own course-specific academic integrity policies that do not conflict with university and college-level policies; course-specific policies should be made available to the students in writing in the first week of class.

*This policy applies, in all respects, to this course.*

**CMU Academic Integrity Policy (**<http://www.cmu.edu/academic-integrity/index.html>)**:**

In the midst of self exploration, the high demands of a challenging academic environment can create situations where some students have difficulty exercising good judgment. Academic challenges can provide many opportunities for high standards to evolve if students actively reflect on these challenges and if the community supports discussions to aid in this process. It is the responsibility of the entire community to establish and maintain the integrity of our university.

This site is offered as a comprehensive and accessible resource compiling and organizing the multitude of information pertaining to academic integrity that is available from across the university. These pages include practical information concerning policies, protocols and best practices as well as articulations of the institutional values from which the policies and protocols grew. The Carnegie Mellon Code, while not formally an honor code, serves as the foundation of these values and frames the expectations of our community with regard to personal integrity.

*This policy applies, in all respects, to this course.*

**The Carnegie Mellon Code**

Students at Carnegie Mellon, because they are members of an academic community dedicated to the achievement of excellence, are expected to meet the highest standards of personal, ethical and moral conduct possible.

These standards require personal integrity, a commitment to honesty without compromise, as well as truth without equivocation and a willingness to place the good of the community above the good of the self. Obligations once undertaken must be met, commitments kept.

As members of the Carnegie Mellon community, individuals are expected to uphold the standards of the community in addition to holding others accountable for said standards. It is rare that the life of a student in an academic community can be so private that it will not affect the community as a whole or that the above standards do not apply.

The discovery, advancement and communication of knowledge are not possible without a commitment to these standards. Creativity cannot exist without acknowledgment of the creativity of others. New knowledge cannot be developed without credit for prior knowledge. Without the ability to trust that these principles will be observed, an academic community cannot exist.

The commitment of its faculty, staff and students to these standards contributes to the high respect in which the Carnegie Mellon degree is held. Students must not destroy that respect by their failure to meet these standards. Students who cannot meet them should voluntarily withdraw from the university.

*This policy applies, in all respects, to this course.*

**Carnegie Mellon University's Policy on Cheating**   
(<http://www.cmu.edu/academic-integrity/cheating/index.html>) states the following:

According to the University Policy on Academic Integrity, cheating "occurs when a student avails her/himself of an unfair or disallowed advantage which includes but is not limited to:

* Theft of or unauthorized access to an exam, answer key or other graded work from previous course offerings.
* Use of an alternate, stand-in or proxy during an examination.
* Copying from the examination or work of another person or source.
* Submission or use of falsified data.
* Using false statements to obtain additional time or other accommodation.
* Falsification of academic credentials.”

*This policy applies, in all respects, to this course.*

**Carnegie Mellon University's Policy on Plagiarism**   
(<http://www.cmu.edu/academic-integrity/plagiarism/index.html>) states the following:

According to the University Policy on Academic Integrity, plagiarism "is defined as the use of work or concepts contributed by other individuals without proper attribution or citation. Unique ideas or materials taken from another source for either written or oral use must be fully acknowledged in academic work to be graded. Examples of sources expected to be referenced include but are not limited to:

* Text, either written or spoken, quoted directly or paraphrased.
* Graphic elements.
* Passages of music, existing either as sound or as notation.
* Mathematical proofs.
* Scientific data.
* Concepts or material derived from the work, published or unpublished, of another person."

*This policy applies, in all respects, to this course.*

**Carnegie Mellon University's Policy on Unauthorized Assistance** (<http://www.cmu.edu/academic-integrity/collaboration/index.html>) states the following:

According to the University Policy on Academic Integrity, unauthorized assistance "refers to the use of sources of support that have not been specifically authorized in this policy statement or by the course instructor(s) in the completion of academic work to be graded. Such sources of support may include but are not limited to advice or help provided by another individual, published or unpublished written sources, and electronic sources. Examples of unauthorized assistance include but are not limited to:

* Collaboration on any assignment beyond the standards authorized by this policy statement and the course instructor(s).
* Submission of work completed or edited in whole or in part by another person.
* Supplying or communicating unauthorized information or materials, including graded work and answer keys from previous course offerings, in any way to another student.
* Use of unauthorized information or materials, including graded work and answer keys from previous course offerings.
* Use of unauthorized devices.
* Submission for credit of previously completed graded work in a second course without first obtaining permission from the instructor(s) of the second course. In the case of concurrent courses, permission to submit the same work for credit in two courses must be obtained from the instructors of both courses."

*This policy applies, in all respects, to this course.*

**Carnegie Mellon University's Policy on Research Misconduct** (<http://www.cmu.edu/academic-integrity/research/index.html>) states the following:

According to the University Policy For Handling Alleged Misconduct In Research, “Carnegie Mellon University is responsible for the integrity of research conducted at the university. As a community of scholars, in which truth and integrity are fundamental, the university must establish procedures for the investigation of allegations of misconduct of research with due care to protect the rights of those accused, those making the allegations, and the university. Furthermore, federal regulations require the university to have explicit procedures for addressing incidents in which there are allegations of misconduct in research.”

The policy goes on to note that “misconduct means:

* fabrication, falsification, plagiarism, or other serious deviation from accepted practices in proposing, carrying out, or reporting results from research;
* material failure to comply with Federal requirements for the protection of researchers, human subjects, or the public or for ensuring the welfare of laboratory animals; or
* failure to meet other material legal requirements governing research.”

“To be deemed misconduct for the purposes of this policy, a ‘material failure to comply with Federal requirements’ or a ‘failure to meet other material legal requirements’ must be intentional or grossly negligent.”

To become familiar with the expectations around the responsible conduct of research, please review the guidelines for Research Ethics published by the Office of Research Integrity and Compliance.

*This policy applies, in all respects, to this course.*