Course Syllabus

Instructor

Dr. Sen-ching “Samson” Cheung **(http://www.vis.uky.edu/%7Echeung/)**

Email: cheung@engr.uky.edu
Physical Office: Room 217, Davis Marksbury Building (859-218-0299)

Office Hours: Schedule appointment at **http://drcheung.youcanbook.me** **(http://drcheung.youcanbook.me)** **(http://drcheung.youcanbook.me)**

Course Description

This course focuses on technologies in protecting infrastructure, networks, programs, and data from unintended or unauthorized access, change, or destruction. It provides a survey of latest developments in cyber-security through study of theoretical foundation and hands-on practical implementation. Topics include basic security technology, cryptography, security management, risk assessment, operations and physical security, software and network security, as well as ethical and legal issues.

Prerequisites:

This course is suitable as an elective for electrical engineering, computer engineering or computer science seniors and graduate students. Good working knowledge of the following courses or equivalent is required:

1. CS 270 System Programming
2. EE 380 Computer Organization
3. Java Programming Language

In addition, some background in the following topics would be helpful:

1. Computer Network (EE586 is recommended)
2. Linux Environment and shell scripting language
3. Matlab

Student Learning Outcomes:

A student who has successfully completed this course should be able to:

1. Analyze different aspects of a cyber-security management strategy
2. Evaluate risks and countermeasures for different cyber-systems
3. Analyze different methods of attacking and defending cyber-systems
4. Apply basic cryptographic primitives in designing secure protocols
5. Analyze network security and construct firewalls in defending network attacks
6. Explain the legal and ethical issues of cyber-security

Required Materials:

1. Stallings and Brown. ***Computer security: principles and practice* *(https://www.amazon.com/Computer-Security-Principles-Practice-4th/dp/0134794109/ref=dp_ob_title_bk)***, fourth edition, Pearson, 2018 (required, third edition acceptable)
2. Loukas. **Cyber-Phyiscal Attacks: A Growing Invisible Threat (https://www.amazon.com/Cyber-Physical-Attacks-Growing-Invisible-Threat/dp/0128012900/ref=mt_paperback?_encoding=UTF8&me=)**, Butterworth-Heinemann, 2015 (required)
3. Narayanan et. al. **Bitcoin and Cybercurrency Technologies (https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf)**, Princeton University Press, 2016 (optional)
4. Selected papers provided by the instructor.
5. Access to a windows based laptop
6. Access to the ***DeterLab testbed* *(http://deter-project.org/)*** for security experimentation. The DeterLab testbed is a general-purpose experimental infrastructure that supports research and development of next-generation cyber security technologies. We will setup accounts on the DeterLab network for you. For this purpose, your names and email addresses (first.last@uky.edu) will be forwarded to the DeterLab administrator.

Course Assignments:

1. Homework and Laboratory Exercises: They will be assigned roughly every 1.5 week. Except for lab 1, all assignments are for a team of at most two students. While we will discuss homework in class, each team must do his or her homework. Late homework will not be accepted without prior notice.
2. Midterm and Final: Online closed-book exams in the style of CISSP (Certified Information Systems Security Professional) certification.
3. Final Competition: The class will be divided into 4-5 teams and each team will compete with each other in a "capture-the-flag" style competition, usually involving attacking or protecting certain

network asset. The competition will be conducted during the time slot for final examination. The winning team will be awarded with a small trophy and all team members will receive bonus points. The performance is graded based on participation and a detailed report on strategies and techniques during preparation stage.

Course Grading:

Your grade will be based on:	**Undergrad**	**Grad**
Security Lab exercises	50%	45%
Midterm, Final	30%	27%
Final Competition	20%	18%
Term Paper		10%
Total	**100%**	**100%**

Grading scale for undergraduates: 90–100% = A, 80–89% = B, 70–79% = C, 60–69% = D, below 60% = E

Grading scale for graduate students (no D): 90-100% = A, 80–89% = B, 70–79% = C, below 70%= E

Mid-term grades, calculated based on all the work collected thus far, will be posted in myUK by the deadline established in the Academic Calendar (**http://www.uky.edu/registrar/content/academic-calendar** **(http://www.uky.edu/registrar/content/academic-calendar)**)

Expectations for graduate students beyond the expectations for undergraduates:

An additional final research paper on an instructor-approved topic is required of all graduate students taking this course. Undergraduate students are encouraged to try them for extra credit. As graduate students are required to have more assignments, each assignment will carry a smaller weight compared to undergraduate students.

Tentative Course Schedule:

Week	Topics	Homework
Week 1	Introduction, Law and Ethics	Lab 1 Introduction to Deterlab
Week 2	Symmetric Key Encryption	Lab 2 Symmetric Key Encryption
Week 3	Public Key Encryption	Lab 3 Public Key Infrastructure
Week 4	Bitcoin and Cybercurrency	Lab 4 Building your own Bitcoin Blockchain
Week 5	Cyber Physical Security: Examples and Definitions	Lab 5 Side-Channel Attacks
Week 6	Cyber Physical Security: Side-Channel Attacks	
Week 7	User Authentication and Access Control	Lab 6 Software Exploits
Week 8	Database & Cloud Security + Buffer Overflow	
Week 9	Spring Break	
Week 10	Software and OS Security & Digital Forensics	Lab 7 Computer Forensics
Week 11	Primer on computer networking	Lab 8

		Man-in-the-middle attack and DNS Hijacking
Week 12	Denial of Service	Lab 9 Denial of Service
Week 13	Intrusion Detection	Lab 10 Intrusion Detection
Week 14	Firewall and Intrusion Prevention	Lab 11 Firewall
Week 15	Work In Team for Final Challenge	
Week 16	Final Challenge	

Class and Final Schedule

Lectures:	TTh 9:30am-10:45pm (FPAT 255)
Final Competition:	12/11 (Tuesday) 10:30am-12:30pm (DMB 2nd floor Soft Lab)

Course Policies

1. Submission of Assignments

All submissions are done through Canvas. Late homework will only be accepted if acceptable excuse is provided to the instructor before the deadline. Otherwise, 50% will be deducted if the submission is less than 24 hours late and the submission window will be closed after 24 hours.

2. Class meeting attendance policy

All students are required to attend lectures. Students need to notify the instructor of absences prior to meeting when possible.

3. Excused Absences

Students need to notify the professor of absences prior to class when possible. S.R. 5.2.4.2 defines the following as acceptable reasons for excused absences: (a) serious illness, (b) illness or death of family member, (c) University-related trips, (d) major religious holidays, and (e) other circumstances found to fit “reasonable cause for nonattendance” by the professor. Students anticipating an absence for a major religious holiday are responsible for notifying the instructor in writing of anticipated absences due to their observance of such holidays no later than the last day in the semester to add a class. Information regarding dates of major religious holidays may be obtained through the religious liaison, Mr. Jake Karnes (859-257-2754). Students are expected to withdraw from the class if more than 20% of the classes scheduled for the semester are missed (excused or unexcused) per university policy.

4. Verification of Absences

Students may be asked to verify their absences in order for them to be considered excused. Senate Rule 5.2.4.2 states that faculty have the right to request “appropriate verification” when students claim an excused absence because of illness or death in the family. Appropriate notification of absences due to university-related trips is required prior to the absence.

Academic Integrity

Per university policy, students shall not plagiarize, cheat, or falsify or misuse academic records. Students are expected to adhere to University policy on cheating and plagiarism in all courses. The minimum penalty for a first offense is a zero on the assignment on which the offense occurred. If the offense is considered severe or the student has other academic offenses on their record, more serious penalties, up to suspension from the university may be imposed.

Plagiarism and cheating are serious breaches of academic conduct. Each student is advised to become familiar with the various forms of academic dishonesty as explained in the Code of Student Rights and Responsibilities. Complete information can be found at the following website: **http://www.uky.edu/Ombud** **(http://www.uky.edu/Ombud)** . A plea of ignorance is not acceptable as a defense against the charge of academic dishonesty. It is important that you review this information as all ideas borrowed from others need to be properly credited.

Part II of Student Rights and Responsibilities (available at **http://www.uky.edu/StudentAffairs/Code/part2.html** **(http://www.uky.edu/StudentAffairs/Code/part2.html)**) states that all academic work, written or otherwise, submitted by students to their instructors or other academic supervisors, is expected to be the result of their own thought, research, or self-expression. In cases where students feel unsure about the question of plagiarism involving their own work, they are obliged to consult their instructors on the matter before submission.

When students submit work purporting to be their own, but which in any way borrows ideas, organization, wording or anything else from another source without appropriate acknowledgement of the fact, the students are guilty of plagiarism. Plagiarism includes reproducing someone else’s work, whether it be a published article, chapter of a book, a paper from a friend or some file, or something similar to this. Plagiarism also includes the practice of employing or allowing another person to alter or revise the work which a student submits as his/her own, whoever that other person may be.

Students may discuss assignments among themselves or with an instructor or tutor, but when the actual work is done, it must be done by the student, and the student alone. When a student's assignment involves research in outside sources of information, the student must carefully acknowledge exactly what, where and how he/she employed them. If the words of someone else are used, the student must put quotation marks around the passage in question and add an appropriate indication of its origin. Making simple changes while leaving the organization, content and phraseology intact is plagiaristic. However, nothing in these Rules shall apply to those ideas which are so generally and freely circulated as to be a part of the public domain (Section 6.3.1).

Please note: Any assignment you turn in may be submitted to an electronic database to check for plagiarism.

Academic Accommodations:

If you have a documented disability that requires academic accommodations, please see the instructor as soon as possible during scheduled office hours. In order to receive accommodations in this course, you must provide the instructor with a Letter of Accommodation from the Disability Resource Center (Suite 407, Multidisciplinary Science Building, 725 Rose Street, 0082, 257-2754, email address: dtbeac1@uky.edu) for coordination of campus disability services available to students with disabilities.

Course Summary:

Date	Details	
Mon Mar 27, 2017	📝 **Lab 7: Computer Forensics (https://uk.instructure.com/courses/1920944/assignments/10068325)**	due by 11:59
Thu Aug 23, 2018	📝 **Introduction (https://uk.instructure.com/courses/1920944/assignments/10068316)**	due by 11:59
Tue Aug 28, 2018	📝 **Law & Ethics (https://uk.instructure.com/courses/1920944/assignments/10068329)**	due by 11:59
Mon Sep 3, 2018	📝 **Symmetric Cipher (https://uk.instructure.com/courses/1920944/assignments/10068331)**	due by 11:59

Date	Details	
Wed Sep 5, 2018	Lab 1: Intro to Linux & DeterLab (https://uk.instructure.com/courses/1920944/assignments/10068319)	due by 12:30
Fri Sep 7, 2018	Lab 2: Symmetric Key Encryption (https://uk.instructure.com/courses/1920944/assignments/10068320)	due by 11:59
Tue Sep 11, 2018	Message Authentication and Public Key Cryptosystems (https://uk.instructure.com/courses/1920944/assignments/10068307)	due by 11:59
Thu Sep 20, 2018	Cyber-Physical Security (https://uk.instructure.com/courses/1920944/assignments/10068310)	due by 11:59
Tue Sep 25, 2018	Lab 3: Public Key Cipher (https://uk.instructure.com/courses/1920944/assignments/10068321)	due by 11:59
Thu Oct 4, 2018	Bitcoin and Cryptocurrencies (lecture notes updated on 10/11/18) (https://uk.instructure.com/courses/1920944/assignments/10068308)	due by 11:59
Fri Oct 5, 2018	Lab 4: Safety of Cyber Physical Systems (https://uk.instructure.com/courses/1920944/assignments/10068322)	due by 11:59
Tue Oct 16, 2018	User Authentication and Access Control (https://uk.instructure.com/courses/1920944/assignments/10068332)	due by 11:59
Wed Oct 17, 2018	Midterm 1 (https://uk.instructure.com/courses/1920944/assignments/10068306)	due by 11:59
Tue Oct 23, 2018	Computer Networking Primer (https://uk.instructure.com/courses/1920944/assignments/10068309)	due by 11:59
	Lab 5: Bitcoin Blockchain (updated 10/18/2018 - update starter code for the latest bitconj-core library) (https://uk.instructure.com/courses/1920944/assignments/10068323)	due by 11:59
Thu Oct 25, 2018	Software Exploits (https://uk.instructure.com/courses/1920944/assignments/10068330)	due by 11:59
Mon Oct 29, 2018	Lab 6: Software Exploits (https://uk.instructure.com/courses/1920944/assignments/10068324)	due by 11:59
Tue Oct 30, 2018	Lab 6: Access control and networking (https://uk.instructure.com/courses/1920944/assignments/10160378)	due by 11:59
Tue Nov 6, 2018	Denial Of Services (https://uk.instructure.com/courses/1920944/assignments/10068312)	due by 11:59

Date	Details	
Thu Nov 8, 2018	Lab 7: DNS Hijacking (https://uk.instructure.com/courses/1920944/assignments/10068326)	due by 11:59
Thu Nov 15, 2018	Firewall and Intrusion Prevention (https://uk.instructure.com/courses/1920944/assignments/10068315)	due by 11:59
	Intrusion Detection and Firewall (https://uk.instructure.com/courses/1920944/assignments/10068317)	due by 11:59
	Lab 8: Denial of Service (https://uk.instructure.com/courses/1920944/assignments/10068327)	due by 11:59
Tue Nov 20, 2018	Lab 9: Network Intrusion (https://uk.instructure.com/courses/1920944/assignments/10068328)	due by 11:59
Thu Nov 29, 2018	Lab 9: Stateful Firewall (https://uk.instructure.com/courses/1920944/assignments/10176518)	due by 11:59
Thu Dec 6, 2018	Final Capture-the-Flag Competition (https://uk.instructure.com/courses/1920944/assignments/10068313)	due by 2:00p
Fri Dec 14, 2018	Final (https://uk.instructure.com/courses/1920944/assignments/10068305)	due by 11:59
	Final Capture-the-Flag Report (https://uk.instructure.com/courses/1920944/assignments/10068314)	due by 11:59
	Web Application Attacks (https://uk.instructure.com/courses/1920944/assignments/10177471)	