

## 1. General Information

1a. Submitted by the College of: ENGINEERING

Date Submitted: 4/28/2016

1b. Department/Division: Electrical and Computer Engineering

1c. Contact Person

Name: Sen-ching Samson Cheung

Email: [cheung@engr.uky.edu](mailto:cheung@engr.uky.edu)

Phone: 8592180299

Responsible Faculty ID (if different from Contact)

Name:

Email:

Phone:

1d. Requested Effective Date: Semester following approval

1e. Should this course be a UK Core Course? No

## 2. Designation and Description of Proposed Course

2a. Will this course also be offered through Distance Learning?: No

2b. Prefix and Number: EE 576

2c. Full Title: Cybersecurity

2d. Transcript Title: Cybersecurity

2e. Cross-listing:

2f. Meeting Patterns

LECTURE: 3

2g. Grading System: Letter (A, B, C, etc.)

2h. Number of credit hours: 3

2i. Is this course repeatable for additional credit? No

If Yes: Maximum number of credit hours:

If Yes: Will this course allow multiple registrations during the same semester?

2j. Course Description for Bulletin: 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.

2k. Prerequisites, if any: CS 270 and EE 380 or consent of instructor

2l. Supplementary Teaching Component:

3. Will this course taught off campus? No

If YES, enter the off campus address:

4. Frequency of Course Offering: Spring,

Will the course be offered every year?: Yes

If No, explain:

5. Are facilities and personnel necessary for the proposed new course available?: Yes

If No, explain:

6. What enrollment (per section per semester) may reasonably be expected?: 20

7. Anticipated Student Demand

Will this course serve students primarily within the degree program?: Yes

Will it be of interest to a significant number of students outside the degree pgm?: No

If Yes, explain:

8. Check the category most applicable to this course: Relatively New – Now Being Widely Established,

If No, explain:

9. Course Relationship to Program(s).

a. Is this course part of a proposed new program?: No

If YES, name the proposed new program:

b. Will this course be a new requirement for ANY program?: No

If YES, list affected programs:

10. Information to be Placed on Syllabus.

a. Is the course 400G or 500?: Yes

b. The syllabus, including course description, student learning outcomes, and grading policies (and 400G-/500-level grading differentiation if applicable, from 10.a above) are attached: Yes

## Distance Learning Form

Instructor Name:

Instructor Email:

Internet/Web-based: No

Interactive Video: No

Hybrid: No

1.How does this course provide for timely and appropriate interaction between students and faculty and among students? Does the course syllabus conform to University Senate Syllabus Guidelines, specifically the Distance Learning Considerations?

2.How do you ensure that the experience for a DL student is comparable to that of a classroom-based student's experience? Aspects to explore: textbooks, course goals, assessment of student learning outcomes, etc.

3.How is the integrity of student work ensured? Please speak to aspects such as password-protected course portals, proctors for exams at interactive video sites; academic offense policy; etc.

4.Will offering this course via DL result in at least 25% or at least 50% (based on total credit hours required for completion) of a degree program being offered via any form of DL, as defined above?

If yes, which percentage, and which program(s)?

5.How are students taking the course via DL assured of equivalent access to student services, similar to that of a student taking the class in a traditional classroom setting?

6.How do course requirements ensure that students make appropriate use of learning resources?

7.Please explain specifically how access is provided to laboratories, facilities, and equipment appropriate to the course or program.

8.How are students informed of procedures for resolving technical complaints? Does the syllabus list the entities available to offer technical help with the delivery and/or receipt of the course, such as the Information Technology Customer Service Center (<http://www.uky.edu/UKIT/>)?

9.Will the course be delivered via services available through the Distance Learning Program (DLP) and the Academic Technology Group (ATL)? NO

If no, explain how student enrolled in DL courses are able to use the technology employed, as well as how students will be provided with assistance in using said technology.

10.Does the syllabus contain all the required components? NO

11.I, the instructor of record, have read and understood all of the university-level statements regarding DL.

Instructor Name:

---

# EE 576 CYBERSECURITY

Spring 2016

---

All the course contents will be posted onto the internal Canvas site <http://uk.instructure.com>.

---

## Instructor

[Dr. Sen-ching “Samson” Cheung](#)

Email: [cheung@engr.uky.edu](mailto:cheung@engr.uky.edu)

Physical Office: Room 217, Davis Marksbury Building (859-218-0299)

Office Hours: Schedule appointment at <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

There is a fair amount of simulation assignments throughout the semester. Basic familiarity of the Unix system is required. We will apply the knowledge from the class in realistic security scenarios, attacking or defending real servers on the [DeterLab testbed](#) for security experimentation. The DeterLab testbed is a general-purpose experimental infrastructure that supports research and development on next-generation cyber security technologies. The testbed allows repeatable medium-scale Internet emulation experiments for a broad range of network security projects, including experiments with malicious code. We will get you accounts on the DeterLab network. For this purpose, your names and email addresses (first.last@uky.edu) will be forwarded to the DeterLab administrator. Furthermore, we will also use an ensemble software of cryptosystems and cryptanalysis tools called [Cryptool](#) in learning different types of encryption, hashing, and digital signatures. DeterLab testbed can be accessed via any ssh connection and Cryptool runs on Win32 platform.

---

## 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](#), third edition, Pearson, 2015 (required)
  2. Singer and Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford, 2013 (optional but highly recommended – [Kindle version](#) costs less than two Grande Mocha from Starbucks!)
  3. Selected papers provided by the instructor.
- 

## Course Assignments:

1. Homework and Laboratory Exercises  
They will be assigned roughly weekly. While we will discuss homework in class, each student 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  
It is a team project of two-three students. All teams will participate in a Capture-the-Flag (CTF) that involves hacking and defending a realistic system.
- 

## Course Grading:

<b>Your grade will be based on:</b>	<b>Weights</b>
Security Lab exercises	40%
Midterm, Final	30%
Final Competition	30%
<b>Total</b>	<b>100%</b>

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>)

---

## Expectations for graduate students beyond the expectations for undergraduates:

Additional advanced security lab exercises will be assigned to graduate students, though undergraduate students are encourage to try them for extra credit. As graduate students are required to have more lab exercises, each exercise will carry a smaller weight compared to undergraduate students.

---

## Tentative Course Schedule:

<b>Day</b>	<b>Offline Lecture</b>	<b>Readings</b>	<b>Homework</b>
Week 1	Introduction, Law, Ethics	Stallings 1, 19	Lab 1
Week 2	Cryptography 1	Stallings 2, 20, 21, B	Intro & Warmup

Week 3	Cryptography 2	Stallings 2, 20, 21, B	Lab 2 CrypTool
Week 4	Authentication & Authorization	Stallings 3	
Week 5	Access control and Multilevel Security Architecture	Stallings 4, 13	Lab 3 Permissions and ACLs
Week 6	Computing Network Primer	Stallings 22	Lab 4 DNS Hijacking
Week 7	Denial-of-Service	Stallings 7, F, I	Lab 5 TCP SYN flood
Week 8	Intrusion Detection	Stallings 8	Lab 6 Intrusion detection
Week 9	Firewall and Intrusion Prevention	Stallings 9	
Week 10	Malicious Software	Stallings 6	Lab 7 Worm detection
Week 11	Operating System Security	Stallings 12	Lab 8 OS Hardening
Week 12	Physical and Human Security	Stallings 16, 17	Lab 9 Computer Forensics
Week 13	Security Auditing	Stallings 18	
Week 14	Cyber-Physical Security I		No Homework
Week 15	Cyber-Physical Security II		
Week 16	Final Challenge		

---

## Class and Final Schedule

Lectures: TTh 9:30am-10:45pm (FPAT 265)  
Final Competition: 5/7 8:00am-10:00am (DMB 2<sup>nd</sup> 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>. 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>) 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](mailto:dtbeac1@uky.edu)) for coordination of campus disability services available to students with disabilities.