CS 490: Cryptography and Computer Security

Instructor: Thoshitha Gamage, Ph.D.
Southern Illinois University at Edwardsville

Spring 2015 Syllabus

Course Information:

Title:	CS 490: Cryptography and Computer Security (3 Credits)
Location:	EB 0140
Time:	T & R 06:00 – 07:15 p.m.
Course Web site:	http://www.cs.siue.edu/~tgamage/S15/CS490

Contact Information:

Office:	EB 2050
Phone ☎:	650-2407
Email ✉:	tgamage@siue.edu
Web Site ⌂:	http://www.cs.siue.edu/~tgamage
Office Hours:	M & W 02:30 – 04:00 p.m.
	T & R 11:00 – 12:30 p.m. *or by appointment*

1 Course Objectives

This course is an advanced undergraduate level introduction to cryptography and computer security. This is a **research emphasis** course with the following objectives.

1. To introduce fundamental modern cryptographic and computer security *constructs* and *concepts*;
2. To facilitate a learning environment that strengthens participants' *theoretical* and *empirical* knowledge, and understanding through hand-on experiments;
3. To improve participants' critical thinking, reading, and writing skills;
4. To introduce *recent advances*, *broader challenges*, and *current trends* in computer security; and
5. To spur self-curiosity in and a research appetite for advanced and/or specialized topics – network, application, web, cloud, OS, etc. – in (more generally) **cyber security**.

By the end of the semester, students are expected to be proficient in cryptographic and computer security basics, security exploits, and defensive mechanisms to aid them in their professional career advancements.

The content of this course is influenced by and was developed in accordance to the IEEE/ACM Computer Science Curriculum Guidelines (2013) http://www.acm.org/education/CS2013-final-report.pdf

2 Minimum Course Prerequisites

MATH 224 : The cryptographic component of this course is substantially formal and mathematical, both in context and in substance, and will either introduce or revise concepts in number theory, finite fields, modular arithmetic, probability theory, statistics, linear algebra etc.

CS 447 : The computer security component of this course will leverage basic understanding of the TCP/IP stack, network communication, and network programming knowledge.

In addition, fluency and significant experience in structured or imperative programming (e.g. C, C++, Java, Python), and **Unix/Linux** is a **MUST** for the hand-on experiments. If you do not meet these prerequisites, talk to the instructor immediately within the first week of classes. I reserve the right to drop participants from the course that do not meet these minimum prerequisites.

3 Reference Textbooks

Most of the core material of this course are derived from the following textbooks, thus they should serve as good references. Students are expected and **required** to take their own notes, and supplement those with their own reading.

Recommended -

MB1e "Computer Security : Art and Science" 1^{st}ed., Matt Bishop, Addison-Wesley, ISBN-13: 978-0201440997 http://nob.cs.ucdavis.edu/book/book-aands/index.html

Alternative/Supplemental -

BF1e "Cryptography and Network Security", 1^{st}ed., Behrooz Forouzan, McGraw-Hill, ISBN-13: 978-0073327532 http://highered.mheducation.com/sites/0072870222/index.html

SB3e "Computer Security : Principles and Practice", 3^{rd}ed., William Stallings and Lawrie Brown, Pearson, ISBN-13: 978-0133773927 http://www.pearsonhighered.com/stallings

Additional Reading - Additional reading may be assigned as the course evolves through the semester hosted through either http://ieeexplore.ieee.org/, http://dl.acm.org/, and/or the course website.

4 Assigned Work and Tentative Grading Policy

The following allocation of grade percentages is *tentative*, and may change during the semester. Unless the circumstances change, I am not planning on curving the final grade.

Grading Allocation		
Exams		40%
Midterm	15%	
Final *(comprehensive!!)*	25%	
Class Participation		5%
Homework		15%
Projects		40%

Final Letter Grade	
90–100	A
80–89	B
70–79	C
60–69	D
below 60	F

4.1 Exams

All exams and quizzes will be held in the lecture room. The final is **comprehensive**.

- **Midterm** : Thursday March 05^{th} 06:00 – 07:15 p.m.
- **Final** : Tuesday May 05^{th} 06:30 – 08:10 p.m.

4.2 Class Participation

You are expected to **proactively** participate in in-class discussions. This aids your learning and that of your classmates, and provides valuable feedback on the lecture. Constructive and proactive participation in in-class discussions and scribing accounts for 5% of your final grade, thus I expect you to attend each and every class. Two randomly (but fairly) designated students per lecture will serve as **scribes**, and the scribe notes are due through *Moodle* within **48 hours** of the conclusion of the lecture. These notes will be available for the rest of class as a baseline set of complementary notes to your own notes. In addition, I reserve the right to take either take a roll call or conduct a pop quiz to count attendance, if required.

If you miss a class, it is *your* responsibility to find out what happened and to collect any material that was handed out in the class. Students are also **required** to check the course website and the SIUE email account regularly for any important updates.

4.3 Homework

There will be roughly ~3-4 homework assignments that will be posted on the course website. Unless otherwise stated, each homework assignment will be due within 2 weeks of posting on the course website.

4.4 Projects

There will be two components to the projects:

1. In the first component, you will be given roughly ~3 hands-on security experiments based on DETERLab with a 2 weeks deadline. These will be posted on the course website.
2. The second component is your own **security themed** research project (preferably) of your own interest. Both analytical and theoretical studies are acceptable, but they **must be** your own genuine contributions. For full points, you are strongly encouraged to include an empirical component in your study either in simulation form or in performance comparison form. You will be required to present your findings to the class during the final week of instruction. In addition, a IEEE conference style 8 page paper of your findings will be due on the day of your presentation as the final report. Undergraduate students will be allowed to team up to 2 members per group with my prior approval.

I will give you the option to choose a language of your choice for programming (though C++, Java, or Python is recommended) but the development platform is fixed to Unix/Linux.

5 Graduate Standing

Graduate students will be assigned regular technical reading assignments posted either through the course website or digital libraries. You are to critique the assigned paper(s) within 1 week and turn-in a typed (not hand written) summary of your critique through Moodle. A sample template for your critique summary will become available through the course website.

In addition, graduate students may have additional mandatory questions in exams and in homework assignments that could also be based on your technical readings. Unless otherwise noted, graduate students will work on their own on projects and are in general expected to have higher programmatic and technical standards. Accordingly, graduate students will be graded on a separate scale.

6 Course Requirements and Policies

6.1 Attendance Policy

For unforeseen circumstances, there will be times when you are unable to attend the lecture. Thus, I allow you to miss at most 2 classes for the semester without any penalties. Medical emergencies are outside this "absentee allowance", but should be accompanied by proper documented proof of medical services. For planned absences, assignments should be turned in before the absence, rather than after. I reserve the right to lower the grade of any student who is markedly deficient in attendance and/or in in-class participation.

6.2 Late Policy

Unless otherwise noted or announced in-class, assignments (projects and homework especially) will typically have a 2 week **strong** deadline. I anticipate most submissions to be **digital** through Moodle. The submission window will open 24 hours in advance of when it's due. It will remain open for an additional 48 hours with a 15% late penalty. No assignments will be accepted beyond this penalty period.

6.3 Responsible Learning Policy

I expect *you* to *own* your degree of success in this class *and*, I expect you to contribute to the success of others. Examples:

- read outside the class on your own (strongly encouraged) in preparation for each lecture, jot down any questions your encounter on your reading, and bring those to the class as discussion points;
- be respectful of the learning environment. Refrain from activities that may disturb the flow of the lecture or the environment;
- cooperate with other students and to share your knowledge during in-class discussions. Respect the differences in learning and understanding of each other. Seek ways of taking advantage of those differences;
  - do not engage in disruptive *"little talk"* while I am conducting the lecture; if you have a concern, raise your hand and grab my attention. be respective of your colleagues' time and desire to learn.
  - Put your cell phones to vibrate mode and refrain from using your computers for casual web browsing. Take full advantage of the opportunity to learn.
- If another student is confused, help him or her out without disturbing the class;
- I enjoy engaging in technical conversations with students with the goal of helping them create an accurate understanding of course material. Participating in such conversations is very favorable for your class participation grade;
- If I am systematically doing something that inhibits your learning, tell me;
- engage in *proactive learning*: speak up when you don't understand, question assumptions, relate course material to your experience outside class, seek out additional experience and reading related to the class. You must *construct* your understanding of the material;
- If a lecture point is unclear, ask questions and ask me to repeat what I said, either in class, during office hours, or by e-mail. You are probably not alone in your confusion;
- promptly review feedback you receive from me or peers to actively clarify the feedback if the material is still unclear, and to incorporate the feedback in your future work;
- spend adequate time on the course. Adequate time includes getting enough rest so that time you spend on course tasks is well-spent time. Adequate time includes proofreading and reviewing your assignments before you hand them in;
- have high expectations of yourself: set goals for yourself and try to do your very best. Consciously think about the balance between what you do to earn a grade and what you do to learn (If I'm doing something that puts these in opposition to each other, please let me know); and,
- check your SIUE assigned student email and the course website regularly for important class announcements.

IMPORTANT: I strongly discourage you getting into discussions with me about grades and how you can get a better one.

6.4 Academic Dishonesty: http://www.siue.edu/policies (3C1 & 3C2)

Do your own work. Your exams, homeworks, and programming projects are subject to the academic honor code. **DO NOT CHEAT IN ANY WAY: DO YOUR OWN WORK!**. Following activities will be considered academic dishonesty:

- submitting work (such as homework assignments and projects) done by somebody else (this includes any human/electronic sources (such as web sites));
- watching and copying your neighbors' solutions during quizzes and/or exams;
- using materials not allowed during quizzes and exams;
- using materials not allowed for the programming projects.

It is quite acceptable to ask others things like "Have you gotten this exception before?," and even have them look briefly at your stack trace and its code It is quite unacceptable, on the other hand, to have them spend hours helping develop or seriously rearrange your program's logic. And, of course, it is unacceptable for two or more people to collaboratively develop the solution for a project. If you are tempted to collaborate on projects, **DON'T!!**.

I expect you to know and observe the SIUE Student Conduct Code (3C1) and Student Academic Code (3C2). Copying of other students' work, working together on individual assignments, plagiarism of published sources and other forms of academic dishonesty will result in zero credit on the assignment for all students involved and a lower grade in the class. A second offense (across the University) will result in an automatic **F** in the course and exposes the violator to University sanctions up to and including expulsion. All offenses will be reported to Student Affairs.

6.4.1 Advice

a Don't wait until the last minute to do homework or projects. Labs get busy, computers break down, and people get sick. These are not sufficient excuses for an extension.
b Save early; save often!
c Contact me if you are confused. Don't wait for office hours; send an email.

6.5 Disability Support Services: http://www.siue.edu/dss

Any student inquiring about academic accommodations because of a disability should contact Disability Support Services so that appropriate and reasonable accommodative services can be determined and recommended. Disability Support Services is located in Student Success Center, Room 1270. Their phone number is 650-3726 and their email is disabilitysupport@siue.edu.

7 Tentative Schedule*

*Subject to adjustment and change. I reserve the right to change topics or add an item of related interest. All changes will be announced in class.

Week	Dates	Topics	References	Assignments/Exams
01	Jan. 13, 15	Introduction and Course Overview Security Goals, Threats, Assumptions, and Trust	**MB1e**/01 **BF1e**/01	
02	Jan. 20, 22	Security Policies: ACM, T-G Techniques: Crytography, Steganography	**MB1e**/02,03,04 **BF1e**/01	
03	Jan. 27, 29	**Confidentiality**: BLP Model, Basic Security Theorem Cipher Techniques, Symmetric-Key Ciphers: DES	**MB1e**/05,09,11 **BF1e**/03,05	
04	Feb. 03, 05	3DES, AES Asymmetric-Key Ciphers: RSA, Rabin, Elgamal	**BF1e**/06,07 **BF1e**/10	
05	Feb. 10, 12	Elliptic Curve Crytosystems Primes	**BF1e**/10 **BF1e**/09	
06	Feb. 17, 19	**Integrity:** Biba, Lipnar's, Clark-Wison Models Cryptographic Checksum: HMAC	**MB1e**/06 **BF1e**/11	
07	Feb. 24, 26	Cryptographic Hashing: SHA, Whirlpool Digital Signatures: DSS	**BF1e**/12 **BF1e**/13	
08	Mar. 03, 05‡	**Key Management:** Kerberos Key Generation	**MB1e**/10	‡ Midterm Exam
09	Mar. 10†, 12†	**Spring Break**		
10	Mar. 17, 19	Cryptographic Key Infrastructure, Storage and Revoking **Authentication:** Zero Knowledge Proofs	**MB1e**/10 **BF1e**/15	
11	Mar. 24, 26	Chinese Wall Model, Confinement Problem Malicious Logic, Intrusion Detection	**MB1e**/07,17,22 **BF1e**/01	
12	Mar. 31, Apr. 02	**Network Security:** SSL and TLS, IPSec, PGP DNS Security, Secure Routing	**MB1e**/11,26 **BF1e**/16,17,18	
13	Apr. 07, 09	**Digital Identity:** Annonymous Communication Application vulnerabilities: XSS, SQL Injection	**MB1e**/14	
14	Apr. 14, 16	Buffer Overflow, Denial-of-Service System Security Design Principles	**MB1e**/13	
15	Apr. 21, 23	Responsible Disclosure and Ethics *— buffer week —*		
16	Apr. 28§, 30§	Final Project Presentations		
17	May. 05	**Final Exam: 06.30 – 08.10 p.m.**		

†Spring Break
‡Midterm Exam
§Final Project: In class presentations