ISA656: Network Security

George Mason University, Computer Science, Spring 2019

Instructor: Prof. Foteini Baldimtsi (foteini@gmu.edu)
Office Hours: Wednesdays 2:30PM-4:30PM, Engineering 5333
Lectures: Wednesdays 4:30PM-7:10PM, Location: Innovation Hall 134

Teaching Assistant: Panagiotis Chatzigiannis (pchatzig@masonlive.gmu.edu).
Office hours: Thursdays 2:30pm-4:00pm, Office: TBA

Course Summary

An in-depth introduction to the theory and practice of network security. It assumes basic knowledge of cryptography and its applications in modern network protocols. This course will train you how to "think like an adversary"---thinking about how adversary might attack a system by subverting and exploiting assumptions made during system design---and will discuss threat modeling and formal cryptographic approaches to defining and proving security or privacy.

The class provides deep coverage of widely used network security protocols such as SSL, TLS, SSH, Kerberos, IPSec, IKE, and PGP. It covers countermeasures to distributed denial of service attacks, security of routing protocols and the Domain Name System, e-mail security and spam countermeasures, wireless security, web security, trust negotiation and decentralized payment systems (Bitcoin like).

Prerequisites: ISA 562 and (ISA 612 or CS 555). There will be substantial programming involved in the assignments, and students should be familiar with setting up a Virtual Machine and programming in Python, C, Java or another language.

Required Materials

Text Book: Kaufman, Perlman, and Speciner. **Network Security: Private Communication in a Public World**, Second Edition, Prentice Hall PTR, 2002, ISBN 0130460192. (Free online in GMU library).

For certain lectures additional material will be posted here. There will also be on-line news articles and research publications that will be required reading before some of the lectures.

Grading

Assignments: 40% (5 assignments that will require both programming and problem solving)
Midterm: 25% (in class exam covering around about 2/3 of material)
Final Project: 25% (You will work on a project in network security with a writeup/presentation due at the end)
Quizzes: 10% (6 quizzes, lowest grade dropped)

HW and Late policy: Homework questions will be posted on Blackboard and solutions have to be submitted through Blackboard (no credit will be given otherwise). Assignments received within 24 hours after the deadline lose 20%, within 48 hours 40% and after that no credit will be given. To be fair with everyone in class no exception will be made to the rule above.

Quizzes will happen in class through Blackboard. You need to have a device with access to blackboard with you in class whenever a quiz takes place.

Communications: We will use **Piazza** to communicate with you. You are welcome to set up study groups, to post interesting security incidents you read about, or to discuss course materials with other students. If you have a question about the course you should: (a) Come to office hours, OR (b) Post on Piazza. Do not use private posts/emails to ask technical questions. The rest of the class is probably also interested in your question, so make it public!

Ethics: To defend a system you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy is that you must respect the privacy and property rights of others at all times, or else **you will fail the course**.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking". Understand what this law prohibits.

Honor code: All students must adhere to the GMU Honor Code. You can discuss lecture material with other students in class but you have to work on the assignments alone. More specifically: (1) You may not share actual code.

In other words, the code you write must be entirely your own, which you must write and debug without looking at other people's code. Do not permit others to copy your code. (2) You must write up your solutions completely on your own, without looking at other people's write-ups. (3) You are welcome to use any textbooks, online sources, blogs, research papers, Wikipedia, etc in your assignment, as long as these are properly cited in any submitted work.

Failure to do this is plagiarism and is serious violation of the GMU Honor Code and basic scientific ethics, and will not be tolerated.

Class Schedule (Tentative):

Lecture	Topic	Suggested Readings	HWS
01/23 Lec. 1	Introduction & Class logistics and Cryptography Toolbox I	Chapters 1.1-1.6 and 2.1-2.4 Symmetric Encryption What does security for encryption schemes means: Ciphertext Only Attack (COA), Known Plaintext Attack (KPA), Chosen Plaintext Attack (CPA), Chosen Ciphertext Attack (CCA).	HW1 out
01/30 Lec. 2	Cryptography Toolbox II	Chapters 3.1-3.3, 3.5, 3.6, 4.1-4.5 Modes of Operation, Hash Functions, MACs Misuse of RC4 in Microsoft Excel, RC4 attack on SSL/TLS, SSL Beast attack (reusing IV in CBC mode)	Quiz 1
02/06 Lec. 3	Padding oracle attacks	Chapters 4.1-4.5 Common pitfalls of CBC-MAC Padding oracle attack (LuckyThirteen attack on TLS, POODLE attack on SSL)	Quiz 2
02/13 Lec. 4	Public Crypto, PKIs, CAs	Chapters 5.1, 5.2, 5.5, 5.7, 6.1, 6.4	HW1 in 2/15 HW2 out
02/20 Lec. 5	Key Exchange, SSL/TLS	Chapters 11.4, 13, 9.1, 15.1-15.5, 19 TLS 1.3 Specification, MIT kerberos	Quiz 3
02/27 Lec. 6	Kerberos		HW2 in 2/29 HW3 out
03/06 Lec. 7	DNS, DNESSEC	A DNSSEC tutorial, Kaminsky attach on DNS, DNSviz tool	Quiz 4
03/20 Lec. 8	IPSec, IKE, Review	Chapters 17,19,21,22 IPSec by Cisco, More on IPSec	HW3 in 3/22 HW4 out
03/27	Midterm		
04/03	PGP, S/MIME,	Chapter 21,22,23	HW4 in

Lec. 9	Email Spam	OpenPGP	04/05 HW5 out
04/10 Lec. 10	Firewalls, Web security		Quiz 5
04/17 Lec 11	Bitcoin & Blockchain	Princeton Bitcoin Book, Bitcoin Blockchain explorer	HW5 in 04/19
04/24 Lec 12	Anonymity & Privacy		Quiz 6
05/01 Lec 13	TBA		
05/08	Final Project Presentations		

Sign in | Recent Site Activity | Report Abuse | Print Page | Powered By **Google Sites**