Spring 2022 EE609 *Syllabus*: Computer and Network Security, 3 credits

Course Description: We will study basic security theory, current practices, and emerging research issues in this class. The course consists of two parts. The first part covers the fundamentals of computer and network security, and the second part focuses on research projects on the state-of-art computer and network security issues and challenges. We will look into specific areas for research, e.g., blockchains for distributed consensus.

Prerequisites: Please talk to the instructor. Basic understanding of computer systems and programming languages.

Class Format: Lectures are combined with discussions and student presentations and discussions of advanced topics. Students are expected to be active participants, by studying the relevant chapters and/or research papers, and participating at in-class discussions.

Class Time and Location: MW 2:00-3:15pm at SAKAM B104 (We will decide virtual or in-person by that time).

Instructor: Yingfei Dong
yingfei@hawaii.

Office Hours: Holmes Hall 442, one hour after the class, or by email appointment.

Textbook:

(1) *Computer Security: Art and Science, 2nd Edition, Matt Bishop, ISBN-10: 0-321-71233-1, ISBN-13: 978-0-321-71233-2, Publisher: Addison-Wesley Professional, Copyright: © 2019 Pearson Education, Inc.*

(2) Computer Security A Hands-on Approach, Wenliang Du, Syracuse University, ISBN-13: 978-1548367947 ISBN-10: 154836794X, Oct 2017.

Handouts/Notes and Supplemental Text: will be available on-line or distributed in classes**.**

Supplemental Text

- Michael Goodrich, Irvine Roberto Tamassia, Introduction to Computer Security, ISBN-10: 0321512944, ISBN-13: 9780321512949, Addison-Wesley, 2011.
- William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, ISBN-10: 0-13-444428-0, or ISBN-13: 978-0-13-444428-4, Prentice Hall, 2017
- Pfleeger, C. *Security in Computing.* Prentice Hall, 1997.

Announcements will be sent to you via Laulima.

Main Topics

- Key Security Concepts,
- Classical Encryption, Block Ciphers and the Data Encryption Standard (DES) and Advanced Encryption Standard (AES)
- Basic Concepts in Number Theory and Finite Fields:
- Pseudorandom Number Generation and Stream Ciphers
- Number Theory: Euler's Totient function, Miller Rabin, factoring, modular exponentiation, discrete logarithm, and Chinese remainder theorem.
- Public-Key Cryptography: RSA, Diffie-Hellman, elliptic curve.
- Cryptographic Hash Functions and Digital Signatures
- Key Management and Distribution
- Network Access Control and Cloud Security
- Transport-Level Security (TLS)
- Wireless Network Security

Grading:

(1) Hands-on Exercise Projects	**40%**
(2) Research Project: Survey & Presentation	**40%**
(3) Homework, Quizzes	**15%**
(4) Participation (contribution in discussions and questions)	**5%**

Assignments Guidelines:

- Unless otherwise specified, all assignments and projects are individual work.
- Assignments and Late Penalty: Assignments and projects will be posted at the class web site. Assignments & projects are due before the beginning of the class on the due day. See Topics and Notes for the due dates. Points will be deducted from late assignments: 50% for the first 24 hours after the due time, 100% after that. No extension will be granted except for documented emergency.
- Start to work on the assignments as early as possible.
- Identification page: All assignments must have your name, and course number at the top of the first page.
- Please staple all the pages together at the top-left corner.
- Please arrange the solutions following the sequence of the questions.
- Word processing: It is required that you type your reports. Use a word processor and appropriate typesetting and drawing tools to do the assignments. Spell-checking the whole document before printing it. You may lose points due to spelling or grammatical errors.

Policies:

- Make-up exams will generally not be given. Missing a quiz or exam will result in a score of zero unless extreme extenuating circumstances are discussed with the professor ahead of time or verifiable proof is presented
- Attendance Policy: You are expected to attend all classes. If you miss a class, it is your responsibility to get hold of whatever may have been discussed in the class.

- If you think you have lost some points due to grading errors, make sure you approach the instructor within a week after the assignment, project, or test is returned to you.
- To get the most out of this class, you need to read the textbooks and spend time using computers regularly. Be prepared for a class by preview the material to be covered in that class and participate in discussions and problem-solving exercises, if applicable, in the class.
- Academic dishonesty will not be tolerated in any form. The integrity of our program depends on the integrity of the work done by each student. The University expects a student to maintain a high standard of individual honor in his/her scholastic work. Please refer to UH Student Conduct Code at http://www.catalog.hawaii.edu/reference/appendix02.htm for Academic Honesty, Cheating, Plagiarism, Disciplinary Action, etc.

Paper Reading List will be available in Laulima Class site

Projects

1) **Track 1:** For students who have taken EE406 (or a similar class), they will
   - **a.** either conduct research projects, e.g., software reverse engineering, blockchain, machine learning security,
   - **b.** or do additional SEED labs, e.g., Shellshock, return-to-libc, firewall, packet sniffing, secure hash, Andriod rooting, cross site request forgery, TLS, etc.
2) **Track 2.** For student who haven't taken EE406 (or a similar class), we will mostly use SEED lab projects as their main focuses, e.g., Set UID attacks, Buffer overflow attacks, TCPIP attacks, Symmetric Encryption, Public Key Encryption and PKI, etc.

Learning outcomes

Students are expected to understand the basic security concepts and understand current challenging issues.

- Learn and understand the basic cryptographic concepts and solutions, including symmetric encryption, public-key encryption, secure hash functions, random number generation, key distribution, access control, etc.
- Grasp open-source tools (Open SSL and PGP), and apply these tools in real world applications.
- Understand the current threats on the Internet (including malware, cross-site scripting attacks, SQL injections, viruses, worm, and Trojan horses).
- Grasp basic security skills, including setting up virtual machines, configuring firewalls, and VPN tunnels.
- Understand that security is a life-long learning process. We must learn and adapt to new threats such as new attacks, and indentify corresponding solutions.
- Be aware of current security research topics, including Denial-of-service attacks, botnets, phishing, spamming, etc.
- Understand the basics of anonymity and privacy issues, such as wikileaks, Freenet.
- Be able to identify a security problem and perform preliminary research on the topic.
- Learn basic literature survey skills.
- Learn oral presentation skills.

Advice on Professional Presentation:

- Mark Hill, Oral Presentation Advice, http://www.cs.wisc.edu/~markhill/conference-talk.html
- Charles Van Loan, The Short Talk, http://www.ee.hawaii.edu/~dong/GoodAdvice/ShortTalk.html
- John Farrell, What to Say in a Good Research Talk,
- http://www.ee.hawaii.edu/~dong/GoodAdvice/ResearchTalk.JohnFarrell.html
- Mark Leone's Collection, http://www.ee.hawaii.edu/~dong/GoodAdvice/CollectionOfAdvice.html

Homework: will be available on-line or distributed in classes. You are encouraged to discuss your homework with your partner, but you must write your answer alone.

Academic dishonesty will not be tolerated in any form. The integrity of our program depends on the integrity of the work done by each student. The University expects a student to maintain a high standard of individual honor in his/her scholastic work. Please refer to UH Student Conduct Code at http://www.catalog.hawaii.edu/reference/appendix02.htm for Academic Honesty, Cheating, Plagiarism, Disciplinary Action, etc.

Specifically, you must do your homework and examinations yourself, on your own, unless specifically stated otherwise in the assignment. You may discuss the homework with anyone, and use any reference material, provided you do not copy any other person's work, either in whole or in part. You may discuss assignments in general terms, but you are not allowed to share any details of actual algorithms or of program code. You may help someone else debug their program as long as you do not substitute in your own code when there are problems. Turning in a copy of someone else's program, even a copy with extensive changes made to it, is a very serious offense in this course. Penalties will be severe and automatic. (Minimum penalty: F grade for the course.)

What is plagiarism? "In short, to plagiarize is to give the impression that you have written or thought something that you have in fact borrowed from another." W. S. Achtert and J. Gibaldi, The MLA Style Manual, New York, Modern Language Association of America, 1985, p. 4.

You are a class of diverse talents, diverse backgrounds, and diverse learning styles. Because not all students learn the same way, the instructor will try a variety of teaching styles to present the material. Some you will like, others you will not. Please be aware, what works for you may not necessarily work for others in the class and vice versa. Therefore, you are expected to actively participate in your own education to make the best of all situations whether you like them or not. Please contact me directly if you have any comments about the class.