جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

Course Syllabus: Contemporary Topics in Computer Security - CS 294S

Division	Computer, Electrical and Mathematical Sciences & Engineering
Course Number	CS 294S
Course Title	Contemporary Topics in Computer Security
Academic Semester	Summer
Academic Year	2018/2019
Semester Start Date	06/16/2019
Semester End Date	08/08/2019
Class Schedule (Days & Time)	09:00 AM - 12:00 PM | Wed Thu

Instructor(s)

Name	Email	Phone	Office Location	Office Hours
Marios Omar Choudary	UMAR.CHOUDARY@KAUST.EDU.SA			

Teaching Assistant(s)

Name	Email

Course Information

Comprehensive Course Description	This class will cover a wide range of security aspects, but will focus on the following main topics: 1) Cryptography. We shall cover many aspects of both symmetric crypto as well as asymmetric crypto, focusing mostly on the former one. Starting with an analysis of historical ciphers, we'll discuss stream ciphers, block ciphers like AES and DES, then Hash functions and MAC algorithms. We shall also discuss methods for authenticated encryption and then also cover aspects of key exchange. Finally we shall cover public key encryption algorithms. 2) OS Security. In this area, we shall cover a variety of topics, including: buffer overflow attacks, malware analysis, web security and access control. 3) Side-channel attacks. This is often a big problem regarding practical implementations of security, either system security or cryptographic algorithms. We shall study several such attacks, including timing-based (e.g. against RSA), cache-based (Meltdown) and power/EM based attacks. 4) Password-based security. Passwords are almost inevitably in our everyday online activities. Hence, we shall cover several aspects related to the use and security of passwords and how to properly make use of them. 5) Information privacy. This is a very popular topic in the recent years, since many more entities are interested in sharing information in a private manner, such that either their identity or the data they transmit remains anonymous. We shall focus on methods for anonymous communications and for private information retrieval. 6) Nation state security. We shall discuss, at least briefly, several of the security mechanisms and goals of nation-wide security institutions, as observed and understood from several public sources. The detailed syllabus is as follows: -Lecture 1: Introduction, historical ciphers, OTP, PRGs -Lecture 2: Cont on PRG (WEP, RC4, LFSR, Salsa, ChaCha, WPA) Negligible functions, advantage, computational security, semantic security. Block ciphers; PRP/PRF, DES, AES. -Lecture 3: Cont. on block ciphers (CPA security, modes of operation: ECB, CBC, CTR, attacks on fixed IV, on padding) Message Authentication Codes and Hash functions. HMAC. Full-disk encryption. -Lecture 4: Authenticated Encryption. Lab 1: Historical ciphers, LFSR attacks, AES attacks, Birthday paradox attack -Lecture 5: Key exchange, public key encryption, TLS case study -Lecture 6: EMV case study. Side-channel attacks part 1: timing attacks, power analysis attacks -Lecture 7: Buffer overflow attacks. Malware. -Lecture 8: Web security -Lecture 9: Access Control -Lecture 10: Side-channel attacks part 2: cache-based attacks (Meltdown case study) -Lecture 11: Password-based security -Lecture 12: Information privacy Possible modification may appear during the class.
Course Description from Program Guide	
Goals and Objectives	The goal of this class is to familiarise students with the concepts of Cryptography, OS security, Web security, Policy and Access Control as well as nation state security.
Required Knowledge	The students should have some basic knowledge of computer programming (we shall use Python for homeworks and labs as well as C), and some basic knowledge of computer architecture, computer networks and discrete probability.
Reference Texts	-Introduction to Cryptography, 2nd edition, Catz and Lindell -Security Engineering, 2nd edition, Ross Anderson
Method of evaluation	**50.00**% - Final exam **25.00**% - Homework /Assignments **25.00**% - Course Project(s)
Nature of the assignments	-Individual homeworks -Individual project
Course Policies	-attendance is mandatory to classes -homeworks and project are mandatory

Additional Information	

Tentative Course Schedule *(Time, topic/emphasis & resources)*		
Week	**Lectures**	**Topic**
1	Wed 06/19/2019 Thu 06/20/2019	-Introduction, historical ciphers, OTP, PRGs -Cont on PRG (WEP, RC4, LFSR, Salsa, ChaCha, WPA) Negligible functions, advantage, computational security, semantic security. Block ciphers; PRP/PRF, DES, AES.
2	Wed 06/26/2019 Thu 06/27/2019	-Cont. on block ciphers (CPA security, modes of operation: ECB, CBC, CTR, attacks on fixed IV, on padding) Message Authentication Codes and Hash functions. HMAC. Full-disk encryption. -Authenticated Encryption. Lab 1: Historical ciphers, LFSR attacks, AES attacks, Birthday paradox attack
3	Wed 07/03/2019 Thu 07/04/2019	-Key exchange, public key encryption, TLS case study -EMV case study. Side-channel attacks part 1: timing attacks, power analysis attacks
4	Wed 07/10/2019 Thu 07/11/2019	-Buffer overflow attacks. Malware. -Web security
5	Wed 07/17/2019 Thu 07/18/2019	-Access Control -Side-channel attacks part 2: cache-based attacks (Meltdown case study)
6	Wed 07/24/2019 Thu 07/25/2019	-Password-based security -Information privacy
7	Wed 07/31/2019 Thu 08/01/2019	-Final presentations and recap of all lectures -Project presentations
8	Wed 08/07/2019 Thu 08/08/2019	-Nation state security -Final exam

Note

The instructor reserves the right to make changes to this syllabus as necessary.