Tentative Syllabus
CENG781 Network Security
20167-2018 Fall

Instructor: Ertan Onur, eronur@metu.edu.tr, 5534, B211

Office Hours: Fridays 09:30-10:30 and by appointment.

Logistics Tuesdays, CENG-A101, 13:40-16:30.

Catalog Description: Basics and principles of cryptography and computer network security, their applications in the Internet and wireless networks, conventional (symmetric) and public-key (asymmetric) cryptography, cryptographic hash functions, message authentication codes and digital signatures, mutual trust and user authentication, transport and network layer security in the Internet, wireless network security, and advanced topics in security.

Course Objectives: By the end of the course, you will be able to
o1: Understand the basic principles of cryptography and their applications,
o2: Describe and discuss the issues that play a role in securing networks,
o3: Remember the fallacies in network security,
o4: Analyze the problems related to the network security and trade-offs thereof,
o5: Evaluate the security protocols that are used in the current operational networked systems.

Communication: Moodle at https://odtuclass.metu.edu.tr

Textbook (TB): Cryptography and Network Security: Principles and Practice by William Stallings, Prentice Hall, 5th Edition, 2011 (http://williamstallings.com/Cryptography/)

Supplemental Books:
Introduction to Modern Cryptography by Katz, Lindell, CRC Press, 1st Edition, 2007
Security and Cooperation in Wireless Networks, by L. Buttyan, J.P. Hubaux, Cambridge Univ., 2007
Network Security: Private Communications in a Public World by Mike Speciner, Radia Perlman, Charlie Kaufman, Prentice Hall, 2nd Edition, 2002

Prerequisites: CENG435 Data Communications and Networking, EE444 Introduction to Computer Networks or similar courses. Undergrads can take the course if they have already taken CENG435 and scored AA.

Grading:

Term project report, data-set and presentation	25+10+10%
Data-set (BONUS)	10%
Midterm	20%
Final	35%

NA Grade: If you miss the midterm and do not deliver an acceptable term project, you will get an NA grade.

Academic Honesty: There will be no tolerance to cheating in the exam and to plagiarism (copying someone else's work as if it is yours). The student who cheats will fail the course and be punished according to METU regulations. We will discuss vulnerabilities in networked systems. You should not exploit those vulnerabilities; please behave responsibly.

Course Outline: I) Introduction to Cryptography and Network Security (Chapters 1, 2.1, 2.2, 2.3) II) Block Ciphers, DES, Block Cipher Operation (Chapters 3, 5, 6) III) Pseudorandom Numbers and Stream Ciphers (Chapter 7) IV) Public-Key Cryptography, RSA, Diffie-Hellman (Chapters 9,10) V) Cryptographic Hash Functions, Message Authentication Codes (Chapter 11, 12) VI) Digital Signatures (Chapter 13) VII) Key Management and Distribution, User Authentication Protocols (Chapter 14, 15) VIII) Transport-level Security (Chapter 16) IX) WLAN Security and Network Access Control (Chapter 17) X) IP Security (Chapter 19) XI) Cellular Network Security XII) Student Presentations