ECE 710 Topic 21
Communication Security, Spring 2017

Instructor: Professor G. Gong
Office: EIT 4158, x35650, ggong@uwaterloo.ca
http://comsecuwaterloo.ca/∼ggong
Office hours: by appointment

Time: TBD

Room: TBD

Course Outline: This course introduces some timely topics in computer and communications security. It covers the advanced topics on cryptography including encryption and authentication, fully homomorphic encryption, and provable security. Network security mechanisms and protocols, network access authentication, wireless security, and radio air link protection. Broadcast and multicast key distribution, trust platforms, temple response hardware, and physical layer security. Some special topics on attacks, privacy model, and RFID for counterfeiting.

Prerequisites: ECE 409 or ECE 458, or equivalent courses taken from other departments or universities.

References:

1. L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012. Chapters 2-3, 6-10, 12-14.
2. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC, 2007.
3. Some notes and supplement materials will be provided.

Course Outline

1. Review of basics of cryptography and security: information security, protection mechanisms, confidentiality, integrity and authenticity, trust and threat model, certificate authority, and practical crypto schemes (PRG, SHA, HMAC, AES, GCM, DSS, ECC).
2. Security metrics and infrastructure of communication systems: perfect forward secrecy, computational complexity, provable security, PKI, X.509 certificates, and key escrow.
3. Network security protocols: the man-in-the-middle attacks, mutual authentication, key establishment, security association, Internet security protocols (IPsec, MAPsec, SSL/TLS), end-to-end/hop-by-hop encryption, and attacks on SSL/TLS.
4. Network access authentication: authentication and key agreement (AKA) in cellular systems, AAA, and extensible authentication protocols (EAP), tunnelled attacks on EAP/TLS, and mobile multi-channel authentication.

5. Wireless network security: special aspects of wireless protection, radio air link protection, IEEE 802.11 security solutions, and attacks.

6. Broadcasting and multicast security: multicast key distribution, hash chain broadcast message authentication, Merkle tree based authentication and signatures.

7. System security: trust platforms, temple response hardware, secure storage, wire typing channel, and physical layer security.

8. Special topics: privacy model, privacy in RFID systems, and game theoretic model for privacy, case study for cloud security.

Course Grading: The overall grade is based on assignment questions, one project and one final exam, which is distributed below.

Assignment Questions:	25%
Project (individual):	25%
Final Examination (open book exam):	50%

Course Project: A list of project problems will be given, however students are allowed to suggest problems related to their own research which should be discussed with the instructor for approval.