ECE 710 Topic 21
Communication Security, Spring 2018

Instructor: Professor G. Gong

Office: [redacted] x35650, ggong@uwaterloo.ca

http://comsecuwaterloo.ca/∼ggong

Office hours: by appointment

Time: [redacted]

Room: [redacted]

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 network security, broadcast and multicast key distribution. Advanced cryptographic algorithms for securing machine learning. Some special topics on blockchain and smart contract, privacy model, RFID for counterfeiting, and physical layer security.

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 2-10, 12, 14.
2. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, CRC, 2007.
3. A. J. Menezes and P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
4. 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, and certificate authority.
2. Security metrics and infrastructure of communication systems: perfect forward secrecy, computational complexity, provable security, PKI, X.509 certificates, and key escrow.
3. Practical symmetric-key cryptographic schemes: pseudorandom generators, stream ciphers and block ciphers, secure hash functions, message authentication code, authenticated encryption, lightweight cryptography, chosen plaintext attack (CPA) and chosen ciphertext attack (CCA).

4. Public-key cryptography: digital signature schemes, elliptic public-key cryptography ECC, identity based schemes, and fully homomorphic encryption (FHE).
5. Network security protocols: the man-in-the-middle attacks, mutual authentication, key establishment, security association, Internet security protocols (IPsec, TLS), end-to-end/hop-by-hop encryption, and attacks on TLS.
6. Network access authentication: authentication and key agreement (AKA) in cellular systems, AAA, password based authentication, Open-authorization, extensible authentication protocols (EAP), tunnelled attacks on EAP/TLS, and mobile multi-channel authentication.
7. Wireless network security: special aspects of wireless protection, radio air link protection, IEEE 802.11 security solutions, and attacks.
8. Broadcasting and multicast security: multicast key distribution, hash chain broadcast authentication, Merkle tree authentication and signatures.
9. Advanced cryptographic algorithms for securing machine learning: secret sharing, multiparty computation, and zero knowledge proof.
10. Special topics: blockchain and smart contract, privacy model, privacy in RFID systems, and wire typing channel.

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 or group of two persons):	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.

Other Resources

- Schneier on Security, http://www.schneier.com/blog/. A blog covering current computer security and privacy issues.
- BugTraq, http://www.securityfocus.com/archive/1. A full disclosure moderated mailing list for the detailed discussion and announcement of computer security vulnerabilities.
- A Graduate Course in Applied Cryptography in Stanford University: `https://crypto.stanford.edu/~dabo`

Academic Integrity, Discipline, Grievances, and Appeals

Academic Integrity: In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. [Check `www.uwaterloo.ca/academicintegrity/` for more information.]

Grievance: A student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4, `www.adm.uwaterloo.ca/infosec/Policies/policy70.htm`. When in doubt please be certain to contact the departments administrative assistant who will provide further assistance.

Discipline: A student is expected to know what constitutes academic integrity [check `www.uwaterloo.ca/academicintegrity/`] to avoid committing an academic offence, and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about rules for group work/collaboration should seek guidance from the course instructor, academic advisor, or the undergraduate Associate Dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline, `www.adm.uwaterloo.ca/infosec/Policies/policy71.htm`. For typical penalties check Guidelines for the Assessment of Penalties, `www.adm.uwaterloo.ca/infosec/guidelines/penaltyguidelines.htm`.

Appeals: A decision made or penalty imposed under Policy 70 (Student Petitions and Grievances) (other than a petition) or Policy 71 (Student Discipline) may be appealed if there is a ground. A student who believes he/she has a ground for an appeal should refer to Policy 72 (Student Appeals) `www.adm.uwaterloo.ca/infosec/Policies/policy72.htm`.

Note for Students with Disabilities: The Office for Persons with Disabilities (OPD), located in Needles Hall, Room 1132, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with the OPD at the beginning of each academic term [check `http://www.studentservices.uwaterloo.ca/disabilities/`].