ECE 716 - Communication Security
Spring 2020

Instructor: Professor G. Gong
Office: E7 5436, x45650, ggong@uwaterloo.ca
https://uwaterloo.ca/scholar/ggong
Office hours: TBA

Course Description This is an advanced course for communication security. The topics to be covered include semantic security, attack analysis, network security protocols, network access authentication, wireless security, broadcast and multicast key distribution, system security, trusted platform, IoT security and privacy, physical layer security, anti-jamming, advanced cryptography, multi-party computation, zero-knowledge proof system, and special topics on privacy of blockchain, smart contract and securing machine learning.

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

Antirequisite ECE 710 - Topic 21.

Resources

Lectures: 02:30-05:20Th, EIT 3141.

References

1. L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012.
2. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014.
3. A. J. Menezes and P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
4. Supplemental materials for the book by Chen-Gong.
5. ECE 716 Course Notes -Available on UW-LEARN.
6. Selected papers.

Course Outline

1. Basics of information and communication security: information security, protection mechanisms, confidentiality, integrity and authenticity, trust and threat model, and secure components.

2. Security metrics and infrastructure: perfect forward secrecy, provable security, pseudorandom generators, randomness criteria, and correlation attacks, PKI, X.509 certificates, and key escrow.

3. Review of practical cryptographic schemes: symmetric-key cryptography (one-time-pad, LWC, WAGE, AES, SHA3, HMAC), chosen plaintext attack (CPA) and chosen ciphertext attack (CCA), public-key cryptography (DH, DSS, RSA, EC-DH, EC-DSA).

4. Network security protocols: the man-in-the-middle attacks, mutual authentication, key establishment, cipher suite negotiation, Internet security protocols (IPsec, TLS), end-to-end/hop-by-hop encryption, and attacks on TLS.

5. Network access authentication: authentication and key agreement (AKA) in cellular systems, AAA, password based authentication, kerberos, open-authorization, EAP, tunnelled attacks, and mobile multi-channel (multi-factor) authentication.

6. Wireless Security: radio air link protection (4G-LTE/5G), IEEE 802.11 security solutions (flowed WEP, CCMP), and attacks (forgery and location).

7. Broadcasting and multicast security: multicast key distribution, hash chain broadcast authentication, Merkle tree authentication and signatures, and one-time signature.

8. Implementations and trusted platform: side-channel attacks, root of trust, secure boot, validation and authorization, secure storage, trusted platform module, and SGX.

9. IoT security and privacy: Internet-of-Things (IoT), privacy preserving identification, RFID (EPC, NFC), attacks on smart cards, and relay attacks.

10. Physical layer security: wiretap channel, wiretap code, anti-jamming attacks, channel reciprocity for authentication, bloom filter for anti-jamming, and encryption over MIMO and OFDM.

11. Advanced Cryptographic Algorithms: secret sharing, multiparty computation, commitment schemes, and zero knowledge proof systems.

12. Special Topics: privacy in blockchain and cryptocurrency, and secure machine learning for federate learning.

Course Grading

The overall grade is based on assignment questions and one project (there is no final exam due to the predicted effect for coronavirus). The due dates and score distribution are tentatively given as follows. The instructor will retain the right to change for having a final exam if the coronavirus is clear out.

		Due Date
Assignment Set 1	20%	May 25
Assignment Set 2	20%	June 15
Assignment Set 3	20%	July 13
Project (individual or group of 2)	40%	August 6

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 before May 31, 2020.

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`