ECE 716 - Communication Security
Spring 2022

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 information theoretic secrecy, semantic security, practical cryptology and attack analysis, network security protocols and access authentication, wireless network security, physical layer security and anti-jamming, broadcast and multicast key distribution, trusted platform, IoT security and privacy, RFID for counterfeiting, advanced cryptography, multi-party computation, zero-knowledge proof system, and special topics on privacy of blockchain and smart contract, differential privacy, and securing machine learning.

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

Antirequisite ECE 710 - Topic 21.

Textbook: There is no text book for this course, but I provide you the following list for references.

3. ECE 716 Course Notes -Available on UW-LEARN.
4. Selected research 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 and stream cipher, AES, SHA3, HMAC), chosen plaintext/ciphertext attacks, time-memory trade-off attacks, public-key cryptography (DH, DSS, RSA, EC-DH, EC-DSA), and faulty attacks.
4. Network security protocols: the man-in-the-middle attacks, mutual authentication, key establishment, Internet security protocols (IPsec, TLS), attacks, network access authentication, password based web authentication, kerberos, and mobile multi-channel authentication.

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.


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), lightweight cryptography, privacy preserving identification, HIB authentication protocols, and relay attacks on RFID (EPC, NFC).

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


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

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, 2022.

Other Resources

- A Graduate Course in Applied Cryptography in Stanford University: https://crypto.stanford.edu/~dabo. (From this site, you may download the text book, authored by Dan Boneh and Victor Shoup.)
