ECE 628 - Computer Network Security
Winter 2023

Instructor: Professor G. Gong

Office: E7 5436, x45650, ggong@uwaterloo.ca

https://uwaterloo.ca/scholar/ggong

Office hours: TBA

Course Description

This course focuses on the fundamental principles of how to secure computer networks. The topics to be covered include applied cryptography, encryption, authentication, and zero-knowledge proofs, semantic security, network security, trusted platform, Decentralized system security, blockchain and cryptocurrency, data privacy enhanced technologies, secure machine learning, physical layer attacks, quantum key distribution,

Background Requirements Students attending this course should have a good working knowledge of probability theory and computer networks.

Resources Lectures: 01:00-3:50Th, E5 5106

References There is no textbook for the course, but the following references will be helpful for your reading.

1. M.T. Goodrich and R. Tamassia, *Introduction to Computer Security*, Addison Wesley, 2011 (Section 3.3, Chapters 6, Sections 9.1, 9.6-9.7).
2. L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012.
3. W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th edition, Pearson, 2017 (Part Five: Chapters 22-24).
4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014 (you may read it if you wish to have a deep crypto knowledge for your future career, but not required from the course).
5. Supplemental materials for the book by Chen-Gong.
6. ECE 628 Course Notes -Available on UW-LEARN.
7. Selected papers.

Course Grading

The overall grade is based on a midterm exam (take-home exam), one project and one final exam.

Course Project

A list of project problems will be given, however students are encouraged to propose their interested problems related to the course materials which should be discussed with the instructor for approval.

Course Outline

1. Introduction to Cryptology: cryptography and cryptanalysis, confidentiality, integrity and authentication, digital signatures, active and passive attacks, and classification of cryptogrphic systems.

2. Networks, Systems and Security Metrics: points of attacks, secure infrastructure, trust and threat model, Shannon's secrecy, complexity theory, semantic security, pseudorandom generators, randomness criteria, and correlation attacks.

3. Symmetric-key Cryptographic Systems: Stream ciphers and block ciphers, lightweight cryptography, encryption models, chosen plaintext/ciphertext attack (CPA), secure hash functions, MAC, authenticated encryption, time-memory trade-off attacks.

4. Public-key Systems: security of public-key cryptography, basic schemes, digital signature, ECC, pairing-based IBC, fully homomorphic encryption, and fault attacks.

5. Network Security: the man-in-the-middle attacks, mutual authentication and key establishment, cipher suite negotiation, network security protocols (IPsec, TLS/SSL, VPN), Web security (https), and attacks on TLS

6. Wireless security: radio air link protection (4G-LTE, 5G), IEEE 802.11 security solutions (flowed WEP, CCMP), physical layer jamming and relay attacks on RFID challenge response.

7. Internet Authentication: hash chain, Merkle tree authentication, password based authentication, Kerberos, and PKI.

8. Decentralized System Security: consensus, practical Byzantine fault tolerance, blockchain, Bitcoin and cryptocurrency, smart contract, zero knowledge proofs and Zcash, and applications to supply-chain management.

9. Privacy Enhanced Technologies: differential privacy, secret sharing, multiparty computation, and secure machine learning.

10. Post-quantum and Quantum Cryptography: one-time digital signature, quantum encryption, and quantum key distribution.

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.)

- 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.