ECE 628 - Computer Network Security
Winter 2015

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

Time: 11:30-02:20Th

Room: RCH 204

Course Description

This course will deal with many aspects of cryptography, cryptanalysis, data and communications security. It covers the topics: introduction to cryptography, encryption and authentication, symmetric key and public crypto systems, provable security of crypto algorithms and protocols, cryptanalysis of crypto systems, security mechanisms and protocols, wireless security, implementation and side channel attacks, some advanced attacks, hardware protections, and applications of e-commence and radio frequency identification (RFID) systems.

Background Requirements

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

References

(a) ECE 628 Course Notes -Available on UW-LEARN.

(b) L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012.

(c) Selected papers.

Course Outline

1. Introduction to Cryptology
    - cryptography and cryptanalysis
    - information security
    - confidentiality, integrity and authentication, and digital signatures
    - wiretapping, active and passive attacks
    - requirements on secure systems
    - classification of cryptosystems

2. Theory of Secure Information Systems
    - Shannon's secrecy
    - complexity theory
    - provable security
3. Networks and Systems
    - applications of cryptography
    - points of attacks
    - security infrastructure
    - trust and threat model
    - hop-to-hop/end-to-end encryption
4. Symmetric-key Systems
    - Pseudo-random sequence/number generators, randomness criteria, nonlinear generators, Blum-Blum-Shub (BBS) generators, and correlation attacks.
    - Stream ciphers, one-time-pad, design principles, and practical stream ciphers (Grain, Trivium, WG, and Snow 3G),
    - Block ciphers, DES, AES, Simon and Speck, encryption models (ECB, CBC, CTR), and time-memory trade-off attacks.
    - Secure hash functions and MAC, MD5, SHA 1, SHA 3, Xor MAC, CBC-MAC, HMAC, GCM, and security proof.
5. Finite Field Arithmetic
    - modular arithmetic
    - Euclid's GCD
    - primality test
    - finite fields
    - CRT
    - factorization of big integers
    - discrete logarithms
6. Public Key Systems
    - security of public-key cryptography
    - RSA encryption and digital signature
    - DH key agreement
    - Digital Signature Standard (DSS)

- elliptic curve cryptography (P1363, FIPS 140)
- pairing-based IBC
- fully homomorphic encryption
- fault attacks

7. Security Mechanisms and Protocols
   - the man-in-the-middle attacks
   - mutual authentication and key establishment
   - cryptographic algorithm negotiation
   - network security protocols (IPsec, SSL/LTS, SSH, and S/MIME)
   - network access authentication (AAA, Kerberos, password based access authentication)
   - protection models
   - firewalls and VPN
   - wireless security (IEEE 802.11, 4G-LTE, Bluetooth)
8. Implementations and Applications
   - smart cards, power attacks and timing attacks
   - Internet-of-Things, near field communication (NFC) and replay attacks
   - copyright protection
   - digital rights management

Course Grading

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

Assignment Questions	20%
Project (individual)	20%
Final Examination	60%