Date: September 9, 2002
Prof.: Jean-Yves Chouinard

CSI-4138/CEG-4394 Design of Secure Computer Systems

Outline (Fall 2002)

Lectures:	Monday,	10h00 to 11h30,	HGN 302
	Wednesday,	8h30 to 10h00,	HGN 302
Laboratories:	Monday,	11h30 to 13h00,	STE 0130
	Wednesday,	10h00 to 11h30,	STE 0130
	Wednesday,	10h00 to 11h30,	STE 2052
Teaching assistants:	Alassaf, Mohamad		
	Guo, Huiping		
	Wang, Wenlan		

Textbook: *Cryptography and Network Security: Principles and Practice* by William Stallings, (second edition), Upper Saddle River, NJ: Prentice-Hall, 1999.

Grading scheme:	Assignments and labs:	**25%**
	Midterm examination:	**25%**
	Final examination:	**50%**

Course description:

Security policies. Security mechanisms. Physical security. Security awareness. User authentication. Application security mechanisms. Encryption. External and internal firewalls. Security of operating systems and software. Security of e-commerce applications. Design of security system and components. Devices for security analysis; sniffers, attack detectors. Information warfare. Ethical issues in computer security.

Prerequisites: CEG-3182 *Networking and Internetworking*, or
CSI-3103 *Data Transmission and Computer Networks*, or
SEG-3150 *Telecommunications Software Engineering*

Course Outline

- Overview of security threats and countermeasures in computer communications*(chapter 1)*
- Conventional (symmetric) encryption and decryption methods and cryptanalysis:*(chapters 2, 3, 4 and 5)*
- Classical encryption methods
- Modern encryption methods: DES, Triple DES, IDEA, RC5
- End-to-end encryption and link encryption
- Key distribution techniques
- Public-key encryption: *(chapters 6 and 7)*
- Diffie-Hellman public-key principle
- Diffie-Hellman key exchange protocol
- Rivest-Shamir-Adleman public-key encryption
- Overview of number theory and modular arithmetics
- Elliptic curve cryptography
- Authentication and digital signatures: *(chapters 8, 9, 10 and 11)*
- Authentication
- Hash functions
- Message authentication code (MAC)
- Digital Signature Standard (DSS)
- Kerberos authentication protocol
- Security in electronic communications: *(chapters 12, 13 and 14)*
- Electronic mail security:
- Pretty Good Privacy (PGP)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- Internet Protocol (IP) security
- World Wide Web (WWW) security:
- Secure Sockets Layer (SSL)
- Secure Electronic Transaction (SET)
- Computer service attacks and countermeasures *(chapters 15 and 16)*
- Intruders, virus, and worms
- Firewalls

Some reference books:

[1] Charles P. Fleeger, *Security in Computing*, second edition, Prentice-Hall, Upper Saddle River, NJ, 1997.

[2] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, second edition, John Wiley and Sons, New-York, 1996.

[3] Alfred J. Menezes, Paul C. van Oorschot, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1997.

[4] Douglas R. Stinson, *"Cryptography: Theory and Practice"*, CRC Press, Boca Raton, 1995.

[5] Dorothy Elizabeth Robling Denning, *Cryptography and Data Security*, Addison-Wesley, 1982.