UNIVERSITY COLLEGE of the FRASER VALLEY

PAC FORM #2

COURSE IMPLEMENTATION DATE:[January 2003]

COURSE TO BE REVIEWED DATE:[September 2006]
(Four years after implementation date)

OFFICIAL COURSE OUTLINE INFORMATION

Students are advised to keep course outlines in personal files for future use.

Shaded headings are subject to change at the discretion of the department and material will vary - see course syllabus available from instructor

FACULTY/DEPARTMENT: Computer Information Systems

COMP 490		3
COURSE NAME/NUMBER	FORMER COURSE NUMBER	UCFV CREDITS

Network Security and Cryptography
COURSE DESCRIPTIVE TITLE

CALENDAR DESCRIPTION:

This course provides students with an understanding of important concepts in network security and cryptography. A practical technological survey of cryptography and network security will be given. This includes conventional encryption algorithms such as DES and IDEA, public-key design and algorithms such as RSA and elliptic curve, digital signatures and authentication protocols, key managements, and applications of authentication such as Kerberos and X.509. IP security and web security will also be covered. Network security plans and procedures will be formulated at the end.

PREREQUISITES: MATH 106, CIS 390 with a grade of C or better, and acceptance to CIS degree program

COREQUISITES: None

SYNONYMOUS COURSE(S)
(a) Replaces: _____ *(Course #)*
(b) Cannot take _____ for further credit *(Course #)*

SERVICE COURSE TO:
_____ *(Department / Program)*
_____ *(Department / Program)*

TOTAL HOURS PER TERM: 45

STRUCTURE OF HOURS:

Lectures:	45	hrs
Seminar:		hrs
Laboratory:		hrs
Field Experience:		hrs
Student Directed Learning:		hrs
Other (Specify):		hrs

TRAINING DAY-BASED INSTRUCTION
LENGTH OF COURSE: _____
HOURS PER DAY: _____

MAXIMUM ENROLMENT: 35

EXPECTED FREQUENCY OF COURSE OFFERING: Once every year

WILL TRANSFER CREDIT BE REQUESTED? YES _____ NO X

TRANSFER CREDIT EXISTS IN BCCAT TRANSFER GUIDE: YES _____ NO X

AUTHORIZATION SIGNATURES:

Course designer(s): Edward Lo
Chairperson: _____ *(Curriculum Committee)*
Department Head: Paul Franklin
Dean: Karen Evans
PAC Approval in Principle Date: _____
PAC Final Approval Date: 2002 10 30

LEARNING OBJECTIVES / GOALS / OUTCOMES/ LEARNING OUTCOMES:

Students will explore network security and cryptography. At the end of this course, the student will have gained knowledge of:

- Conventional encryption algorithms
- Public-key encryption
- Digital signatures and authentication protocols
- E-mail security
- IP and web security
- Network security practices
- Identification of security issues in an IT deployment plan
- Intrusion detection and responses
- Various network security attacks and violations
- Network security plans and procedures

This will provide the student with the basic skills required in the network security industry.

METHODS: Lecture

PRIOR LEARNING ASSESSMENT RECOGNITION (PLAR):

Credit can be awarded for this course through PLAR YES _____ NO ___X___

METHODS OF OBTAINING PLAR: Not Applicable

TEXTBOOKS, REFERENCES, MATERIALS:

Cryptography and Network Security: Principles and Security, 3rd Edition, William Stallings, Prentice-Hall, 2002.

Network Security Essentials: Applications and Standards, William Stallings, Prentice-Hall, 2000.

The CERT Guide to System and Network Security Practices, Julia H. Allen, Addison-Wesley, 2001.

Linux System Security, Scott Mann and Ellen L. Mitchell, Prentice-Hall, 2000.

Windows 2000 Security: Technical Reference, Internet Security Systems, Inc., Microsoft Press, 2000.

SUPPLIES / MATERIALS:

STUDENT EVALUATION:

participation	10%
assignments and a project	30%
mid term exam	20%
final exam (comprehensive)	40%

COURSE CONTENT:

Various type of security attacks.
The Network access security model.
Classical and modern conventional encryption techniques.
Algorithms of conventional algorithms
Pubic-key encryption
Digital signatures and authentication protocols
Applications of authentication
Email security
IP and Web security
System and network security procedures
Security issues and requirements
Intrusion detection and response preparation
Detecting intrusions
Responding to intrusions