Douglas College

EFFECTIVE: JANUARY, 2009
CURRICULUM GUIDELINES

A.	Division:	Education	Effective Date:	January, 2009			
B.	Department / Program Area:	Commerce & Business Admin. Computing Science And Information Systems	Revision			New Course	X
			If Revision, Section(s) Revised:				
			Date of Previous Revision:				
			Date of Current Revision:				

C: CSIS3150 **D**: NETWORK SECURITY **E:** 3

Subject & Course No.	Descriptive Title	Semester Credits

F: Calendar Description:

This course provides the student with fundamental understanding of network security from a network administrator's perspective. The student will learn the concepts and technologies required to secure a network. Viruses, worms and Trojans are discussed and the student will learn to implement secured network infrastructure and security policy. Topics include risk analysis, network protocols, architecture security, types of attacks, authentication, encryption, network security applications and appliances, firewalls, virtual private network and intrusion detection system. The student will learn how to make networks secure with the use of tools to analyze traffic and study attacks.

G: Allocation of Contact Hours to Type of Instruction / Learning Settings

Primary Methods of Instructional Delivery and/or Learning Settings:

Lectures and Seminars

Number of Contact Hours: (per week for each descriptor)

Lecture:	2 Hours per week
Seminar/Lab:	2 Hours per week
Total:	4 Hours per week

Number of Weeks per Semester:

15 Weeks X 4 Hours per Week = 60 Hours

H: Course Prerequisites:

CSIS2350 or CISY3445

I: Course Corequisites:

NIL

J: Course for which this Course is a Prerequisite

NIL

K: Maximum Class Size:

20

L: PLEASE INDICATE**:**

	Non-Credit
	College Credit Non-Transfer
X	College Credit Transfer:

SEE BC TRANSFER GUIDE FOR TRANSFER DETAILS (www.bctransferguide.ca)

M: Course Objectives / Learning Outcomes

The student will be able to:

1) describe security terminologies, management models, policy requirements and industries best practice;
2) describe security issues in OSI protocols;
3) conduct basic risk analysis and identify security vulnerability in enterprise network systems;
4) describe cryptographic algorithms, their characteristics and application to network security;
5) design and implement secure network infrastructure with network security components such as VLAN, VPN, firewall and/or proxy servers;
6) analyze network traffic and protocols using tools such as tcpdump, ethereal or other packet sniffers.

N: Course Content

1) Introduction to Security Management Practices
   - information security framework (e.g. ISO17799 or COBIT)
   - security models, confidentiality, integrity and availability
   - security evaluation criteria (e.g. TCS, ITSEC)
   - risk analysis, administrative control and security policies
2) Password Management And User Authentication
   - password management and attack methods (e.g. dictionary attack)
   - hash functions (SHA1, SHA2) and shadow password
   - challenge response authentication, mutual authentication, Kerberos authentication
   - man-in-the-middle attack
3) Cryptography And Key Management
   - review on cryptography (perfect secrecy, cipher text)
   - symmetric and asymmetric cryptography (block ciphers, DES, 3DES and AES)
   - asymmetric cryptography, message integrity and digital signature,
   - key exchange algorithm and key management
   - Public Key Infrastructure (PKI)
4) Virtual Private Network
   - introduction to VPN (PPTP, Site-to-site VPN, Client based VPN)
   - IPSec Negotiation, IKE authentication mechanism
   - encryption, integrity checking and packet encapsulation in IPSec
   - site-to-site VPN vs. client-based VPN
   - dead peer discovery mechanism
5) Network Infrastructure And Perimeter Protection
   - firewall topology and implementation, NAT, security zone and demilitarized zone
   - physical security, device redundancy, router security and VLAN switch
   - port control, packet filtering, session filtering, circuit gateway, application gateway
   - device based firewall vs. host based firewall
6) Protocol Security
   - OSI protocol analysis and sniffing tools
   - routing protocol security - RIP, OSPF, BGP routing protocols (router authentication, directed broadcast control, black hold filtering, unicast reverse path forwarding, path integrity)
   - ICMP protocol security (smurf attack, ping of death, syn flooding attack)
   - IP security (spoofing, hijacking, injection and DoS by connection reset)
   - data link layer security issue (IP permit lists, protocol filtering and control, LAN flooding)
7) Application Level Security
   - authentication applications (Kerberos, X.509, PKI)
   - network service security (SNMP, DNS, NAT)
   - electronic mail security (PEM, PGP, S/MIME)
   - Web security and e-commerce (SSL, TLS, HTTPS, SET)
   - fault tolerance mechanisms
8) Intrusion Detection And Prevention
   - malicious software (virus, worms, Trojan Horse) , denial of service and buffer overflow attack
   - network traffic signature, port scanning and activity monitoring
   - host based and network based IDS deployment
   - intrusion detection system and incident response
   - SMTP gateway and proxy server

9) Wireless Security
- wireless architecture and standards (802.11, 802.15, 802.16)
- SSID, shared key authentication, WEP, EAP, WAP
- defences against war driving

O: Methods of Instruction
Lecture, seminar, demonstration, and hands-on assignments/projects

P: Textbooks and Materials to be Purchased by Students
William Stallings. Network Security Essentials: Applications and Standards. Latest edition. Prentice Hall.

Q: Means of Assessment

Lab Assignments	20% - 35%
Participation	0% - 10%
Quizzes	5% - 20%
Midterm Examination	25% - 30%
Final Examination	25% - 30%
Total	100%

R: Prior Learning Assessment and Recognition: specify whether course is open for PLAR
Yes

Course Designer(s): Hugh Poon / Raymond Yu

Education Council / Curriculum Committee Representative

Dean: Rosilyn G. Coulson

Registrar: Trish Angus