NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 262 - NETWORK COMMUNICATION, SECURITY AND AUTHENTICATION (4 CR.)

Current information on NOVA's Cybersecurity Program is located at www.nvcc.edu/cybersecurity

Course Description
Covers an in-depth exploration of various communication protocols with a concentration on TCP/IP. Explores communication protocols from the point of view of the hacker in order to highlight protocol weaknesses. Includes Internet architecture, routing, addressing, topology, fragmentation and protocol analysis, and the use of various utilities to explore TCP/IP. Lecture 4 hours per week.

General Course Purpose
This course provides a "deep dive" into TCP/IP and other networking protocols and technologies. The student will learn how to use packet sniffing tools, such as Wireshark, to review network traffic to detect attack signatures and will be able to demonstrate, when provided with specific attack scenarios, an understanding of how to apply encryption and authentication technologies, such as IPSec and SSL, as countermeasures to such attacks. This course also includes content, as indicated below in parenthesis behind each learning objective, that directly maps to DHS/NSA's Center of Academic Excellence – 2 Year (CAE2Y) criteria.

Course Prerequisites/Corequisites
ITN 260

Course Objectives
Upon successful completion of this course, the student will have a working knowledge of:

A. Network Security Policy.
B. TCP/IP Protocol, Application Services and utilities.
C. Network Authentication and Encryption.
D. Wireless Security

Course Content
1.0 Network Security Policy
2.0 Security Design Principles
3.0 TCP/IP Protocols
4.0 Network Authentication
5.0 Network Encryption
6.0 Wireless Security
7.0 Required Additional Topics

Student Learning Outcomes

1.0 Network Security Policy
1.1 Describe Authorization, Authentication, Confidentiality and Non-Repudiation.
1.2 Define risk management and its role in creating the network security policy.
1.3 Describe the risk management phases and the activities associated with each phase.
1.4 Define the process of identifying attack surfaces/vectors and attack trees (CT9, CT10).
1.5 Describe network security goals, philosophy and decisions related to creating a security policy.
1.6 Define the difference between policies, standards, guidelines and procedures.
1.7 Explain the elements of the security policy as it relates to users, maintenance personnel, contractors, clearances, position description and sensitivity.
1.8 Describe administrative security control as it relates to such topics as attribution, passwords, copyrights and classification of media and its handling.
1.9 Describe the Security Assessment and Authorization (SAA) and other compliance methods for ensuring that systems are compliant with security policies.

.

2.0 Security Design Principles
2.1 .Understand the role of security design as an enforcer/implementation tool for desired security policies.

2.2 Describe the Security System Development Life Cycle (IA4).
2.3 Understand basic security design roles, including the role of separation (of domains) and isolation, simplicity of design, minimization of implementation, fail safe defaults vs. fail secure, modulatory, layering, principle of Least Astonishment, open design, and usability.(FS1, FS2, FS4, FS5, FS6, FS7, FS8, FS10, FS11, FS11).
2.4 Describe the system mode of operation (i.e. compartmented/partitioned, dedicated, multilevel, system-high) and the impact to security architecture and policy.
2.5 Describe security models, including Bell La-Padula, Biba, Clark-Wilson, Non-Interference Model, Chinese Wall and others,
2.6 Analyze common security failures and identify specific design principles that have been violated. (FS)
2.7 When provided with a specific scenario, be able to identify the needed design principle to resolve the security problem. (FS)
2.8 Be able to understand the importance of minimizing the effects of security mechanisms to enable usability and describe why good human machine interfaces are important to system use. (FS)
2.9 Be able to examine the architecture of a typical complex system and identify significant vulnerabilities, risks, and points at which specific security technologies/methods should be employed.(IA)

3.0 TCP/IP

3.1 Describe the encapsulation process and its employment in the OSI model.
3.2 Explain attacks against the data link layer, network and transport protocols.
3.3 Explain the use of firewalls and other security devices in defending against attacks on network protocols.
3.4 Explain the employment and operation of the Network Address Translation (NAT).
3.5 Explain the employment and operation of TCP Wrappers.
3.6 Explain the employment and operation of security protocols such as SSL, TLS, and IPSec.(CD3)

4.0 Network Authentication

4.1 Recognize how authentication, authorization and identification techniques are used to protect the network.
4.2 Describe the three major authentication principles (factors).
4.3 Describe the most common attacks against passwords, smart cards (i.e. microprobing), and biometrics and the defense against those attacks, including multifactor authentication and HSPD-12. (CT4)
4.4 Describe False Acceptance Rates (FARs), False Rejection Rates (FRRs), and Cross-Over Error Rates (CER) and the impact on FARs and FRRs when tuning biometric systems.
4.5 Explain the employment of Kerberos and other authentication protocols, their operation, strengths and weaknesses.

5.0 Network Encryption

5.1 Explain the security functions of cryptography (confidentiality, integrity, and authentication). (CD3, CR10)
5.2 Define such terms as encryption, cryptography, cryptanalysis, encryption key, and encryption algorithm.
5.3 Explain and identify common symmetric key cryptosystems, their strengths and weaknesses.(CR1)
5.4 Explain asymmetric key cryptosystems, their strength and weaknesses. (CR1)
5.5 Understand the function and operation of the /AES encryption algorithm and the evolution from DES to AES.(CR1)
5.6 Understand the function and operation of the Diffie-Hellman key exchange.
5.7 Understand the function and operation of the RSA encryption algorithm.(CR2)
5.8 Explain the function and operation of digital signatures.
5.9 Explain the function and operation of the Public Key Infrastructure (PKI), including the role of the CA and protection of the keying material and CA environment.(CR2)
5.10 Explain the function and operation of the common hashing algorithms(MD4, MD5, SHA-1, SHA-2, SHA-3) for protecting integrity, protecting authentication data, and their relative resistance to collisions, (CR3)
5.11 Explain the Digital Signature Standard (DSS) . (CR4)
5.12 Explain the function and operation of common cryptographic protocols such as SSL and IPSec and theiruse in Virtual Private Networks. (CD4, CR8)

5.13 Explain Key Management (creation, exchange/distribution issues, revocation, suspension, escrow). (CR5)

5.14 Explain the different types of cryptographic attacks, including brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.) (CR7),

6.0 Wireless Security

6.1 Explain cellular-based wireless systems and Wireless Local Area networks.

6.2 Describe current attacks on mobile phones and wireless systems.

6.3 Describe the various components of the Wireless Local Area Network.

6.4 Describe the different Wireless Local Area Network types.

6.5 Describe the operation of CSMA/CA.

6.6 Describe wireless topology.

6.7 Describe WEP, WPA, and WPA2 and their advantages and vulnerabilities. Describe the various mobile and wireless threats and their mitigations. (CT4)

7.0 Required Additional Topics

7.1 Describe emanations security, including TEMPEST and the various elements and requirements of TEMPEST security, including attenuation, banding, cabling, filtered power, grounding, shielding, TEMPEST separation, and zone of control/zoning.

7.2 Social engineering techniques. (CT6)

Required Time Allocation per Topic

In order to standardize the core topics of ITN 263 so that a course taught at one campus is equivalent to the same course taught at another campus, the following student contact hours per topic are required. Each syllabus should be created to adhere as closely as possible to these allocations. Of course, the topics cannot be followed sequentially. Many topics are taught best as an integrated whole, often revisiting the topic several times, each time at a higher level. There are normally 60 student-contact-hours per semester for a four credit course. (This includes 15 weeks of instruction and does not include the final exam week so 15* 4 = 60 hours. Sections of the course that are given in alternative formats from the standard 16 week section still meet for the same number of contact hours.) The final exam time is not included in the time table. The category, Other Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.

Topic	Time in Hours	Percentages
Network Security Policy	8	13%
Security Design Principles	8	13%
TCP/IP Protocols	16	27%
Network Authentication	6	10%
Network Encryption	6	10%
Wireless Security	3	5%
Required Additional Topics	1	2%
Exams, Quizzes	4	7%
Optional Topics	8	13%
Total	60	100%