NVCC COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 220 - WIRELESS – NETWORK SECURITY (W-NS) (3 CR.)

COURSE INFORMATION

Provides instruction in design and implement security systems in a wireless windows network environment. Course content includes use of wireless, Internet, and windows-based protocols and management techniques in wireless security systems.

Lecture – 3 hours per week

CO-REQUISITES OR PRE-REQUISITES

Prerequisite is ITN 120 and pre- or co-requisite is ITN 208. Students must be able to read and write at a college level.

COURSE OBJECTIVES+

Upon completion of this course, the student will be able to:

- Explain how to conduct a Risk Assessment
- Discuss Threat Analysis and Hacking Methodology
- Explain Rudimentary Security Measures
- Explain Intermediate Security Measures
- Explain Advanced Security Measures
- Discuss various WLAN Auditing Tools
- Discuss Hardware and Software Security Solutions
- Define and explain Prevention and countermeasures
- Discuss WLAN Security Implementation and Management

COURSE CONTENT

- Risk Assessment
- Threat Analysis and Hacking Methodology
- Rudimentary Security Measures
- Intermediate Security Measures
- Advanced Security Measures
- WLAN Auditing Tools
- Hardware and Software Security Solutions
- Prevention and countermeasures
- Implementation and Management

STUDENT LEARNING OUTCOMES

RISK ASSESSMENT

- Assets to protect
- Threats to protect against
- Legal protection
- Costs
- Basic security measures
- Threat analysis
- Impact analysis
THREAT ANALYSIS AND HACKING METHODOLOGY

- Target profiling
- Physical security
- Social engineering
- Wireless bridges
- Packet analysis
- Information theft
- Malicious data insertion
- Denial of Service (DoS)
- Peer-to-peer hacking
- Unauthorized control

RUDIMENTARY SECURITY MEASURES

- SSID
- MAC filters
- Static WEP
- Default configurations
- Firmware upgrades
- Physical security
- Periodic inventory

INTERMEDIATE SECURITY MEASURES

- Rogue equipment
- Cell sizing
- Protocol filters
- SNMP
- Discovery protocols
- Wireless segment configuration
- Removing vulnerabilities
- Client security
- IP Services

ADVANCED SECURITY MEASURES

- Wireless security policy
- Authentication and encryption
- Wireless DMZ and VLANs
- Audits
- Traffic pattern analysis
- Authenticated DHCP

WIRELESS LAN AUDITING TOOLS

- Discovery tools
- Password crackers
- Share enumerators
- Network management and control
- Wireless protocol analyzers
• Manufacturer defaults
• Password sniffers
• Antennas and WLAN equipment
• OS fingerprinting and port scanning
• Application sniffers
• Networking utilities
• Network discovery and management
• Hijacking users
• RF Jamming and Dataflooding tools
• WEP crackers

HARDWARE AND SOFTWARE SOLUTIONS

• RADIUS with AAA Support
• RADIUS Details
• Kerberos
• Static and Dynamic WEP and TKIP
• 802.1x
• Extensible Authentication Protocol (EAP)
• VPNs
• Encryption Schemes
• Routers
• Switch-Repeaters
• Firewalls
• MobileIP VPN Solutions
• Enterprise Wireless Gateways
• Switches, VLANs, & Hubs
• SSH2 Tunneling & Port Redirection
• Thin Client Solutions

PREVENTION AND COUNTERMEASURES

• 802.1x
• 802.11i
• TKIP
• AES
• Intrusion detection
• US Federal and state laws

IMPLEMENTATION AND MANAGEMENT

• Design and implementation
• Equipment configuration and placement
• Interoperability and layering
• Security management