KU Element Check List: 2014 Optional Knowledge Units – All Programs

3.0 Optional Knowledge Units

3.1 Advanced Cryptography

The intent of this Knowledge Unit is to provide students with knowledge of cryptographic algorithms, protocols, and their uses in the protection of information in various states.

3.1.1 Topic(s):
- ____ Number Theory
- ____ Probability and Statistics
- ____ Understanding of the major algorithms (AES, RSA, EC)
- ____ Suite B Algorithms
- ____ Understanding of the families of attacks (differential, man-in-the-middle, linear, etc.)
- ____ Hashing and Signatures
- ____ Key Management
- ____ Modes and appropriate uses
- ____ Classical Cryptanalysis (a la Konheim)
- ____ Identity-based Cryptography
- ____ Digital Signatures
- ____ Virtual Private Networks
- ____ Quantum Key Cryptography

3.1.2 Outcome(s):
Students will be able to:
- ____ Describe how various cryptographic algorithms and protocols work.
- ____ Evaluate security mechanisms based on cryptography.
- ____ Describe the application of cryptography in SSL, virtual private networks, secure storage, and other security applications.
- ____ Take a mode or protocol diagram and identify how an error propagates through the cryptosystem.

3.2 Advanced Network Technology & Protocols

The intent of this Knowledge Unit is to provide students with an understanding of the latest network technologies and more complex security issues involved in network communications. Examples include (but not limited to): software defined networking, converged voice/data networking.

3.2.1 Topic(s):
- ____ *Routing algorithms and protocols
  - ____ Software Defined Networking
- ____ Principles, protocols, implications
- ____ IPv6 Networking Suite
- ____ BGP
- ____ Quality of Service
- ____ Network Services
- ____ Social Networks
- ____ Network Topologies
- ____ Voice over IP (VoIP)
- ____ Multicasting
- ____ *Advanced Network Security Topics
  - ____ Secure DNS, Network Address Translation, Deep Packet Inspection, Transport Layer Security

3.2.2 Outcome(s):
Students will be able to:
- ____ Describe current networking technologies and trends.
- ____ Describe and discuss data network architectures and protocols, to include their advantages and disadvantages, applications, and security issues.

* = Can include a summary justification for that section.

KU Element Check List: 2014 Optional Knowledge Units – All Programs

3.3 Algorithms
The intent of this Knowledge Unit is to provide students with the ability to select and apply algorithms to solve specific problems and to analyze the effectiveness of algorithms in context.

3.3.1 Topic(s):
____ Algorithm Analysis
____ Computational Complexity
____ Best/Worst/Average Case Behavior
____ Optimization
____ Searching / Sorting

3.3.2 Outcome(s):
Students will be able to:
____ Describe how to perform an analysis of algorithms to determine best and worst case behavior.

3.4 Analog Telecommunications Systems
The intent of this Knowledge Unit is to provide students with a basic knowledge of the architectures and issues associated with analog communications systems.

3.4.1 Topic(s):
____ Signaling Methods
____ Architecture
____ Trunks, Switching
____ Grade of Service
____ Blocking
____ Call Arrival Models
____ Interference Issues

3.4.2 Outcome(s):
Students will be able to:
____ Describe the basic concepts of modern analog communications systems, using block diagrams.
____ Briefly describe concepts such as the different types of modulation and their advantages and applications, bandwidth, noise and the importance of the signal-to-noise ratio.

3.5 Cloud Computing
The intent of this Knowledge Unit is to provide students with a basic understanding of the technologies and services that enable cloud computing, different types of cloud computing models and the security and legal issues associated with cloud computing.

3.5.1 Topic(s):
____ Virtualization platforms
____ *Cloud Services
_____ SaaS, PaaS, DaaS, IaaS
____ Service Oriented Architectures
____ *Deployment Models
_____ private, public, community, hybrid
____ Security
____ Storage
____ Legal/Privacy Issues

3.5.2 Outcome(s):
Students will be able to:
____ Describe each type of service/model of cloud computing
____ Compare and contrast: local resource requirements, local control, network requirements, and security (attacks, mitigations, overall vulnerability)

3.6 Cybersecurity Planning and Management
The intent of this Knowledge Unit is to provide students with the ability to develop plans and processes for a holistic approach to cybersecurity for an organization.

3.6.1 Topic(s):
____ CBK
____ Operational, Tactical, Strategic Plan and Management
____ Business Continuity / Disaster Recovery
____ C-Level Functions
____ Making Cybersecurity a strategy (part of core organizational strategy)
____ Change control

3.6.2 Outcome(s):
Students will be able to:
____ Examine the placement of security functions in a system and describe the strengths and weaknesses
____ Develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response.
____ *Develop system specific plans for:
____ The protection of intellectual property
____ The implementation of access controls, and
____ Patch and change management.

3.7 Data Administration
The intent of this Knowledge Unit is to provide students with methods to protect the confidentiality, integrity, and availability of data throughout the data life cycle.

3.7.1 Topic(s):
____ Big Data
____ Hadoop / Mongo DB / HBASE
____ Data Policies
____ Data Quality
____ Data Ownership
____ Data Warehousing
____ Long Term Archival
____ Data Validation
____ Data Security (access control, encryption)

3.7.2 Outcome(s):
Students will be able to:
____ Identify relevant security issues given a system and data management structure

3.8 Data Structures
The intent of this Knowledge Unit is to provide students with an understanding of the basic abstract data types, associated operations and applying them to solve problems.

3.8.1 Topic(s):
____ Strings, Lists, Vectors, Arrays
____ Heaps, Queues, Stacks, Buffers
____ Searching and Sorting
____ Trees
____ Data Formats

3.8.2 Outcome(s):
Students will be able to:
____ List the most common structures and data formats for storing data in a computer system.
____ Discuss the advantages and disadvantages of different data structures/formats.

3.9 Database Management Systems

The intent of this Knowledge Unit is to provide students with the skills to utilize database management system to solve specific problems.

3.9.1 Topic(s):

____ Overview of database types (e.g., flat, relational, network, object-oriented)
____ SQL (for queries)
____ Advanced SQL (for DBMS administration – e.g., user creation/deletion, permissions and access controls)
____ Indexing, Inference, Aggregation, Polyinstantiation
____ How to protect data (confidentiality, integrity and availability in a DBMS context)
____ Vulnerabilities (e.g., SQL injection)

3.9.2 Outcome(s):

Students will be able to:

____ List the most common structures for storing data in a database management system.
____ Configure a commodity DBMS for secure access.
____ Describe alternatives to relational DBMSs and their unique security issues.
____ Describe the role of a database, a DBMS, and a database server within a complex system supporting multiple applications.
____ Demonstrate basic SQL proficiency for table creation, data insertion and data query.
____ Describe DBMS access controls and privilege levels and apply them to a simple database.
____ Develop a DB structure for a specific system/problem.

3.10 Digital Communications

The intent of this Knowledge Unit is to provide students with knowledge of the protocols and methodologies used in modern digital communications systems.

3.10.1 Topic(s):

____ Components of a digital communications system
____ Digital Signaling
____ Spread Spectrum Signals
____ *Multi-User Communication Access Techniques
____ CDMA, TDMA, FDMA, SDMA, PDMA

3.10.2 Outcome(s):

Students will be able to:

____ Describe digital communications systems in terms of subsystems and modulation techniques.
____ Describe the current state of the art in digital communications.
____ Compare and contrast different approaches to digital communications and describe the advantages and disadvantages of each.

3.11 Digital Forensics

The intent of this Knowledge Unit is to provide students with the skills to apply forensics techniques throughout an investigation life cycle with a focus on complying with legal requirements.

3.11.1 Topic(s):

_____ *Legal Compliance
    _____ Applicable Laws
    _____ Affidavits
    _____ How to Testify
    _____ Case Law
    _____ Chain of custody
_____ *Digital Investigations
    _____ E-Discovery
    _____ Authentication of Evidence
    _____ Chain of Custody Procedures
    _____ Metadata
    _____ Root Cause Analysis
    _____ Using Virtual Machines for Analysis

3.11.2 Outcome(s):

Students will be able to:

_____ Discuss the rules, laws, policies, and procedures that affect digital forensics
_____ Use one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.
_____ Describe the steps in performing digital forensics from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, through the completion of legal proceedings.

3.12 Host Forensics

The intent of this Knowledge Unit is to provide students with the ability to apply forensics techniques to investigate and analyze a host in a network.

3.12.1 Topic(s):

_____ File Systems and File System Forensics
_____ Hypervisor Analysis
_____ Registry Analysis
_____ Cryptanalysis
_____ Rainbow Tables
_____ Steganography
_____ Networking Concepts, Services, Protocols
_____ Operating Systems Concepts
_____ Live System Investigations
_____ (must include hands-on activities)

3.12.2 Outcome(s):

Students will be able to:

_____ Describe what can/cannot be retrieved from various OSes.
_____ Describe the methodologies used in host forensics.

3.13 Device Forensics

The intent of this Knowledge Unit is to provide students with the ability to apply forensics techniques to investigate and analyze a device.

3.13.1 Topic(s):
____ Mobile Device Analysis
____ Tablets
____ SmartPhones
____ GPS
____ (must include hands-on activities)

3.13.2 Outcome(s):
Students will be able to:
____ Describe methods for the acquisition/analysis of mobile devices (e.g., device storage, system data, cell tower logs).
____ Explain the legal issues related to mobile device forensic activities.

3.14 Media Forensics

The intent of this Knowledge Unit is to provide students with the ability to apply forensics techniques to investigate and analyze a particular media in context.

3.14.1 Topic(s):
____ Drive Acquisition
____ *Authentication of Evidence
____ Verification and Validation
____ Hashes
____ Metadata
____ Live vs. Static Acquisition
____ Sparse vs. Full Imaging
____ Slack Space
____ Hidden Files/clusters/partitions
____ (must include hands-on activities)

3.14.2 Outcome(s):
Students will be able to:
____ Describe methods and approaches for forensic analysis on specified media.

3.15 Network Forensics

The intent of this Knowledge Unit is to provide students with the ability apply forensics techniques to investigate and analyze network traffic.

3.15.1 Topic(s):
____ Packet Capture and Analysis
____ Intrusion Detection and Prevention
____ Interlacing of device and network forensics
____ Log-file Analysis
____ Forensic Imaging and Analysis
____ (must include hands-on activities)

3.15.2 Outcome(s):
Students will be able to:
____ Describe the methodologies used in network forensics.
____ Analyze and decipher network traffic, identify anomalous or malicious activity, and provide a summary of the effects on the system.

3.16 Embedded Systems

The intent of this Knowledge Unit is to provide students with the ability to develop applications that run on embedded devices while complying with device constraints.

3.16.1 Topic(s):
_____ Real-time Operating Systems
_____ Microcontroller architectures
_____ Interrupt handling and timing issues
_____ Resource management in real time systems
_____ C Programming
_____ Java, JavaScript or some other runtime programming environment

3.16.2 Outcome(s):
Students will be able to:
_____ Discuss embedded system architectures, real time OS issues such as concurrency and synchronization, and real time resource management.

3.17 Forensic Accounting

The intent of this Knowledge Unit is to provide students with the ability to apply forensics techniques to respond to and investigate financial incidents.

3.17.1 Topic(s):
_____ Investigative Accounting
_____ Fraudulent Financial Reporting
_____ Misappropriation of Assets
_____ Indirect Methods of Reconstructing Income
_____ Money Laundering
_____ Transnational financial flows
_____ Litigation services
_____ Evidence Management
_____ Economic Damages and Business Valuations

3.17.2 Outcome(s):
Students will be able to:
_____ Describe common forms of financial statement fraud and related detection techniques.
_____ Describe and implement methods of indirectly estimating concealed revenue and income.
_____ Describe common methods of money laundering and related methods of prevention and detection (including related laws and regulations).
_____ Compute loss, damages, and business value for occurrences of fraud, theft and fraudulent financial statements.

3.18 Formal Methods

The intent of this Knowledge Unit is to provide students with a basic understanding of how mathematical logic can be applied to the design of secure systems.

3.18.1 Topic(s):
_____ Concept of Formal Methods
_____ Mathematical Logic
_____ *Applications
　　_____ Role in system design
　　_____ Role in software engineering
_____ Limitations
_____ Bell-LaPadula (as an example formal model)
_____ Automated Reasoning Tools
_____ System Modeling and Specification
_____ Proofs and Verification

3.18.2 Outcome(s):
Students will be able to:
_____ Apply formal security policy models to real world scenarios.

* = Can include a summary justification for that section.

3.19 Fraud Prevention and Management

The intent of this Knowledge Unit is to provide students with the necessary knowledge to develop plans and processes for a holistic approach to preventing and mitigating fraud throughout the system lifecycle.

3.19.1 Topic(s):

____ Symptom Recognition
____ Data Driven Detection
____ Investigation of Theft
____ Concealment
____ Conversion Methods
____ Inquiry and Reporting
____ Financial, Revenue and Inventory
____ Liability and inadequate disclosure
____ Consumer fraud

3.19.2 Outcome(s):

Students will be able to:

____ Describe the components of the fraud triangle – necessary condition for fraud.
____ Describe the cost and effectiveness of common fraud detection and prevention methods.
____ Analyze record keeping and management procedures for assets and to identify/correct weaknesses.
____ Describe legal and ethical requirements for detecting, preventing and reporting fraud.
____ Describe investigative procedures for fraud.
____ Describe common methods of financial statement fraud.

3.20 Hardware Reverse Engineering

The intent of this Knowledge Unit is to provide students with an introduction to the basic procedures necessary to perform reverse engineering of hardware components to determine their functionality, inputs, outputs, and stored data.

3.20.1 Topic(s):

____ *Principles of Reverse Engineering
    ____ Stimulus, Data Collection, Data Analysis
    ____ Specification development
    ____ Capability Enhancement / Modification Techniques
    ____ Detecting Modification
____ Stimulation Methods / Instrumentation (probing and measurement)
____ JTAG IEEE 1149.1
____ Defining and Enumerating Interfaces
____ Functional Decomposition

3.20.2 Outcome(s):

Students will be able to:

____ Perform basic procedures such as probing, measuring, and data collection to identify functionality and to affect modifications.

3.21 Hardware/Firmware Security
The intent of this Knowledge Unit is to provide students with an understanding of the diverse components in hardware/firmware, their roles, and the associated security concerns.

3.21.1 Topic(s):
_____ Microcode
_____ Firmware
_____ Hardware Abstraction Layers
_____ Virtualization Layers

3.21.2 Outcome(s):
Students will be able to:
_____ Describe how systems are initialized, how software is loaded, and how software and hardware interact.
_____ Describe the role of intermediate software such as hardware abstraction layers or other forms of middleware.

3.22 IA Architectures
The intent of this Knowledge Unit is to provide students with an understanding of common security architectures for the protection of information systems and data.

3.22.1 Topic(s):
_____ Defense in Depth
_____ DMZs
_____ Proxy Servers
_____ Composition and Security
_____ Cascading
_____ Emergent Properties
_____ Dependencies
_____ TCB Subsets
_____ Enterprise Architectures / Security Architectures
_____ Secure network design

3.22.2 Outcome(s):
Students will be able to:
_____ Examine a specific architecture and identify potential vulnerabilities.
_____ Design a secure architecture for a given application.

3.23 IA Compliance
The intent of this Knowledge Unit is to provide students with an understanding of the rules, regulations and issues related to compliance with applicable laws and regulations.

3.23.1 Topic(s):
_____ HIPAA
_____ Sarbanes Oxley
_____ FERPA
_____ Data Breach Disclosure Laws
_____ FISMA
_____ Gramm Leach Bliley
_____ PCI DSS

3.23.2 Outcome(s):
Students will be able to:
_____ List the applicable laws for compliance in a given situation.
_____ Describe what the laws mandate and where they apply.
_____ Conduct audits to determine compliance with laws.

3.24 IA Standards

The intent of this Knowledge Unit is to provide students with an understanding of the common standards related to information assurance.

3.24.1 Topic(s):
- ____ HIPAA
- ____ FERPA
- ____ Sarbanes-Oxley
- ____ Understanding appropriate commercial standards
- ____ Knowing which standards apply to specific situations
- ____ Rainbow Series

3.24.2 Outcome(s):

Students will be able to:
- ____ Describe the impact of legal/regulatory standards on a given system.
- ____ Describe how standards, such as the Orange Book, may be applied to the requirements for a sub-contractor or customer.

3.25 Independent Study / Directed Study / Special Topics / Advanced Topics

The intent of this Knowledge Unit is to provide credit for courses that address emerging issues related to information assurance and cyber defense.

3.25.1 Topic(s):
- ____ Courses focused on emerging technologies and their security relevant issues or new Tools, Techniques and Methods related to IA/Cyber Defense
- ____ This "wild-card" Knowledge Unit allows any school to submit an IA/Cyber Defense course for credit towards satisfying the academic requirements to be designated as a CAE. It will beup to the on-site review process to validate if the course is worthy of credit.)

3.26 Industrial Control Systems

The intent of this Knowledge Unit is to provide students with an understanding of the basics of industrial control systems, where they are likely to be found, and vulnerabilities they are likely to have.

3.26.1 Topic(s):
- ____ SCADA Firewalls
  - ____ Hardware Components
  - ____ Programmable Logic Controllers (PLCs)
  - ____ Protocols (MODBUS, PROFINET, DNP3, OPC, ICCP, SERIAL)
  - ____ Networking (RS232/485, ZIGBEE, 900MHz, BlueTooth, X.25)
  - ____ Types of ICSs (e.g., power distribution systems, manufacturing)
  - ____ Models of ICS systems (time driven vs. event driven)
  - ____ Common Vulnerabilities in Critical Infrastructure Systems
  - ____ Ladder Logic

3.26.2 Outcome(s):

Students will be able to:
- ____ Describe the use and application of PLCs in automation.
- ____ Describe the components and applications of industrial control systems.
- ____ Explain various control schemes and their differences.
- ____ Demonstrate the ability to understand, evaluate and implement security functionality across an industrial network

3.27 Intro to Theory of Computation

The intent of this Knowledge Unit is to provide students with the basic knowledge of finite automata and their application to computation.

3.27.1 Topic(s):
_____ Computability
_____ Complexity
_____ Turing machines
_____ Deterministic and non-deterministic finite automata

3.27.2 Outcome(s):
Students will be able to:
_____ Describe the concepts of complexity and computability.

3.28 Intrusion Detection / Prevention Systems

The intent of this Knowledge Unit is to provide students with knowledge and skills related to detecting and analyzing vulnerabilities and threats and taking steps to mitigate associated risks.

3.28.1 Topic(s):
_____ Deep Packet Inspection
_____ Log File Analysis
_____ Log Aggregation
_____ Cross Log Comparison and Analysis
_____ Anomaly Detection
_____ Misuse Detection (Signature Detection)
_____ Specification-based Detection
_____ Host-based Intrusion Detection and Prevention
_____ Network-based Intrusion Detection and Prevention
_____ Distributed Intrusion Detection
_____ Hierarchical IDSes
_____ Honeynets/Honeypots

3.28.2 Outcome(s):
Students will be able to:
_____ Demonstrate the ability to detect, identify, resolve and document host or network intrusions.
_____ Demonstrate the ability to detect various types of malware (keyloggers, rootkits) and unauthorized devices (rogue wireless access points) on a live network.
_____ Demonstrate the ability to configure IDS/IPS systems to reduce false positives and false negatives.

3.29 Life-Cycle Security

The intent of this Knowledge Unit is to provide students with an understanding of how security principles can be applied to improve security throughout the system or product lifecycle.

3.29.1 Topic(s):
_____ System Life-Cycle Phases and Issues
_____ Development Processes
_____ Configuration Management
_____ Developmental Threats
_____ Software Assurance Maturity Model
_____ Building Security In Maturity Model

3.29.2 Outcome(s):
Students will be able to
_____ Analyze a security failure and identify how decisions in other phases of the system life-cycle influenced the eventual failure.
_____ List and describe the phases of the system life-cycle.
_____ List and describe the elements of a maturity model.

* = Can include a summary justification for that section.

3.30 Low Level Programming

The intent of this Knowledge Unit is to provide students will the skill and ability to program with low level languages to perform low level operations.

3.30.1 Topic(s):

____ C
____ Assembly
____ Appropriate and secure use of library functions
____ Detailed language syntax
____ Pointers and pointer manipulation
____ Recursive programming
____ Modularization
____ Defensive programming

3.30.2 Outcome(s):

Students will be able to:

____ Utilize low level programming languages to implement complex programs such as internal operating system components and drivers to interface with and control hardware devices.

3.31 Mobile Technologies

The intent of this Knowledge Unit is to provide students with an understanding of the hardware, communications, management and programming environments associated with mobile technologies.

3.31.1 Topic(s):

____ *2G -> 3G -> 4G / LTE -> 5G
    ____ Standards Heritage
    ____ Core Architecture Evolution
____ Design Choices
____ Encryption
____ Mobile Use of SS7
____ RRC Signaling
____ Billing/Charging
____ Wireless Security (WEP vs WPA2)

3.31.2 Outcome(s):

Students will be able to:

____ Describe how a mobile device maintains connectivity to the network while in motion, to include how infrastructure nodes handle passing the mobile device from one node to the next.
____ Explain the weaknesses of WEP and which ones have been addressed and how.

* = Can include a summary justification for that section.

3.32 Network Security Administration

The intent of this Knowledge Unit is to provide students with knowledge of the methods of analyzing and mitigating threats within a network environment.

3.32.1 Topic(s):
- ____ Network Components
- ____ Network Protocols
- ____ Network Security Devices
- ____ Network Security Services
- ____ Protection of Communicated Data
- ____ Network Configuration
- ____ Security Automation
- ____ Network Security Policies
- ____ Packet Capture and Analysis

3.32.2 Outcome(s):
Students will be able to:
- ____ Appropriately position network security components within a network architecture to implement a layered defense.
- ____ Securely configure network devices and services and establish secure communications between networks.

3.33 Operating Systems Hardening

The intent of this Knowledge Unit is to provide students with the ability to apply methods such as managing applications, services, and network ports to improve the robustness of operating systems.

3.33.1 Topic(s):
- ____ Secure Installation
- ____ Removing unnecessary components
- ____ File system maintenance (isolation of sensitive data)
- ____ User restrictions (access and authorizations)
- ____ User / Group / File Management
- ____ Password Standards and Requirements
- ____ Shutting Down Unnecessary/Unneeded Services
- ____ Closing Unnecessary/Unneeded Ports
- ____ Patch Management / Software Updates
- ____ Virtualization
- ____ Vulnerability Scanning

3.33.2 Outcome(s):
Students will be able to:
- ____ Describe, for a given OS, the steps necessary for hardening the OS with respect to various applications.
- ____ Securely install a given OS, remove or shut down unnecessary components and services, close unnecessary ports, and ensure that all patches and updates are applied.

3.34 Operating Systems Theory

The intent of this Knowledge Unit is to provide students with an understanding of the issues related to the design and implementation of operating system concepts, components and interfaces.

3.34.1 Topic(s):
- ____ Privilege States
- ____ Processes & Threads, Process/Thread Management
- ____ Memory Management, Virtual Memory
- ____ Inter-process Communications
- ____ Concurrency and Synchronization, Deadlocks
- ____ File Systems
- ____ Input / Output
- ____ Real-time operating systems / security issues
- ____ Distributed OS architectures & security issues
- ____ Race Conditions
- ____ Buffer Overflows
- ____ Virtualization
- ____ Clear Interface Semantics

3.34.2 Outcome(s):
- ____ Students will have an understanding of operating systems theory and implementation. They will understand OS internals to the level that they can design and implement significant architectural changes to an existing OS.

3.35 Overview of Cyber Operations

The intent of this Knowledge Unit is to provide students with an understanding of the authorities, roles and steps associated with cyber operations.

3.35.1 Topic(s):
- ____ Legal Authorities and Ethics
- ____ *Stages of a Cyber Operation (and details of each phase)
  - ____ Target Identification
  - ____ Reconnaissance
  - ____ Gaining Access
  - ____ Hiding Presence
  - ____ Establishing Persistence
  - ____ Execution
  - ____ Assessment
- ____ Basic Process Modeling
- ____ Validating Procedures
- ____ Handling failures to follow procedures
- ____ Case studies of actual cyber operations

3.35.2 Outcome(s):

Students will be able to:
- ____ Describe the laws that provide US entities the authority to perform cyber operations.
- ____ List the phases of a well organized cyber operation and describe the goals and objectives of each phase.
- ____ Identify specific phases of a cyber operation in network traffic.
- ____ Describe potential motivations that might prompt an entity to perform a cyber operation.

3.36 Penetration Testing

The intent of this Knowledge Unit is to provide students with methods of discovering ways of exploiting vulnerabilities to gain access to a system.

3.36.1 Topic(s):
____ Flaw Hypothesis Methodology
____ Other methodologies (e.g., OSSTMM)
____ Identifying flaws from documentation
____ Identifying flaws from source code analysis
____ Vulnerability Scanning
____ Understanding families of attacks
____ Understanding flaws that lead to vulnerabilities
____ Enumeration, foot printing
____ Attack Surface Discovery
____ Attack Vectors

3.36.2 Outcome(s):
Students will be able to:
____ Plan, organize and perform penetration testing on a simple network.

3.37 QA / Functional Testing

The intent of this Knowledge Unit is to provide students with methods to assess how well a functional unit meets a requirement.

3.37.1 Topic(s):
____ Testing methodologies (white, grey, black box testing)
____ Test coverage analysis
____ Automatic and manual generation of test inputs
____ Test execution
____ Validation of results

3.37.2 Outcome(s):
Students will be able to:
____ Develop effective tests in a structured, organized manner.
____ Perform security functional testing to demonstrate that security policies and mechanisms are completely and correctly implemented.

3.38 RF Principles

The intent of this Knowledge Unit is to provide students with a basic understanding of radio frequency communications.

3.38.1 Topic(s):
____ *Basics of:
    ____ Electromagnetic radiation, Antennas, Information Modulation, Digital Modulation, Spectral representation, Bandwidth, BER, Eb/No vs. S/N
____ Limiting Access in RF
____ Propagation Principles

3.38.2 Outcome(s):
Students will be able to:
____ Identify methods for isolating RF emissions
____ Identify techniques for obfuscating RF transmissions
____ Discuss the tradeoffs associated with bandwidth data rate, modulation, complexity, acceptable BER, and signal spreading

3.39 Secure Programming Practices

The intent of this Knowledge Unit is to provide students with an understanding of the characteristics of secure programs and the ability to implement programs that are free from vulnerabilities.

3.39.1 Topic(s):

_____ Specification of Security Requirements
_____ Principles of Secure Programming
_____ Robust Programming
_____ *Defensive Programming
    _____ Input Validation, Type checking
_____ *Programming Flaws
    _____ Buffer Overflows, Integer Errors
_____ Static Analysis
_____ Data Obfuscation
_____ Data Protection

3.39.2 Outcome(s):

Students will be able to:

_____ Produce software components that satisfy their functional requirements without introducing vulnerabilities
_____ Describe the characteristics of secure programming.

3.40 Security Program Management

The intent of this Knowledge Unit is to provide students with the knowledge necessary to define and implement a security program for the protection of an organizations systems and data.

3.40.1 Topic(s):

_____ *Project management
    _____ Resource management
    _____ Project budgeting (cost benefit, net present value, internal rate of return)
_____ Risk management and Analysis
_____ Quality Assurance / Quality Control
_____ Monitoring and Control
_____ Deliverables
_____ Timelines
_____ Security Awareness, Training and Education
_____ Security Baselines
_____ Change Management, Patch Management
_____ Roles and Responsibilities of the Security Organization
_____ Compliance with Applicable Laws and Regulations

3.40.2 Outcome(s):

Students will be able to:

_____ Apply their knowledge to develop a security program, identifying goals, objectives and metrics.
_____ Apply their knowledge to effectively manage a security program.
_____ Assess the effectiveness of a security program.

* = Can include a summary justification for that section.

3.41 Security Risk Analysis

The intent of this Knowledge Unit is to provide students with sufficient understanding of risk assessment models, methodologies and processes such that they can perform a risk assessment of a particular systems and recommend mitigations to identified risks.

3.41.1 Topic(s):
____   Risk Assessment/Analysis Methodologies
____   Risk Measurement and Evaluation Methodologies
____   Risk Management Models
____   Risk Management Processes
____   Risk Mitigation Economics
____   Risk Transference/Acceptance/Mitigation
____   Communication of Risk

3.41.2 Outcome(s):
Students will be able to:
____   Describe how risk relates to a system security policy.
____   Describe various risk analysis methodologies.
____   Evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
____   Compare the advantages and disadvantages of various risk assessment methodologies
____   Select the optimal methodology based on needs, advantages and disadvantages.

3.42 Software Security Analysis

The intent of this Knowledge Unit is to provide students with an understanding of the tools and methods for analyzing software, either in source code or binary form.

3.42.1 Topic(s):
____   Testing Methodologies
____   Source and Binary Code Analysis
____   Static and Dynamic Analysis Techniques
____   Sandboxing
____   Common analysis tools and methods

3.42.2 Outcome(s):
Students will be able to:
____   Describe software security analysis tools and techniques.
____   Apply their knowledge to perform software security analysis, using common tools, against previously unknown software components.

3.43 Software Assurance

The intent of this Knowledge Unit is to provide students with the ability to describe why software assurance is important to the development of secure systems and describe the methods and techniques that lead to secure software.

3.43.1 Topic(s):
_____ Robust programming
_____ Secure Software Concepts, Requirements, Design, Implementation and Testing
_____ Secure Development Life-Cycle Phases: requirements, design, development, testing, deployment, operations, maintenance and disposal.
_____ Software testing and acceptance
_____ Threat modeling
_____ Fuzz testing
_____ BUG BAR
_____ Characteristics of secure software
_____ Secure Software is not software that implements security functions (e.g., crypto, access control)

3.43.2 Outcome(s):
_____ Describe the importance of secure software, and the programming practices and development processes and methodologies that lead to secure software.

3.44 Software Reverse Engineering

The intent of this Knowledge Unit is to provide students with the capability to perform reverse engineering of executable code to determine its function and affects, or to recover the source code implementation.

3.44.1 Topic(s):
_____ Specification Recovery
_____ Malware Analysis
_____ Reverse Engineering Tools & Techniques
_____ Sandboxing

3.44.2 Outcome(s):
Students will be able to:
_____ Use a common SW RE tool to safely perform static and dynamic analysis of software (or malware) of unknown origin for the purposes of recovering the original implementation and/or understanding the software functionality.

3.45 Supply Chain Security

The intent of this Knowledge Unit is to provide students with an understanding of the security issues associated with building complex systems out of third party components of unknown (and potentially unknowable) origin.

3.45.1 Topic(s):
_____ Global Development
_____ Off Shore Production
_____ Transport and Logistics of IT Components
_____ Evaluation of 3rd Party Development Practices
_____ Understanding of the Capabilities and Limits of Software and Hardware Reverse Engineering

3.45.2 Outcome(s):
Students will be able to:
_____ Describe the issues related to outsourcing hardware and/or software development and/or integration.
_____ Describe methods to mitigate these issues, and the limitations of these methods.

* = Can include a summary justification for that section.

3.46 Systems Certification and Accreditation

The intent of this Knowledge Unit is to provide students with an understanding of the processes and regulations associated with the analysis/evaluation of operational systems and the authorities and processes for the approval of their operation.

3.46.1 Topic(s):
_____ DoD Policies and Directives
_____ Roles / Players
_____ Components of the C&A Process
_____ Certification Boards and Panels
_____ NIST Risk Management Framework (SP800-37)

3.46.2 Outcome(s):
Students will be able to:
_____ Describe the DoD system certification and accreditation processes.
_____ Define certification and accreditation.

3.47 Systems Programming

The intent of this Knowledge Unit is to ensure that students are proficient in the development of complex, low level software (e.g., software interacting directly with the hardware platform or within the deepest level of an operating system), typically in the C or assembly programming language.

3.47.1 Topic(s):
_____ Hardware / software interfaces and interactions
_____ Programming to operating systems internal interfaces
_____ Low level programming languages (C, Assembly)

3.47.2 Outcome(s):
Students will be able to:
_____ Implement new functions in an OS kernel
_____ Develop complex and sophisticated programs, such as a device driver, that can be embedded into an OS kernel.
_____ Write a program that implements a network stack to manage network communications.
_____ Write a functional, stand-alone assembly language program of the complexity of a basic telnet client, with no help from external libraries.

3.48 Systems Security Engineering

The intent of this Knowledge Unit is to provide students with a thorough understanding of the skills necessary to participate in the development of large scale systems. Students will understand that techniques, methods, and issues involved across the entire system life-cycle, from requirements identification and analysis, through various levels of design, implementation, testing and operation/maintenance.

3.48.1 Topic(s):
_____ Design of testing
_____ Testing methodologies
_____ Emergent Properties
_____ Systems Engineering
_____ System Integration
_____ Make or Buy Analysis
_____ Systems Security Analysis
_____ Enterprise system components

3.48.2 Outcome(s):
Students will be able to:
_____ Analyze system components and determine how they will interact in a composed system.
_____ Analyze a system design and determine if the design will meet the system security requirements.

3.49 Virtualization Technologies

The intent of this Knowledge Unit is to provide students with an understanding of how modern host virtualization is implemented, deployed, and used. Students will understand the interfaces between major components of virtualized systems, and the implications these interfaces have for security.

3.49.1 Topic(s):

_____ Virtualization Architectures
_____ Virtualization techniques for code execution
_____ Memory management in virtual environments
_____ Networking in virtual environments
_____ Storage in virtual environments
_____ Scheduling of virtual machines
_____ Migration and snapshots
_____ Virtual management layers
_____ Digital Forensics in virtual environments

3.49.2 Outcome(s):

Students will be able to:

_____ Describe the fundamental concepts of virtualization.
_____ Compare and contrast the different virtualization architectures.

3.50 Vulnerability Analysis

The intent of this Knowledge Unit is to provide students with a thorough understanding of system vulnerabilities, to include what they are, how they can be found/identified, the different types of vulnerabilities, how to determine the root cause of a vulnerability, and how to mitigate their effect on an operational system.

3.50.1 Topic(s):

_____ Definition of "vulnerability"
_____ Failures of Procedures
_____ *Taxonomy
　　　_____ Buffer overflows, privilege escalation, rootkits
　　　_____ trojans/backdoors/viruses
　　　_____ Return oriented programming
_____ Social Engineering Vulnerabilities
_____ Vulnerability characteristics
_____ Root causes of vulnerabilities
_____ Administrative Privileges and Their Effect on Vulnerabilities
_____ Mitigation strategies
_____ Tools and Techniques for Identifying Vulnerabilities

3.50.2 Outcome(s):

Students will be able to:

_____ Describe characteristics of malware.
_____ Identify malware.
_____ Apply tools and techniques for identifying vulnerabilities.

3.51 Wireless Sensor Networks

The intent of this Knowledge Unit is to provide students with a basic understanding of wireless sensor network architectures and the issues associated with them.

3.51.1 Topic(s):

    ____ Managed vs. Ad-hoc
    ____ Cross Layer Optimization
    ____ MAC approaches
    ____ Architectures
    ____ Routing Protocols
    ____ Authentication Hash Tables
    ____ Data Integrity
    ____ Data Poisoning
    ____ Resource Starvation
    ____ Energy Harvesting

3.51.2 Outcome(s):

Students will be able to:

    ____ Describe the challenges associated with wireless sensor networks, including coordination, energy efficiency, self organization and security.

* = Can include a summary justification for that section.