

# **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.

## **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)

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

## **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.

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

## **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.

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

## **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.

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

### **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.

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

## **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.

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

## **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.



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

### **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.

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

### **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 be up 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

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

### **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.

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

### **3.30 Low Level Programming**

The intent of this Knowledge Unit is to provide students with 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.

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

## **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.

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

## **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.

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

### **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

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

### **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.



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

### **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.

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

### **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.

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

### **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.

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

### **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.

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

### **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.