CAE IA/Cyber Defense
Updated Academic Requirements

The intent of the modifications to the academic requirements of the CAE IA programs was to update them to better reflect the state to which the discipline of IA has evolved since the original publication of the training standards. The framework of Knowledge Units (KUs) and Focus Areas (FAs) was chosen to make the requirements easier to update in the future and to allow differentiation amongst the schools by recognizing the specific areas in which they focus their research and/or educational offerings (e.g., Digital Forensics, Systems Security Engineering, Secure Software Development).

~NIETP team

New Academic Requirements

- **Based on Knowledge Units**
    - **Knowledge Units composed of:**
        - **A <u>minimum</u> list of required topics to be covered**
        - **One or more "outcomes" or learning objectives**
    - **Designation based on meeting a defined set of core and a minimum of five (5) optional Knowledge Units for 4 year (plus) institutions and zero (0) for 2 year institutions.**
        - **Defined "Cores"**
            - **2 year programs (with technical or applied emphasis)**
            - **4 year + programs (with technical or applied emphasis)**
- **Additional Cyber Defense Focus Areas**
    - **Composed of a collection of Core and Optional Knowledge Units**

CORE Knowledge Units
(2 year programs)

- Basic Data Analysis
- Basic Scripting or Introductory Programming (4 yr core)
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

CORE Knowledge Units
(4 + year programs + 2 year core)

- Databases
- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts
- Probability and Statistics
- Programming

Knowledge Units

There are many ways to demonstrate that a program meets/fulfills a Knowledge Unit

- Course Syllabus
- Prerequisite Course(s)
- Prerequisite Degree
- Student Assignments
- Modules in a course/collection of courses
- Certifications (CCNA, etc)

A course may fulfill the requirements of multiple Knowledge Units.

Optional Knowledge Units

- Advanced Cryptography
- Advanced Network Technology and Protocols
- Algorithms
- Analog Telecommunications
- Cloud Computing
- Cybersecurity Planning and Management
- Data Administration
- Data Structures
- Database Management Systems
- Digital Communications
- Digital Forensics
    - Device Forensics
    - Host Forensics
    - Media Forensics
    - Network Forensics
- Embedded Systems
- Forensic Accounting
- Formal Methods
- Fraud Prevention and Management
- Hardware Reverse Engineering
- Hardware/Firmware Security
- IA Architectures
- IA Compliance
- IA Standards
- Independent/Directed Study/Research
- Industrial Control Systems
- Intro to Theory of Computation
- Intrusion Detection
- Life-Cycle Security
- Low Level Programming
- Mobile Technologies
- Network Security Administration
- Operating Systems Hardening
- Operating Systems Theory
- Overview of Cyber Operations
- Penetration Testing
- QA / Functional Testing
- RF Principles
- Secure Programming Practices
- Security Program Management
- Security Risk Analysis
- Software Assurance
- Software Reverse Engineering
- Software Security Analysis
- Supply Chain Security
- Systems Programming
- Systems Certification and Accreditation
- Systems Security Engineering
- Virtualization Technologies
- Vulnerability Analysis
- Wireless Sensor Networks

Basic Data Analysis

Definition:

The intent of this Knowledge Unit is to provide students with basic abilities to manipulate data into meaningful information.

Topics:

- Summary Statistics
- Graphing / Charts
- Spreadsheet Functions
- Problem solving

Outcomes:

- Students will be able to apply standard statistical inference procedures to draw conclusions from data.

Basic Scripting

Definition:

The intent of this Knowledge Unit is to provide students with the ability to create simple scripts/programs to automate and perform simple operations. This knowledge should include basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

Topics:

- Basic Security
  - Bounds checking, input validation
- Program Commands
- Program Control Structures
- Variable Declaration
- Debugging
- Scripting Language (e.g. PERL, Python, BASH, VB Scripting, Powershell)
- Basic Boolean logic/operations.
  - AND / OR / XOR / NOT

Outcomes:

- Students will be able to demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).
- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
- Students will be able to write simple linear and looping scripts.

Cyber Defense

Definition:

The intent of this Knowledge Unit is to provide students with a basic awareness of the options available to mitigate threats within a system.

Topics:

- Network mapping (enumeration and identification of network components)
- Network security techniques and components
    - Access controls, flow control, cryptography, firewalls, intrusion detection systems, etc.
- Applications of Cryptography
- Malicious activity detection / forms of attack
- Appropriate Countermeasures
- Trust relationships
- Defense in Depth
    - Layering of security mechanisms to achieve desired security
- Patching
    - OS and Application Updates
- Vulnerability Scanning
- Vulnerability Windows (0-day to patch availability)

Outcomes:

- Students will be able to describe potential system attacks and the actors that might perform them.
- Students will be able to describe cyber defense tools, methods and components.
- Students will be able to apply cyber defense methods to prepare a system to repel attacks.
- Students will be able to describe appropriate measures to be taken should a system compromise occur.

Cyber Threats

Definition:

The intent of this Knowledge Unit is to provide students with basic information about the threats that may be present in the cyber realm.

Topics:

- Adversaries and targets
- Motivations and Techniques
- The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)
- Types of Attacks
    - Password guessing / cracking
    - Backdoors / trojans / viruses / wireless attacks
    - Sniffing / spoofing / session hijacking
    - Denial of service / distributed DOS / BOTs
    - MAC spoofing / web app attacks / 0-day exploits
    - And the vulnerabilities that enable them …
- Attack Timing (within x minutes of being attached to the net)
- Social Engineering
- Events that indicate an attack is/has happened
- Legal Issues
- Attack surfaces / vectors
- Attack trees
- Insider problem
- Covert Channels
- Threat Information Sources (e.g., CERT)

Outcomes:

- Students will be able to identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk.
- Students will be able to describe different types of attacks and their characteristics.

Fundamental Security Design Principles

Definition:

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

Topics:

- Separation (of domains)
- Isolation
- Encapsulation
- Least Privilege
- Simplicity (of design)
- Minimization (of implementation)
- Fail Safe Defaults / Fail Secure
- Modularity
- Layering
- Least Astonishment
- Open Design
- Usability

Outcomes:

- Students will be able to list the first principles of security.
- Students will be able to describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.
- Students will be able to analyze common security failures and identify specific design principles that have been violated.
- Given a specific scenario, students will be able to identify the needed design principle.
- Students will be able to describe why good human machine interfaces are important to system use.
- Students will understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms

Resources:

- The Protection of Information in Computer Systems (Saltzer an Schroeder, 1975)
- Saltzer and Kaashoek (2009)
- Computer Security Technology Planning Study (Anderson Report, introduced the reference monitor concept)
- Bell-LaPadula Model (first multi-level security policy model)
- Biba Integrity Model
- System Security Analysis/Certification (Clark Weissman, introduced the flaw hypothesis methodology)
- Security Controls for Computer Systems (Ware report, first raised computer security as an issue)
- The Trusted Computer System Evaluation Criteria (The “Orange Book”)

IA Fundamentals

Definition:

The intent of this Knowledge Unit is to provide students with basic concepts of information assurance fundamentals.

Topics:

- Threats and Adversaries
- Vulnerabilities and Risks
- Basic Risk Assessment
- Security Life-Cycle
- Intrusion Detection and Prevention Systems
- Cryptography
- Data Security (in transmission, at rest, in processing)
- Security Models
- Access Control Models (MAC, DAC, RBAC)
- Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
- Security Mechanisms (e.g., Identification/Authentication, Audit)

Outcomes:

- Students shall be able to list the fundamental concepts of the Information Assurance / Cyber Defense discipline.
- Students will be able to describe how the fundamental concepts of cyber defense can be used to provide system security.
- Students will 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.

Resources:

- Computer Security: Art and Science, by Matt Bishop

Intro to Cryptography

Definition:

The intent of this Knowledge Unit is to provide students with a basic ability to understand where and how cryptography is used.

Topics:

- Symmetric Cryptography (DES, Twofish)
- Public Key Cryptography
  - Public Key Infrastructure
  - Certificates
- Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)
  - For integrity
  - For protecting authentication data
  - Collision resistance
- Digital Signatures (Authentication)
- Key Management (creation, exchange/distribution)
- Cryptographic Modes (and their strengths and weaknesses)
- Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)
- Common Cryptographic Protocols
- DES -> AES (evolution from DES to AES)
- Security Functions (data protection, data integrity, authentication)

Outcomes:

- Students will be able to identify the elements of a cryptographic system.
- Students will be able to describe the differences between symmetric and asymmetric algorithms.
- Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
- Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc.

Resources:

- Cryptography: A Very Short Introduction, Piper and Murphy

IT System Components

Definition:

The intent of this Knowledge Unit is to provide students with an understanding of the basic components in an information technology system and their roles in system operation.

Topics:

- Workstations
- Servers
- Network Storage Devices
- Routers / Switches / Gateways
- Guards / CDSes / VPNs / Firewalls
- IDSes, IPSes
- Mobile Devices
- Peripheral Devices / Security Peripherals

Outcomes:

- Students will be able to describe the hardware components of modern computing environments and their individual functions.

Networking Concepts

Definition:

The intent of this Knowledge Unit is to provide students with basic understanding of network components and how they interact.

Topics:

- Overview of Networking (OSI Model)
- Network Media
- Network architectures (LANs, WANs)
- Network Devices (Routers, Switches, VPNs, Firewalls)
- Network Services
- Network Protocols (TCP/IP, HTTP, DNS, SMTP, UDP)
- Network Topologies
- Overview of Network Security Issues

Outcomes:

- Students will be able to describe the fundamental concepts, technologies, components and issues related to communications and data networks.
- Students will be able to describe a basic network architecture given a specific need and set of hosts/clients.
- Students will be able to track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
- Students will be able to use a network monitoring tools (e.g., WireShark).
- Students will be able to use a network mapping tool (e.g., Nmap).

Policy, Legal, Ethics and Compliance

Definition:

The intent of this Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

Topics:

- HIPAA / FERPA
- Computer Security Act
- Sarbanes – Oxley
- Gramm – Leach – Bliley
- Privacy (COPPA)
- Payment Card Industry Data Security Standard (PCI DSS)
- State, US and international standards / jurisdictions
- Laws and Authorities
- US Patriot Act
- BYOD issues
- Americans with Disabilities Act, Section 508

Outcomes:

- Students shall be able to list the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data.
- Students shall be able to describe their responsibilities related to the handling of information about vulnerabilities.
- Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.

Systems Administration

Definition:

The intent of this Knowledge Unit is to provide students with skill to perform basic operations involved in system administration.

Topics:

- OS Installation
- User accounts management
- Password policies
- Authentications Methods
- Command Line Interfaces
- Configuration Management
- Updates and patches
- Access Controls
- Logging and Auditing (for performance and security)
- Managing System Services
- Virtualization
- Backup and Restoring Data
- File System Security
- Network Configuration (port security)
- Host (Workstation/Server) Intrusion Detection
- Security Policy Development

Outcomes:

- Students will be able to apply the knowledge gained to successfully install and securely configure, operate and maintain a commodity OS, to include: setting up user accounts, configuring appropriate authentication policies, configuring audit capabilities, performing back-ups, installing patches and updates, reviewing security logs, and restoring the system from a backup.

Databases

Definition:

The intent of this Knowledge Unit is to teach students how database systems are used, managed, and issues associated with protecting the associated data assets.

Topics:

- Relational Databases
- No SQL Databases
- Object Based vs. Object Oriented
- Overview of Database Vulnerabilities
- Overview of Database topics/issues (indexing, inference, aggregation, polyinstantiation)
- Hashing and Encryption
- Database access controls (DAC, MAC, RBAC, Clark-Wilson)
- Information flow between databases/servers and applications
- Database security models
- Security issues of inference and aggregation
- Common DBMS vulnerabilities

Outcomes:

- Students will be able to describe common security models of database management systems.
- Students will be able to identify and describe common security concerns in database management systems.
- Students will be able to apply security principles to the design and development of database systems and database structures.

Network Defense

Definition:

The intent of this Knowledge Unit is to teach students the techniques that can be taken to protect a network and communication assets from cyber threats.

Topics:

- Implementing IDS/IPS
- Implementing Firewalls and VPNs
- Defense in Depth
- Honeypots and Honeynets
- Network Monitoring
- Network Traffic Analysis
- Minimizing Exposure (Attack Surface and Vectors)
- Network Access Control (internal and external)
- DMZs / Proxy Servers
- Network Hardening
- Mission Assurance
- Network Policy Development and Enforcement
- Network Operational Procedures
- Network Attacks (e.g., session hijacking, Man-in-the-Middle)

Outcomes:

- Students will be able to describe the various concepts in network defense.
- Students will be able to apply their knowledge to implement network defense measures.
- Students will be able to use a network monitoring tools (e.g., WireShark).
- Students will be able to use a network mapping tool (e.g., Nmap).

Network Technology and Protocols

Definition:

The intent of this Knowledge Unit is to provide students with an understanding of the components in a network environment, their roles, and communication methods.

Topics:

- Network Architectures
- Networks Infrastructure
- Network Services
- Network Protocols (TCP/IP – v4 and v6, DNS, HTTP, SSL, TLS)
- Network Address Translation and Sub-netting
- Network Analysis/Troubleshooting
- Network Evolution (Change Management, BYOD)
- Remote and Distributed Management

Outcomes:

- Students will be able to apply their knowledge of network technologies to design and construct a working network.
- Students will be able to analyze a trace of packets to identify the establishment of a TCP connection.
- Students will be able to demonstrate the use of a network monitor to display packets.

Operating Systems Concepts

Definition:

The intent of this Knowledge Unit is to provide students with an understanding of the roles of an operating system, its basic functions, and the services provided by the operating system.

Topics:

- Privileged and non-privileged states
- Processes and Threads (and their management)
- Memory (real, virtual, and management)
- Files Systems
- Access Controls (Models and Mechanisms)
    - Access control lists
- Virtualization / Hypervisors
- How does the an OS protect itself from attack?
- Fundamental Security Design Principles as applied to an OS
    - Domain separation, process isolation, resource encapsulation, least privilege

Outcomes:

- Students will be able to identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems).

Probability and Statistics

Definition:

The intent of this Knowledge Unit is to provide students with the ability to use basic statistics to analyze and attach meaning to datasets.

Topics:

- Probability as a concept
- Random variables/events
- Odds of an event happening
- Data Interpretation
- Statistical Problem Solving
- Probability Distributions

Outcomes:

- Students will be able to evaluate probabilities to solve applied problems.
- Students will be able to describe how basic statistics and statistical methods can be applied in a given situation.

Programming

Definition:

The intent of this Knowledge Unit is to provide students with the skills necessary to implement algorithms using programming languages to solve problems.

Topics:

- Programming Languange, such as: C
- Programming constructs and concepts variables, strings, assignments, sequential execution, loops, functions.
- Security issues, such as type checking and parameter validation.
- Basic Boolean logic/operations.
    - AND / OR / XOR / NOT

Outcomes:

- Students will be able to demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner.
- Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
- Students will be able to demonstrate the ability to design and develop basic programs for modern computing platforms (e.g., PC, cloud, mobile, web).

Optional Knowledge Units

Advanced Cryptography

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to describe how various cryptographic algorithms and protocols work.
- Students will be able to evaluate security mechanisms based on cryptography.
- Students will be able to describe the application of cryptography in SSL, virtual private networks, secure storage, and other security applications.
- Students will be able to take a mode or protocol diagram and identify how an error propagates through the cryptosystem.

Advanced Network Technology & Protocols

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to describe current networking technologies and trends.
- Students will be able to describe and discuss data network architectures and protocols, to include their advantages and disadvantages, applications, and security issues.

Algorithms

Definition:

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.

Topics:

- Algorithm Analysis
- Computational Complexity
- Best/Worst/Average Case Behavior
- Optimization
- Searching / Sorting

Outcomes:

- Students will be able to describe how to perform an analysis of algorithms to determine best and worst case behavior.

Analog Telecommunications Systems

Definition:

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

Topics:

- Signaling Methods
- Architecture
- Trunks, Switching
- Grade of Service
- Blocking
- Call Arrival Models
- Interference Issues

Outcomes:

- Students will be able to describe the basic concepts of modern analog communications systems, using block diagrams.
- Students will be able to 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.

Cloud Computing

Definition:

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.

Topics:

- Virtualization platforms
- Cloud Services
    - SaaS, PaaS, DaaS, IaaS
- Service Oriented Architectures
- Deployment Models
    - private, public, community, hybrid
- Security
- Storage
- Legal/Privacy Issues

Outcomes:

- Students will be able to describe each type of service/model of cloud computing
- Students will be able to compare and contrast: local resource requirements, local control, network requirements, and security (attacks, mitigations, overall vulnerability)

Cybersecurity Planning and Management

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to examine the placement of security functions in a system and describe the strengths and weaknesses
- Students will be able to develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response.
- Students will be able to develop system specific plans for:
    - The protection of intellectual property
    - The implementation of access controls, and
    - Patch and change management.

Data Administration

Definition:

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.

Topics:

- Big Data
- Hadoop / Mongo DB / HBASE
- Data Policies
- Data Quality
- Data Ownership
- Data Warehousing
- Long Term Archival
- Data Validation
- Data Security (access control, encryption)

Outcomes:

- Students will be able to identify relevant security issues given a system and data management structure

Data Structures

Definition:

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.

Topics:

- Strings, Lists, Vectors, Arrays
- Heaps, Queues, Stacks, Buffers
- Searching and Sorting
- Trees
- Data Formats

Outcomes:

- Students will be able to list the most common structures and data formats for storing data in a computer system.
- Students will be able to discuss the advantages and disadvantages of different data structures/formats.

Database Management Systems

Definition:

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

Topics:

- 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)

Outcomes:

- Students will be able to list the most common structures for storing data in a database management system.
- Students will be able to configure a commodity DBMS for secure access.
- Students will be able to describe alternatives to relational DBMSs and their unique security issues.
- Students will be able to describe the role of a database, a DBMS, and a database server within a complex system supporting multiple applications.
- Students will be able to demonstrate basic SQL proficiency for table creation, data insertion and data query.
- Students will be able to describe DBMS access controls and privilege levels and apply them to a simple database.
- Students will be able to develop a DB structure for a specific system/problem.

Digital Communications

Definition:

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

Topics:

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

Outcomes:

- Students will be able to describe digital communications systems in terms of subsystems and modulation techniques.
- Students will be able to describe the current state of the art in digital communications.
- Students will be able to compare and contrast different approaches to digital communications and describe the advantages and disadvantages of each.

Digital Forensics

Definition:

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.

Topics:

- 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

Outcomes:

- Students shall be able to discuss the rules, laws, policies, and procedures that affect digital forensics
- Students shall be able to use one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.
- Students will be able to 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.

Resources:

- Guide to Computer Forensics & Investigations, Nelson et. al.
- Department of Defense Cyber Crime Center (DC3)

Host Forensics

Definition:

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.

Topics:

- 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)

Outcomes:

- Students will be able to describe what can/cannot be retrieved from various OSes.
- Students will be able to describe the methodologies used in host forensics.

Device Forensics

Definition:

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

Topics:

- Mobile Device Analysis
- Tablets
- SmartPhones
- GPS
- (must include hands-on activities)

Outcomes:

- Students will be able to describe methods for the acquisition/analysis of mobile devices (e.g., device storage, system data, cell tower logs).
- Students will be able to explain the legal issues related to mobile device forensic activities.

Media Forensics

Definition:

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.

Topics:

- 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)

Outcomes:

- Students will be able to describe methods and approaches for forensic analysis on specified media.

Network Forensics

Definition:

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

Topics:

- 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)

Outcomes:

- Students will be able to describe the methodologies used in network forensics.
- Students will be able to analyze and decipher network traffic, identify anomalous or malicious activity, and provide a summary of the effects on the system.

Embedded Systems

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to discuss embedded system architectures, real time OS issues such as concurrency and synchronization, and real time resource management.

Forensic Accounting

Definition:

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

Topics:

- 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

Outcomes:

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

Formal Methods

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to apply formal security policy models to real world scenarios.

Fraud Prevention and Management

Definition:

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.

Topics:

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

Outcomes:

- Students will be able to describe the components of the fraud triangle – necessary condition for fraud.
- Students will be able to describe the cost and effectiveness of common fraud detection and prevention methods.
- Students will be able to analyze record keeping and management procedures for assets and to identify/correct weaknesses.
- Students will be able to describe legal and ethical requirements for detecting, preventing and reporting fraud.
- Students will be able to describe investigative procedures for fraud.
- Students will be able to describe common methods of financial statement fraud.

Hardware Reverse Engineering

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to perform basic procedures such as probing, measuring, and data collection to identify functionality and to affect modifications.

Hardware/Firmware Security

Definition:

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.

Topics:

- Microcode
- Firmware
- Hardware Abstraction Layers
- Virtualization Layers

Outcomes:

- Students will be able to describe how systems are initialized, how software is loaded, and how software and hardware interact.
- Students will be able to describe the role of intermediate software such as hardware abstraction layers or other forms of middleware.

IA Architectures

Definition:

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.

Topics:

- Defense in Depth
- DMZs
- Proxy Servers
- Composition and Security
- Cascading
- Emergent Properties
- Dependencies
- TCB Subsets
- Enterprise Architectures / Security Architectures
- Secure network design

Outcomes:

- Students will be able to examine a specific architecture and identify potential vulnerabilities.
- Students will be able to design a secure architecture for a given application.

IA Compliance

Definition:

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.

Topics:

- HIPAA
- Sarbanes Oxley
- FERPA
- Data Breach Disclosure Laws
- FISMA
- Gramm Leach Bliley
- PCI DSS

Outcomes:

- Students shall be able to list the applicable laws for compliance in a given situation.
- Students shall be able to describe what the laws mandate and where they apply.
- Students will be able to conduct audits to determine compliance with laws.

IA Standards

Definition:

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

Topics:

- HIPAA
- FERPA
- Sarbanes-Oxley
- Understanding appropriate commercial standards
- Knowing which standards apply to specific situations
- Rainbow Series

Outcomes:

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

Independent Study / Directed Study / Special Topics / Advanced Topics

Definition:

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

Topics:

- 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.)

Industrial Control Systems

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to describe the use and application of PLCs in automation.
- Students will be able to describe the components and applications of industrial control systems.
- Students will be able to explain various control schemes and their differences.
- Students shall be able to demonstrate the ability to understand, evaluate and implement security functionality across an industrial network

Resources:

- NIST SP800-53 and NIST SP800-82
- NERC CIP
- NRC REG 5.71 Cyber Security Programs for Nuclear Facilities

Intro to Theory of Computation

Definition:

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

Topics:

- Computability
- Complexity
- Turing machines
- Deterministic and non-deterministic finite automata

Outcomes:

- Students will be able to describe the concepts of complexity and computability.

Intrusion Detection / Prevention Systems

Definition:

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.

Topics:

- 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

Outcomes:

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

Resources:

- tools such as TCPDUMP, SNORT, WireShark

Life-Cycle Security

Definition:

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.

Topics:

- System Life-Cycle Phases and Issues
- Development Processes
- Configuration Management
- Developmental Threats
- Software Assurance Maturity Model
- Building Security In Maturity Model

Outcomes:

- 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.
- Students will be able to list and describe the phases of the system life-cycle.
- Students will be able to list and describe the elements of a maturity model.

Resources:

- NIST Risk Management Framework and NIST SP 800-37

Low Level Programming

Definition:

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.

Topics:

- C
- Assembly
- appropriate and secure use of library functions
- detailed language syntax
- pointers and pointer manipulation
- recursive programming
- modularization
- defensive programming

Outcomes:

- 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.

Mobile Technologies

Definition:

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.

Topics:

- 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)

Outcomes:

- 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.
- Students will be able to explain the weaknesses of WEP and which ones have been addressed and how.

Network Security Administration

Definition:

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

Topics:

- 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

Outcomes:

- Students will be able to appropriate position network security components within a network architecture to implement a layered defense.
- Students will be able to securely configure network devices and services and establish secure communications between networks.

Operating Systems Hardening

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to describe, for a given OS, the steps necessary for hardening the OS with respect to various applications.
- Students will be able to 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.

Resources:

- NSA Guides for Configuring Windows, Windows Server, Solaris, Linux, Apple iOS and MAC OS X.

Operating Systems Theory

Definition:

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.

Topics:

- 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

Outcomes:

- 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.

Overview of Cyber Operations

Definition:

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

Topics:

- 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

Outcomes:

- The student will be able to describe the laws that provide US entities the authority to perform cyber operations.
- The student will be able to list the phases of a well organized cyber operation and describe the goals and objectives of each phase.
- The student will be able to identify specific phases of a cyber operation in network traffic.
- The student will be able to describe potential motivations that might prompt an entity to perform a cyber operation.

Penetration Testing

Definition:

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

Topics:

- 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

Outcomes:

- Students will be able to plan, organize and perform penetration testing on a simple network.

Resources:

- Web Hacker’s Handbook
- Backtrack 5
- Open Source Security Testing Methodology Manual (OSSTMM)

QA / Functional Testing

Definition:

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

Topics:

- Testing methodologies (white, grey, black box testing)
- Test coverage analysis
- Automatic and manual generation of test inputs
- Test execution
- Validation of results

Outcomes:

- Students will be able to develop effective tests in a structured, organized manner.
- Students will be able to perform security functional testing to demonstrate that security policies and mechanisms are completely and correctly implemented.

RF Principles

Definition:

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

Topics:

- Basics of:
  - Electromagnetic radiation, Antennas, Information Modulation, Digital Modulation, Spectral representation, Bandwidth, BER, Eb/No vs. S/N
- Limiting Access in RF
- Propogation Principles

Outcomes:

- Students should be able to identify methods for isolating RF emissions
- Students should be able to identify techniques for obfuscating RF transmissions
- Students should be able to discuss the tradeoffs associated with bandwidth data rate, modulation, complexity, acceptable BER, and signal spreading

Secure Programming Practices

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to produce software components that satisfy their functional requirements without introducing vulnerabilities
- Students will be able to describe the characteristics of secure programming.

Resources:

- Security Injections (web resource at Towson University)
- Microsoft SDL
- 19 Deadly Sins, by Michael Howard
- 23 Deadly Sins, by Viega
- Web Hacker’s Handbook

Security Program Management

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to apply their knowledge to develop a security program, identifying goals, objectives and metrics.
- Students will be able to apply their knowledge to effectively manage a security program.
- Students will be able to assess the effectiveness of a security program.

Resources:

- Project Management Body of Knowledge (PMBOK) (PMI.org)
- ISO 27000 Series Standards

Security Risk Analysis

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to describe how risk relates to a system security policy.
- Students will be able to describe various risk analysis methodologies.
- Students will be able to evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
- Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
- Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

Resources:

- PMBOK – Project Management Body of Knowledge
- NIST 800-30

Software Security Analysis

Definition:

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.

Topics:

- Testing Methodologies
- Source and Binary Code Analysis
- Static and Dynamic Analysis Techniques
- Sandboxing
- Common analysis tools and methods

Outcomes:

- Students will be able to describe software security analysis tools and techniques.
- Students will be able to apply their knowledge to perform software security analysis, using common tools, against previously unknown software components.

Software Assurance

Definition:

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.

Topics:

- 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)

Outcome:

- Students will be able to describe the importance of secure software, and the programming practices and development processes and methodologies that lead to secure software.

Resources:

- Geekonomics: The Real Cost of Insecure Software, David Rice

Software Reverse Engineering

Definition:

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.

Topics:

- Specification Recovery
- Malware Analysis
- Reverse Engineering Tools & Techniques
- Sandboxing

Outcomes:

- 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.

Resources:

- IDA Pro
- The IDA Pro Book, Chris Eagle

Supply Chain Security

Definition:

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.

Topics:

- 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

Outcomes:

- Drew Hamilton, Auburn University

Systems Certification and Accreditation

Definition:

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.

Topics:

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

Outcomes:

- Students will be able to describe the DoD system certification and accreditation processes.
- Students will be able to define certification and accreditation.

Systems Programming

Definition:

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.

Topics:

- Hardware / software interfaces and interactions
- Programming to operating systems internal interfaces
- Low level programming languages (C, Assembly)

Outcomes:

- Students shall be able to implement new functions in an OS kernel
- Students will be able to develop complex and sophisticated programs, such as a device driver, that can be embedded into an OS kernel.
- Students will be able to write a program that implements a network stack to manage network communications.
- Students will be able to write a functional, stand-alone assembly language program of the complexity of a basic telnet client, with no help from external libraries.

Systems Security Engineering

Definition:

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.

Topics:

- Design of testing
- Testing methodologies
- Emergent Properties
- Systems Engineering
- System Integration
- Make or Buy Analysis
- Systems Security Analysis
- Enterprise system components

Outcomes:

- Students will be able to analyze system components and determine how they will interact in a composed system.
- Students will be able to analyze a system design and determine if the design will meet the system security requirements.

Virtualization Technologies

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to describe the fundamental concepts of virtualization.
- Students will be able to compare and contrast the different virtualization architectures.

Resources:

- The Evolution of an x86 Virtual Machine Monitor, Agesen, et. al.
- Yogi Dandass (MS State)

Vulnerability Analysis

Definition:

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.

Topics:

- 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

Outcomes:

- Students will be able to describe characteristics of malware.
- Students will be able to identify malware.
- Students will be able to apply tools and techniques for identifying vulnerabilities.

Wireless Sensor Networks

Definition:

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.

Topics:

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

Outcomes:

- Students will be able to describe the challenges associated with wireless sensor networks, including coordination, energy efficiency, self organization and security.