Fundamentals of Cyber Security (5 credits)

Course Description

This course provides students with an introduction to cyber threats and defense against them, networking concepts, IT system components, IA fundamentals, basic scripting, and basic data analysis; and an overview of cyber operations, digital forensics, and incident analysis and response.

Unit 1.1 (Required for Cyber Security Certificate 1.1 in *Cyber Threats*)

Outcomes

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

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)

Unit 1.2 (Required for Cyber Security Certificate 1.2 in *Cyber Defense*)

Outcomes

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

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)

Unit 1.3 (Required for Cyber Security Certificate 1.3 in *Networking Concepts*)

Outcomes

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

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

Unit 1.4 (Required for Cyber Security Certificate 1.4 in *IT System Components*)

Outcomes

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

Topics

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

Unit 1.5 (Required for Cyber Security Certificate 1.5 in *IA Fundamentals*)

Outcomes

1. Students shall be able to list the fundamental concepts of the Information Assurance / Cyber Defense discipline.
2. Students will be able to describe how the fundamental concepts of cyber defense can be used to provide system security.
3. 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.

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)

Unit 1.6 (Required for Cyber Security Certificate 1.6 in *Basic Scripting*)

Outcomes

1. 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).
2. Students will be able to write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
3. Students will be able to write simple linear and looping scripts.

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

Unit 1.7 (Required for Cyber Security Certificate 1.7 in *Basic Data Analysis*)

Outcomes

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

Topics

Summary Statistics
Graphing / Charts

Spreadsheet Functions
Problem solving

Unit 1.8 (Required for Cyber Security Certificate 1.8 in *Overview of Cyber Operations*)

Outcomes

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

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

Unit 1.9 (Required for Cyber Security Certificate 1.9 in *Digital Forensics*)

Outcomes

1. Students shall be able to discuss the rules, laws, policies, and procedures that affect digital forensics
2. Students shall be able to use one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.
3. 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.

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

Policy Development, Compliance, Cyber Law, and Cyber Investigations (4 credits)

Course Description

This course informs students of important policy, legal, and ethical matters; communicates IA compliance and IA standards; and develops applied skills in life-cycle security, supply chain security, and fraud prevention and management.

Unit 2.1 (Required for Cyber Security Certificate 2.1 in *Policy, Legal, Ethics and Compliance*)

Outcomes

1. 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.
2. Students shall be able to describe their responsibilities related to the handling of information about vulnerabilities.
3. Students will be able to describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.

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

Unit 2.2 (Required for Cyber Security Certificate 2.2 in *IA Compliance*)

Outcomes

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

Topics

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

Unit 2.3 (Required for Cyber Security Certificate 2.3 in *IA Standards*)

Outcomes

1. Students will be able to describe the impact of legal/regulatory standards on a given system.
2. 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.

Topics

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

Unit 2.4 (Required for Cyber Security Certificate 2.4 in *Life-Cycle Security*)

Outcomes

1. 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.
2. Students will be able to list and describe the phases of the system life-cycle.
3. Students will be able to list and describe the elements of a maturity model.

Topics

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

Unit 2.5 (Required for Cyber Security Certificate 2.5 in *Supply Chain Security*)

Outcomes

1. Specified by Drew Hamilton, Auburn University

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

Unit 2.6 (Required for Cyber Security Certificate 2.6 in *Fraud Prevention and Management*)

Outcomes

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

6. Students will be able to describe common methods of financial statement fraud.

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

Network and Systems Security Administration (4 credits)

Course Description

This course provides students with effective working knowledge in vulnerability analysis and security risk analysis, cyber-security planning and management, security program management, and systems certification and accreditation; and delivers applied skills in systems administration, network technology and protocols, introductory cryptography, and intrusion detection and prevention systems.

Unit 3.1 (Required for Cyber Security Certificate 3.1 in *Vulnerability Analysis*)

Outcomes

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

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

Unit 3.2 (Required for Cyber Security Certificate 3.2 in *Security Risk Analysis*)

Outcomes

1. Students will be able to describe how risk relates to a system security policy.
2. Students will be able to describe various risk analysis methodologies.
3. 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.
4. Students will be able to compare the advantages and disadvantages of various risk assessment methodologies
5. Students will be able to select the optimal methodology based on needs, advantages and disadvantages.

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

Unit 3.3 (Required for Cyber Security Certificate 3.3 in *Cybersecurity Planning and Management*)

Outcomes

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

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

Unit 3.4 (Required for Cyber Security Certificate 3.4 in *Security Program Management*)

Outcomes

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

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

Unit 3.5 (Required for Cyber Security Certificate 3.5 in *Systems Certification and Accreditation*)

Outcomes

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

Topics

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

Unit 3.6 (Required for Cyber Security Certificate 3.6 in *Systems Administration*)

Outcomes

1. 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.

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

Unit 3.7 (Required for Cyber Security Certificate 3.7 in *Network Technology and Protocols*)

Outcomes

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

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

Unit 3.8 (Required for Cyber Security Certificate 3.8 in *Intro to Cryptography*)

Outcomes

1. Students will be able to identify the elements of a cryptographic system.
2. Students will be able to describe the differences between symmetric and asymmetric algorithms.
3. Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation.
4. 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.

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)

Unit 3.9 (Required for Cyber Security Certificate 3.9 in *Intrusion Detection / Prevention Systems*)

Outcomes

1. Students will be able to demonstrate the ability to detect, identify, resolve and document host or network intrusions.
2. 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.
3. Students will be able to demonstrate the ability to configure IDS/IPS systems to reduce false positives and false negatives.

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

Network Security Engineering (4 credits)

Course Description

This course adds to students' applied cyber-security skills a deeper level of expertise within network security engineering, including advanced network topology and protocols, network defense, network forensics, digital communications, and penetration testing.

Unit 4.1 (Required for Cyber Security Certificate 4.1 in *Advanced Network Technology & Protocols*)

Outcomes

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

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

Unit 4.2 (Required for Cyber Security Certificate 4.2 in *Network Defense*)

Outcomes

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

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)

Unit 4.3 (Required for Cyber Security Certificate 4.3 in *Network Forensics*)

Outcomes

1. Students will be able to describe the methodologies used in network forensics.
2. 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.

Topics

Packet Capture and Analysis
Intrusion Detection and Prevention
Interlacing of device and network forensics
Log-file Analysis
Forensic Imaging and Analysis
Hands-on activities

Unit 4.4 (Required for Cyber Security Certificate 4.4 in *Digital Communications*)

Outcomes

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

Topics

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

Unit 4.5 (Required for Cyber Security Certificate 4.5 in *Penetration Testing*)

Outcomes

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

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

Systems Security Engineering (4 credits)

Course Description

This course adds to students' applied cyber-security skills a deeper level of expertise within systems security engineering, including fundamental security design principles, IA architectures, operating systems concepts, operating systems hardening, low-level programming, and QA and functional testing.

Unit 5.1 (Required for Cyber Security Certificate 5.1 in *Systems Security Engineering*)

Outcomes

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

Topics

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

Unit 5.2 (Required for Cyber Security Certificate 5.2 in *Fundamental Security Design Principles*)

Outcomes

1. Students will be able to list the first principles of security.
2. 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.
3. Students will be able to analyze common security failures and identify specific design principles that have been violated.
4. Given a specific scenario, students will be able to identify the needed design principle.
5. Students will be able to describe why good human machine interfaces are important to system use.
6. Students will understand the interaction between security and system usability and the importance for minimizing the affects of security mechanisms

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

Unit 5.3 (Required for Cyber Security Certificate 5.3 in *IA Architectures*)

Outcomes

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

Topics

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

Unit 5.4 (Required for Cyber Security Certificate 5.4 in *Operating Systems Concepts*)

Outcomes

1. 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).

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

Unit 5.5 (Required for Cyber Security Certificate 5.5 in *Operating Systems Hardening*)

Outcomes

1. Students will be able to describe, for a given OS, the steps necessary for hardening the OS with respect to various applications.
2. 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.

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

Unit 5.6 (Required for Cyber Security Certificate 5.6 in *Low Level Programming*)

Outcomes

1. 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.

Topics

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

Unit 5.7 (Required for Cyber Security Certificate 5.7 in *QA / Functional Testing*)

Outcomes

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

Topics

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

Secure Mobile Technology and Telecommunications (4 credits)

Course Description

This course enables students to gain operational understanding and working skills in secure mobile technologies, including RF principles, systems programming, wireless sensor networks, hardware and firmware security, and analog telecommunications systems.

Unit 6.1 (Required for Cyber Security Certificate 6.1 in *Mobile Technologies*)

Outcomes

1. 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.
2. Students will be able to explain the weaknesses of WEP and which ones have been addressed and how.

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)

Unit 6.2 (Required for Cyber Security Certificate 6.2 in *RF Principles*)

Outcomes

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

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

Unit 6.3 (Required for Cyber Security Certificate 6.3 in *Systems Programming*)

Outcomes

1. Students shall be able to implement new functions in an OS kernel
2. Students will be able to develop complex and sophisticated programs, such as a device driver, that can be embedded into an OS kernel.
3. Students will be able to write a program that implements a network stack to manage network communications.

4. 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.

Topics

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

Unit 6.4 (Required for Cyber Security Certificate 6.4 in *Wireless Sensor Networks*)

Outcomes

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

Topics

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

Unit 6.5 (Required for Cyber Security Certificate 6.5 in *Hardware/Firmware Security*)

Outcomes

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

Topics

Microcode
Firmware
Hardware Abstraction Layers
Virtualization Layers

Unit 6.6 (Required for Cyber Security Certificate 6.6 in *Analog Telecommunications Systems*)

Outcomes

1. Students will be able to describe the basic concepts of modern analog communications systems, using block diagrams.
2. 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.

Topics

Signaling Methods
Architecture
Trunks, Switching
Grade of Service

Blocking
Call Arrival Models
Interference Issues

Secure Cloud Computing and Software Development (4 credits)

Course Description

This course teaches students secure programming and development skills and practices, data structures, operating systems theory, virtualization technologies, and advanced cryptography within the context of secure cloud computing.

Unit 7.1 (Required for Cyber Security Certificate 7.1 in *Secure Programming Practices*)

Outcomes

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

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

Unit 7.2 (Required for Cyber Security Certificate 7.2 in *Data Structures*)

Outcomes

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

Topics

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

Unit 7.3 (Required for Cyber Security Certificate 7.3 in *Operating Systems Theory*)

Outcomes

1. 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.

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

Unit 7.4 (Required for Cyber Security Certificate 7.4 in *Virtualization Technologies*)

Outcomes

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

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

Unit 7.5 (Required for Cyber Security Certificate 7.5 in *Advanced Cryptography*)

Outcomes

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

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

Unit 7.6 (Required for Cyber Security Certificate 7.6 in *Cloud Computing*)

Outcomes

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

Topics

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

Digital Forensics, Data Security Analysis, and Data Management Systems Security (4 credits)

Course Description

This course enables students to attain competency in database security, data administration, forensic accounting, device forensics, host forensics, media forensics, and the principles of software reverse engineering.

Unit 8.1 (Required for Cyber Security Certificate 8.1 in *Databases*)

Outcomes

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

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

Unit 8.2 (Required for Cyber Security Certificate 8.2 in *Database Management Systems*)

Outcomes

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

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)

Unit 8.3 (Required for Cyber Security Certificate 8.3 in *Data Administration*)

Outcomes

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

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)

Unit 8.4 (Required for Cyber Security Certificate 8.4 in *Forensic Accounting*)

Outcomes

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

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

Unit 8.5 (Required for Cyber Security Certificate 8.5 in *Device Forensics*)

Outcomes

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

Topics

Mobile Device Analysis
Tablets
SmartPhones
GPS
Hands-on activities

Unit 8.6 (Required for Cyber Security Certificate 8.6 in *Host Forensics*)

Outcomes

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

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
Hands-on activities

Unit 8.7 (Required for Cyber Security Certificate 8.7 in *Media Forensics*)

Outcomes

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

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
Hands-on activities

Unit 8.8 (Required for Cyber Security Certificate 8.8 in *Software Reverse Engineering*)

Outcomes

1. 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.

Topics

Specification Recovery
Malware Analysis
Reverse Engineering Tools & Techniques
Sandboxing