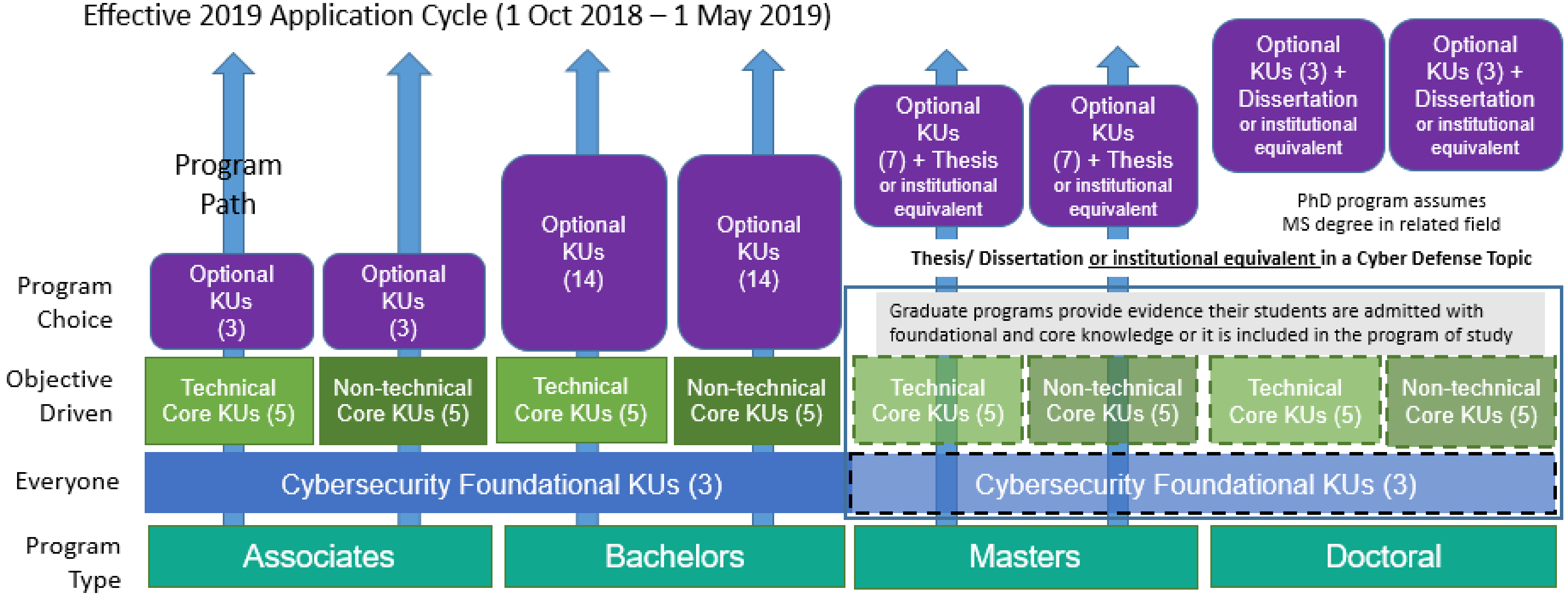
Centers of Academic Excellence in Cyber Defense (CAE-CD)
2019 Knowledge Units

Knowledge Unit Usage Notional Structure

Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) Designation Requirements,

Effective 2019 Application Cycle (1 Oct 2018 – 1 May 2019)



Program Path

Program Choice

Objective Driven

Everyone

Program Type

Optional KUs (3)

Optional KUs (3)

Optional KUs (14)

Optional KUs (14)

Optional KUs (7) + Thesis or institutional equivalent

Optional KUs (7) + Thesis or institutional equivalent

Optional KUs (3) + Dissertation or institutional equivalent

Optional KUs (3) + Dissertation or institutional equivalent

PhD program assumes MS degree in related field

Thesis/ Dissertation or institutional equivalent in a Cyber Defense Topic

Graduate programs provide evidence their students are admitted with foundational and core knowledge or it is included in the program of study

Technical Core KUs (5)

Non-technical Core KUs (5)

Technical Core KUs (5)

Non-technical Core KUs (5)

Technical Core KUs (5)

Non-technical Core KUs (5)

Technical Core KUs (5)

Non-technical Core KUs (5)

Cybersecurity Foundational KUs (3)

Cybersecurity Foundational KUs (3)

Associates

Bachelors

Masters

Doctoral

Knowledge Units (KUs):

Foundational: Cybersecurity Foundations, Cybersecurity Principles, and IT Systems Components

Technical Core: Basic Scripting and Programming; Basic Networking; Network Defense; Basic Cryptography; Operating Systems Concepts

Nontechnical Core: Cyber Threats; Policy, Legal, Ethics, and Compliance; Security Program Management; Security Risk Analysis; Cybersecurity Planning and Management

Model KU Structure

Name: The name used to identify a knowledge unit. The name is followed by a three letter key in parenthesis. The key is for indexing in data structures.

Description: A short narrative description of the scope and contents of the knowledge unit. The intent of this knowledge unit is to provide students with a [basic/intermediate/advanced] awareness of [details].

Outcomes: A description of student based outcomes associated to the knowledge unit.

Students will be able to [outcome #1].
Students will be able to [outcome #2].

KU Topics: A list of elements in the KU. These topics should be listed in an appropriate hierarchy of detail. The format of the topics element should appear as follows:

High level name 1 – description of the high level name
  Sub level name 1 – description of first sub level element
  Sub level name 2 – description of second sub level element
High level name 2 – description of the high level name
. . .
High level name N – description of the high level name

Vocabulary: A list of vocabulary terms

Related Knowledge Units: A list of KUs that are related to this one

Specializations: List of Specializations which use this KU

NICE Framework Categories: A connection to NICE Framework at the Categories level

Foundational KU’s

Cybersecurity Foundations
Cybersecurity Principles
IT Systems Components

The foundational knowledge units are required of all programs seeking designation. For associate and baccalaureate programs the foundational knowledge units will be mapped as part of the designation process. For Graduate level programs, the institution will need to define how they meet the foundational knowledge when it is considered pre-requisite to the graduate program.

Cybersecurity Foundations (CSF)

The intent of the Cybersecurity Foundations Knowledge Unit is to provide students with a basic understanding of the fundamental concepts behind cybersecurity. This is a high level introduction or familiarization of the Topics, not a deep dive into specifics.

Outcomes

To complete this KU, students should be able to:

1. Describe the fundamental concepts of the cyber security discipline and use to provide system security.
2. Describe potential system attacks and the actors that might perform them.
3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
4. Describe appropriate measures to be taken should a system compromise occur.
5. Properly use the Vocabulary associated with cyber security.

Topics

To complete this KU, all Topics and sub-Topics must be completed

1. Threats and Adversaries (threat actors, malware, natural phenomena)
2. Vulnerabilities and Risk management (include backups and recovery)
3. Common Attacks
4. Basic Risk Assessment
5. Security Life-Cycle
6. Applications of Cryptography and PKI
7. Data Security (in transmission, at rest, in processing)
8. Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
9. Access Control Models (MAC, DAC, RBAC, Lattice)
10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
11. Session Management
12. Exception Management
13. Security Mechanisms (e.g., Identification/Authentication, Audit)
14. Malicious activity detection / forms of attack
15. Appropriate Countermeasures
16. Legal issues
17. Ethics (Ethics associated with cybersecurity profession)

Vocabulary

Advanced persistent threat (APT), attacker, Block ciphers, DoS, DDoS, malware, mitigations, residual risk, risk, stream ciphers, vulnerability

NICE Framework Categories

Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)
Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)
Investigate (IN)		

Cybersecurity Principles (CSP)

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

Outcomes

To complete this KU, students should be able to:

1. Define the principles of cybersecurity.
2. Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.
3. Analyze common security failures and identify specific design principles that have been violated.
4. Given a specific scenario, identify the design principles involved or needed.
5. Understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.

Topics

1. Principles (must cover all of the sub-Topics)
    a. Separation (of domains/duties)
    b. Isolation
    c. Encapsulation
    d. Modularity
    e. Simplicity of design (Economy of Mechanism)
    f. Minimization of implementation (Least Common Mechanism)
    g. Open Design
    h. Complete Mediation
    i. Layering (Defense in depth)
    j. Least Privilege
    k. Fail Safe Defaults / Fail Secure
    l. Least Astonishment (Psychological Acceptability)
    m. Minimize Trust Surface (Reluctance to trust)
    n. Usability
    o. Trust relationships

Vocabulary

Packet, risk, secure system, trust, trusted system, trustworthy, vulnerability

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

IT Systems Components (ISC)

The intent of the IT Systems Components Knowledge Unit is to provide students with a basic understanding of the components in an information technology system and their roles in system operation. This is a high level introduction or familiarization of the Topics, not a deep dive into specifics.

Outcomes

To complete this KU, students should be able to:

1. Describe the hardware components of modern computing environments and their individual functions.
2. Describe the basic security implications of modern computing environments.
3. Understand the Federal, State and Local Cyber Defense partners/structures.
4. Properly use the Vocabulary associated with cyber security.

Topics

1. Endpoint protection
   a. Workstations, servers, appliances, mobile devices, peripheral devices (Printers, scanners, external storage)
2. Storage Devices
3. System Architectures
   a. Virtualization / Containers
   b. Cloud
4. Alternative environments (SCADA, real time systems, critical infrastructures)
5. Networks (Internet, LANs, wireless)
6. Network mapping (enumeration and identification of network components)
7. Network Security Components (Data Loss Prevention, VPNs / Firewalls)
8. Intrusion Detection and Prevention Systems, Incident Response
9. Managed Services
10. Software Security (secure coding principles, software issues by type)
11. Configuration Management
12. Patching
    a. OS and Application Updates
13. Vulnerability Scanning (core)
    a. Vulnerability Windows (0-day to patch availability)
14. People and security (social engineering)
15. Physical and environmental security concerns
16. Internet Of Things (IOT)
17. Cyber Defense Partnerships (Federal, State, Local, Industry)

Vocabulary

BYOD, IaaS, PaaS, SaaS, SAN, USB

NICE Framework Categories

Securely Provision (SP)
Protect and Defend (PR)
Investigate (IN)
Operate and Maintain (OM)
Analyze (AN)
Oversee and Govern (OV)
Collect and Operate (CO)

Technical Core KUs

Basic Cryptography
Basic Networking
Basic Scripting and Programming
Network Defense
Operating Systems Concepts

Each program at the associate or baccalaureate level a set of core knowledge units needs to be chosen to support their program of study requirements. The five knowledge units listed above constitute the set of Technical core which apply for all programs of study leading to technical jobs.

Basic Cryptography (BCY)

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

Outcomes

To complete this KU, students should be able to do some of the following:

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

1. Common cryptographic uses
    a. Security Functions (data protection, data integrity, authentication, non-repudiation)
    b. Block vs. stream data
    c. Digital Signatures (Authentication)
2. Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)
    a. Integrity checking
    b. For protecting authentication data
    c. Collision resistance
3. Symmetric Cryptography (DES, Twofish)
4. Public Key Cryptography (Diffie-Hellman, RSA, ECC, ElGamal, DSA)
    a. Public Key Infrastructure
    b. Certificates
    c. Key Management (creation, exchange/distribution)
5. Cryptography in practice
    a. Common Cryptographic Protocols
    b. DES -> AES (evolution from DES to AES)
    c. Cryptographic Modes (and their strengths and weaknesses)
    d. Cryptographic standards (FIPS 140 series)
6. Cryptographic failures
    a. Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)
    b. Implementation failures

NICE Framework Categories

Securely Provision (SP)
Protect and Defend (PR)
Investigate (IN)
Operate and Maintain (OM)
Analyze (AN)
Oversee and Govern (OV)
Collect and Operate (CO)

Specializations

Data Management Systems Security
Digital Forensics (Specialization)
Health Care Security

Related Knowledge Units

Introduction to Cryptography (2014)

Basic Networking (BNW)

The intent of the Basic Networking Knowledge Unit is to provide students with basic understanding of how networks are built and operate, and to give students some experience with basic network analysis tools. Students are exposed to the concept of potential vulnerabilities in a network.

Outcomes

To complete this KU, students should be able to do some of the following:

1. Describe the fundamental concepts, technologies, components and issues related to communications and data networks.
2. Design a basic network architecture given a specific need and set of hosts/clients.
3. Track and identify the packets involved in a simple TCP connection (or a trace of such a connection).
4. Use a network monitoring tools to observe the flow of packets (e.g., WireShark).
5. Perform network mapping (enumeration and identification of network components) (e.g., Nmap).
6. Describe common network vulnerabilities.

Topics

1. Networking models (OSI and IP).
2. Network media (wired, optical, and wireless)
3. Network Architectures and topologies (PAN, LAN/WAN, DMZ, Enclaves, VLAN, NAT, subnetting, supernetting)
4. Common Network Devices and their role in the network. (Routers, Switches, Hosts, VPNs, Firewalls)
5. Network Protocols introduction (IP, TCP, UDP, ICMP)
6. Network Services and protocols introduction (DNS, NTP, VLAN, etc.).
7. Network Applications and protocols introduction (SMTP, HTTP, VoIP, SSH, etc.).
8. Use of basic network administration tools.
9. Overview of Network Security Issues

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Management Systems Security
Data Security Analysis
Digital Forensics (Specialization)
Health Care Security
Industrial Control Systems-SCADA Security
Secure Mobile Technology

Related Knowledge Units

Network Defense (2014 Core CDE)
Network Technology and Protocols (2014 Core CDE)
Advanced Network Technology and Protocols
Network Security Administration
Intrusion Detection/Prevention Systems
Wireless Sensor Networks

Original Knowledge Unit

Networking Concepts (2014)

Suggested textbooks
Network+ Guide to networks
CompTIA Network+ Guide to Managing and Troubleshooting Networks by Mike Meyers

Basic Scripting and Programming (BSP)

The intent of this Basic Scripting and Programming Knowledge Unit is to provide students with the basic ability to create simple scripts/programs to automate and perform simple operations, and to provide students with the skills necessary to implement algorithms using programming languages to solve problems. This knowledge includes basic security practices in developing scripts/programs (e.g., bounds checking, input validation).

Outcomes

To complete this KU, students should be able to:

1. Demonstrate their proficiency in the use of scripting languages to write simple scripts (e.g., to automate system administration tasks).
2. Write simple linear and looping scripts.
3. Write simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
4. Demonstrate proficiency in the use of a programming language to solve complex problems in a secure and robust manner.

Topics

1. Implement basic security concepts
    a. Permissions, bounds checking, input validation, type checking and parameter validation
2. Be familiar with the concept and basic implementation of regular expressions.
3. Understand basic data structures and algorithms
4. Basic Boolean logic/operations.
    a. AND / OR / XOR / NOT
5. Scripting on both Windows and Linux
    a. Language (e.g. PERL, Python, BASH, JAVA, VB Scripting, Powershell)
6. Properly apply basic programming constructs and concepts including:
    a. Variables and types (int, float, char, etc.)
    b. Strings, arrays, structures
    c. Sequential and parallel execution
    d. Assignments (:=, =, ++, --, etc.)
    e. Decisions and branching (if, if ... else, elseif, switch, case, etc.)
    f. Loops (for, while, repeat, etc.)
    g. Functions, procedures, and calls
    h. Debugging techniques

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Security Analysis
Digital Forensics (Specialization)

Related Knowledge Units

Programming (2014)

Network Defense (NDF)

The intent of the Network Defense Knowledge Unit is to provide students with knowledge of the concepts used in defending a network, and the basic tools and techniques that can be taken to protect a network and communication assets from cyber threats.

Outcomes

To complete this KU, students should be able to do some of the following:

1. Describe the key concepts in network defense (defense in depth, minimizing exposure, etc.).
2. Explain how network defense tools (firewalls, IDS, etc.) are used to defend against attacks and mitigate vulnerabilities.
3. Analyze how security policies are implemented on systems to protect a network.
4. Evaluate how network operational procedures relate to network security.

Topics

Because of the nature of the material - All topics and sub topics are required in this KU

1. Outline concepts of network defense, such as:
    a. Defense in Depth
    b. Network attacks
    c. Network Hardening
    d. Minimizing Exposure (Attack Surface and Vectors)
2. Network defense/monitoring tools:
    a. Implementing Firewalls
    b. DMZs / Proxy Servers
    c. VPNs
    d. Honeypots and Honeynets
    e. Implementing IDS/IPS
3. Network Operations
    a. Network Security Monitoring
    b. Network Traffic Analysis
4. Network security policies as they relate to network defense/security:
    a. Network Access Control (internal and external)
    b. Network Policy Development and Enforcement

NICE Framework Categories

Securely Provision (SP)
Protect and Defend (PR)
Investigate (IN)
Operate and Maintain (OM)
Analyze (AN)
Oversee and Govern (OV)
Collect and Operate (CO)

Specializations

Health Care Security
Industrial Control Systems-SCADA Security
Network Security Administration (Specialization)

Related Knowledge Units

Networking Concepts (2014 Core 2Y)
Network Technology and Protocols (2014 Core CDE)
Advanced Network Technology and Protocols
Network Security Administration
Intrusion Detection/Prevention Systems
Wireless Sensor Networks

Original Knowledge Unit

Network Defense (2014)

Operating Systems Concepts (OSC)

The intent of this Operating Systems Concepts 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.

Outcomes

To complete this KU, students should be able to do the following:

1. Describe the role and basic functions of an operating system, and how operating systems interact with hardware and software applications.
2. Identify and describe basic security issues of operating systems.

Topics

To complete this KU, all Topics and sub-Topics must be completed

1. Privileged and non-privileged states
2. Application processes and threads
3. Memory (real, virtual, and management)
4. Files systems
5. Virtualization / hypervisors
6. Creation and operation of virtualization technology
7. Fundamental security design principles as applied to an OS
8. Access controls (models and mechanisms)
9. Domain separation, process isolation, resource encapsulation, least privilege

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Management Systems Security
Digital Forensics
Industrial Control Systems-SCADA Security

Related Knowledge Units

Operating Systems Concepts (2014)

Non-Technical Core KUs

Cyber Threats
Cybersecurity Planning and Management
Policy, Legal, Ethics, and Compliance
Security Program Management
Security Risk Analysis

Each program at the associate or baccalaureate level a set of core knowledge units needs to be chosen to support their program of study requirements. The five knowledge units listed above constitute the set of non-technical core which apply for all programs of study leading to non-technical jobs.

Cyber Threats (CTH)

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

Outcomes

To complete this KU, students should be able to:

1. Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk.
2. Describe different types of attacks and their characteristics.

Topics

To complete this KU, all Topics and sub-Topics must be completed.

1. Motivations and Techniques
2. The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)
3. Types of Attacks (and vulnerabilities that enable them)
    a. Password guessing / cracking
    b. Backdoors / trojans / viruses / wireless attacks
    c. Sniffing / spoofing / session hijacking
    d. Denial of service / distributed
    e. DOS / BOTs
    f. MAC spoofing / web app attacks / 0-day exploits
    g. Advanced Persistent Threat (APT)
4. Events that indicate an attack is/has happened
5. Attack Timing (within x minutes of being attached to the net)
6. Attack surfaces / vectors, and trees
7. Covert Channels
8. Social Engineering
9. Insider problem
10. Threat Information Sources (e.g., CERT)
11. Legal Issues associated with cyber threats

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Management Systems Security
Health Care Security
Industrial Control Systems-SCADA Security
Network Security Administration (Specialization)

Network Security Engineering
Secure Embedded Systems
Secure Mobile Technology
Secure Software Development
Secure Telecommunications
Security Incident Analysis and Response
System Security Administration
Systems Security Engineering (Specialization)

Related Knowledge Units

Cyber Threats (2014)

Cybersecurity Planning and Management (CPM)

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

Outcomes

To complete this KU, students should be able to:

1. Examine the placement of security functions in a system and describe the strengths and weaknesses
2. Develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response.
3. Develop system specific plans for:
    a. The protection of intellectual property
    b. The implementation of access controls
    c. Patch and change management
4. Outline and explain the roles of personnel in planning and managing security, including:
    a. Board of Directors
    b. Senior Management
    c. Chief Information Security Officer (CISO)
    d. IT Management (CIO, IT Director, etc)
    e. Functional Area Management
    f. Information Security personnel
    g. End users

Topics

1. Broad coverage of the cybersecurity Common Body of Knowledge (CBK) and how it affects planning and management.
2. Differentiate and provided examples of Operational, Tactical, and Strategic Planning and Management
3. Examine C-Level Functions which impact cybersecurity.
4. Making cybersecurity a strategic essential (part of core organizational strategy)
5. Identify requirements and create plans for Business Continuity / Disaster Recovery
6. Develop processes and procedures for incident response
7. Planning for protection of intellectual property
8. Managing the implementation of access controls
9. Managing patch and change control

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Management Systems Security
Industrial Control Systems-SCADA Security
Security Incident Analysis and Response

Related Knowledge Units

Cybersecurity Planning and Management (2014)

Policy, Legal, Ethics, and Compliance (PLE)

The intent of the Policy, Legal, Ethics, and Compliance Knowledge Unit is to provide students with and understanding of information assurance in context and the rules and guidelines that control them.

Outcomes

To complete this KU, students should be able to:

1. 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. Describe their responsibilities related to the handling of data as it pertains to legal, ethical and/or agency auditing issues.
3. Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it.

Topics

To complete this KU, all Topics and sub-Topics must be completed.

1. Federal Laws and Authorities
    a. Computer Security Act
    b. Sarbanes – Oxley
    c. Gramm – Leach – Bliley
    d. Privacy (COPPA) HIPAA / FERPA
    e. USA Patriot Act
    f. Americans with Disabilities Act, Section 508
    g. Other Federal laws and regulations
2. State, US and international standards / jurisdictions
3. Payment Card Industry Data Security Standard (PCI DSS)
4. BYOD issues

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Management Systems Security
Digital Forensics (Specialization)
Health Care Security
Network Security Administration (Specialization)
Secure Cloud Computing
Secure Embedded Systems
Secure Mobile Technology
Secure Telecommunications

Related Knowledge Units

Policy, Legal, Ethics, and Compliance (2014)

Suggested textbooks

Title: Cyberethics: Morality and Law in Cyberspace, Sixth Edition, Author: Spinello ISBN: 978-1-284-08139-8

Security Program Management (SPM)

The intent of the Security Program Management 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.

Outcomes

To complete this KU, students should be able to:

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

Topics

1. Goals and objectives of a security program.
2. Measuring the effectiveness of a security program (metrics).
3. Roles and Responsibilities of the Security Organization
4. Security Policies.
    a. Compliance with Applicable Laws and Regulations
    b. Security best practices and frameworks.
5. Security Baselining
6. Program Monitoring and Control
7. Security Awareness, Training and Education
8. Security program addresses:
    a. Physical Security
    b. Personnel Security
    c. System and Data Identification
    d. System security plans.
    e. Configuration and Patch management
    f. System Documentation
    g. Incident Response Program
    h. Disaster Recovery Program.
    i. Certification and Accreditation

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Security Analysis
Health Care Security

Original Knowledge Unit

Security Program Management (2014)

Security Risk Analysis (SRA)

The intent of the Security Risk Analysis 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.

Outcomes

To complete this KU, students should be able to:

1. Describe how risk relates to a system security policy.
2. Describe various risk analysis methodologies.
3. Evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
4. Compare the advantages and disadvantages of various risk assessment methodologies
5. Select the optimal methodology based on needs, advantages and disadvantages.

Topics

1. Risk Assessment/Analysis Methodologies
2. Risk Measurement and Evaluation Methodologies
3. Risk Management Models
4. Risk Management Processes
5. Risk Mitigation Economics
6. Risk Transference/Acceptance/Mitigation
7. Communication of Risk

NICE Framework Categories

Securely Provision (SP)
Operate and Maintain (OM)
Oversee and Govern (OV)
Protect and Defend (PR)
Analyze (AN)
Collect and Operate (CO)
Investigate (IN)

Specializations

Data Management Systems Security
Data Security Analysis
Industrial Control Systems-SCADA Security
Secure Cloud Computing
Secure Mobile Technology

Related Knowledge Units

Security Risk Analysis (2014)

Optional KU’s

Programs need to document their programs of study using knowledge units. The categories of knowledge units are foundational (used in all programs), core (either technical or nontechnical) which form the base of the program. The remainder of the knowledge units are called optional KUs, and this is a category that can be adopted by any program as needed to document their program of study. Additionally, opposing core KUs may be used as optional KUs (i.e. If technical core is chosen, then non-technical core may be used as optional KUs and if non-technical core is chosen, then technical core may be used as optional KUs.)

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

Advanced Algorithms (AAL)

The intent of the Advanced Algorithms 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.

Outcomes

1. Students should understand and be able to implement the algorithms listed in the topics.

Topics

1. Bloom filters
2. Naive Bayes
3. Map-Reduce
4. Dynamic Programming algorithms
5. Markov Chain Monte Carlo
6. Coding and Compression
7. Artificial Intelligence algorithms

Specializations

None

Related Knowledge Units

Algorithms (2014)

Advanced Cryptography (ACR)

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

Outcomes

To complete this KU, students should be able to:

1. Describe how various cryptographic algorithms and protocols work.
2. Evaluate security mechanisms based on cryptography.
3. Describe the application of cryptography in SSL, virtual private networks, secure storage, and other security applications.
4. Take a mode or protocol diagram and identify how an error propagates through the cryptosystem.

Topics

1. Number Theory
2. Probability and Statistics
3. Understanding of the major algorithms (AES, RSA, EC)
4. Suite B Algorithms
5. Understanding of the families of attacks (differential, man-in-the-middle, linear, etc.)
6. Hashing and Signatures
7. Key Management
8. Modes and appropriate uses
9. Classical Cryptanalysis (a la Konheim)
10. Identity-based Cryptography
11. Digital Signatures
12. Virtual Private Networks
13. Quantum Key Cryptography

Specializations

Network Security Engineering
Secure Cloud Computing

Related Knowledge Units

Advanced Cryptography (2014)

Advanced Network Technology and Protocols (ANT)

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

Outcomes

To complete this KU, students should be able to:

1. Explore in depth advanced and novel areas of networks and protocols.
2. Describe and discuss the security issues and implications of advanced and novel networks and protocols.
3. Develop the intellectual tools to explore and understand advance network concepts and protocols.

Topics

Topics would be a selection from among the following:

1. Advanced Routing algorithms and protocols
   a. BGP
   b. OSPF
   c. MPLS
2. Software Defined Networking
   a. Principles, protocols, implications
3. IPv6 Networking Suite
   a. IPv6 Security Issues
4. Quality of Service
5. Network Services
6. Social Network implementation and security issues.
7. Voice over IP (VoIP)
8. Multicasting
9. Advanced Network Security Topics
   a. Secure DNS
   b. Network Address Translation
   c. Deep Packet Inspection
   d. Transport Layer Security

Specializations

Network Security Administration
Network Security Engineering
Secure Cloud Computing
Secure Mobile Technology
Secure Telecommunications
Systems Security Engineering

Related Knowledge Units

Networking Concepts
Network Defense
Network Technology and Protocols
Network Security Administration
Intrusion Detection/Prevention Systems
Wireless Sensor Networks

Original Knowledge Unit

Advanced Network Technology and Protocols (2014)

Algorithms (ALG)

The intent of the Algorithms 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.

Outcomes

1. Students should understand and be able to implement the algorithms listed in the topics.

Topics

1. Algorithm Analysis
2. Computational Complexity
3. Best/Worst/Average Case Behavior
4. Optimization
5. Searching / Sorting
6. String matching algorithms
7. Iterative
8. Recursion
9. Greedy Algorithm
10. Hill Climbing

Specializations

Secure Software Development

Related Knowledge Units

Algorithms (2014)

Analog Telecommunications (ATC)

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

Outcomes

To complete this KU, students should be able to:

1. Describe the basic concepts of modern analog communications systems, using block diagrams.
2. 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

1. Signaling Methods
2. Architecture
3. Trunks, Switching
4. Grade of Service
5. Blocking
6. Call Arrival Models
7. Interference Issues

Specializations

Network Security Engineering
Secure Telecommunications

Related Knowledge Units

Analog Telecommunications (2014)

Basic Cyber Operations (BCO)

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

Outcomes

To complete this KU, students should be able to:

1. Describe the laws that provide US entities the authority to perform cyber operations.
2. List the phases of a well-organized cyber operation and describe the goals and objectives of each phase.
3. Identify specific phases of a cyber operation in network traffic.
4. Describe potential motivations that might prompt an entity to perform a cyber operation.

Topics

1. Legal Authorities and Ethics
2. Stages of a Cyber Operation (and details of each phase)
    a. Target Identification
    b. Reconnaissance o Gaining Access o Hiding Presence
    c. Establishing Persistence
    d. Execution
    e. Assessment
3. Basic Process Modeling
4. Validating Procedures
5. Handling failures to follow procedures
6. Case studies of actual cyber operations

Specializations

None

Related Knowledge Units

Overview of Cyber Operations (2014)

Cloud Computing (CCO)

The intent of the Cloud Computing 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.

Outcomes

To complete this KU, students should be able to:

1. Describe each type of service/model of cloud computing
2. Compare and contrast: local resource requirements, local control, network requirements, and security (attacks, mitigations, overall vulnerability)

Topics

1. Virtualization platforms
2. Cloud Services
    a. SaaS, PaaS, DaaS, IaaS
3. Service Oriented Architectures
4. Deployment Models
    a. private, public, community, hybrid
5. Security
6. Storage
7. Legal/Privacy Issues

Specializations

Data Management Systems Security
Secure Cloud Computing

Related Knowledge Units

Cloud Computing (2014)

Cyber Crime (CCR)

The intent of the Cyber Crime Knowledge Unit is to provide students with an understanding of Cyber Crimes and other abuses arising in a cyber environment.

Outcomes

To complete this KU, students should be able to:

1. Examine how the internet is used for cybercrime, cyber-stalking, and other abusive behaviors.
2. Evaluate the effectiveness of applications of cybersecurity in preventing crime and abuse.

Topics

1. Cyber Crime Types
    a. Intrusions
    b. Ransomware
    c. Espionage
    d. Intellectual Property
    e. Fraud and Financial
2. Cyber Stalking and Predators
3. Cyber Bullying
4. Sexual Exploitation
5. Identity Theft
6. Cyber Assisted Crimes
7. Cyber Terrorism
8. Cyber Crime Laws
    a. US Federal Laws
    b. International Laws
    c. Treaties

Specializations

Cyber Investigations

Cybersecurity Ethics (CSE)

The intent of the Cybersecurity Ethics Knowledge Unit is to provide students with an understanding of ethics in a cyber context, to examine typical situations where ethical dilemmas arise and to provide the students with tools for ethical decision making.

Outcomes

To complete this KU, students should be able to:

1. Explain how ethical foundations are applied to situations arising from the interconnected world.
2. Examine diverse ethical dilemmas.
3. Describe the role of cybersecurity in supporting and encouraging ethics, as well as where cybersecurity practices can cause ethical conflicts.

Topics

1. Ethical Codes and Frameworks
2. Ethics and Cyberspace
3. Ethical Issues
4. Property Availability Rights of others
5. Respect and principles of community Resource use, allocation, and abuse Censorship
6. Ethics-based decision tools
7. Cybersecurity and social responsibility

Specializations

Cyber Investigations

Data Administration (DBA)

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

Outcomes

To complete this KU, students should be able to:

1. Draw and describe a data and information lifecycle, identifying specific and general security issues at all stages.
2. Define and evaluate data and information quality, accessibility, and utility.
3. Examine how the origination, change, distribution, storage, and deletion of information is managed and secured.
4. Compare and contrast data and information ownership, stewardship, management, possession, and governance.
5. Outline the role of data and information classification in security.

Topics

1. Data/Information lifecycle
    a. Capture/Acquisition
    b. Maintenance
    c. Synthesis/transformation/aggregation
    d. Usage
    e. Publication/Distribution
    f. Archival
    g. Disposition/Purging
2. Data/Information Quality
    a. Accuracy, Completeness, relevance, consistency, integrity
    b. Data cleansing
    c. Verification/Validation
3. Data/Information accessibility
4. Data/Information utility
5. Data storage and archiving
    a. Data Warehousing
    b. Long Term Archival
    c. Big Data
        i. Hadoop / Mongo DB / HBASE
6. Data/Information control
    a. Ownership - Who information belongs to.
    b. Stewardship - Responsibility for assembling and protecting data.
    c. Management - Providing the right data in the right place at the right time.
    d. Possession - Data residing in a system.
    e. Governance - How data should be managed and used.
7. Data Policies
    a. Internal
    b. External
8. Data/Information Security (access control, encryption)
9. Data/Information classification systems.

a. Level of classification
b. Classification criteria
c. Need to know.
d. Classification/Declassification processes
e. Classification authorities

Specializations

Data Management Systems Security
Data Security Analysis
Health Care Security

Related Knowledge Units

Databases
Database Management Systems

Original Knowledge Unit

Data Administration

Data Structures (DST)

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

Outcomes

To complete this KU, students should be able to:

1. List the most common structures and data formats for storing data in a computer system.
2. Discuss the advantages and disadvantages of different data structures/formats.
3. Utilize common data structures
4. Implement data structures

Topics

1. Numerical
2. Strings
3. Lists (Linked List, Double Linked List, other list types, hash tables)
4. Arrays
5. Vectors
6. Heaps
7. Queues
8. Stacks
9. Buffers
10. Trees
11. Objects
12. Data Formats in languages
13. Categories

Specializations

Secure Software Development
Systems Security Engineering

Related Knowledge Units

Data Structures (2014)

Suggested textbooks

- Algorithms, 4th Edition by Robert Sedgewick and Kevin Wayne Addison-Wesley Professional, 2011, ISBN 0-321- 57351-X.
- Open Data Structures, by Pat Morin
- Mark A. Weiss, Data Structures and Algorithm Analysis in Java, Second Edition, Addison Wesley, 2007. ISBN # 0- 321-37013-9

Database Management Systems (DMS)

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

Outcomes

To complete this KU, students should be able to:

1. Compare and contrast database types including relational, hierarchical, distributed, and other models.
2. Describe the role of a database, a DBMS, and a database server within a complex system supporting multiple applications.
3. Apply SQL to create and administer databases and to manipulate the data they contain.
4. Describe DBMS access controls, privilege levels, and security principles and apply them to a simple database.
5. Outline common structures for storing data in a database management system.
6. Design and deploy a simple database for a specified application.

Topics

1. Overview of database types with advantages and disadvantages
    a. Flat
    b. Relational
    c. Network
    d. Hierarchical
    e. Object-Oriented
    f. Object-based
    g. Key-value
    h. Distributed
2. SQL Data Manipulation Language
    a. SELECT
    b. INSERT
    c. DELETE
    d. UPDATE
3. SQL Data Definition Language
4. SQL Database Administration
    a. User creation/deletion, permissions and access controls)
5. Database concepts
    a. Indexing, Inference, Aggregation, Polyinstantiation
6. Database Security
    a. How to protect data (confidentiality, integrity and availability in a DBMS context)
    b. Vulnerabilities (e.g., SQL injection)

Specializations

Data Management Systems Security
Health Care Security

Related Knowledge Units

Databases
Data Administration

Original Knowledge Unit

Database Management Systems (2014)

Databases (DAT)

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

Outcomes

To complete this KU, students should be able to:

1. Describe the role of a database, a database management system (DBMS), and a database server within a complex system supporting one or more applications.
2. Outline different models for databases and cases where they may be used.
3. Identify and describe common security concerns in databases and database management systems.

Topics

To complete this KU, all Topics and sub-Topics must be completed

1. Outline different types and structures of modern database management systems and their application, such as:
    a. Relational Databases
    b. Hierarchical
    c. No SQL Databases
    d. Object-Based
    e. Object-Oriented
    f. Distributed (Hadoop, Mongo, etc.)
2. Overview of database security models and concerns, such as:
    a. Inference
    b. Aggregation
    c. Injection
    d. Hashing and encryption
    e. Data corruption
    f. Unauthorized access
    g. Database access controls (DAC, MAC, RBAC, Clark-Wilson)

Vocabulary

database, server, client, tables, SQL, query, DBMS

Specializations

Data Management Systems Security
Health Care Security

Related Knowledge Units

Database Management Systems

Data Administration

Original Knowledge Unit

Databases (2014)

Device Forensics (DVF)

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

Outcomes

To complete this KU, students should be able to:

1. Describe methods for the acquisition/analysis of widespread, non-PC devices.
2. Explain the legal issues related to non-PC device forensic activities.

Topics

1. Mobile Device Analysis (e.g. smart phones, tablets)
2. Embedded Systems (e.g. GPS, games consoles, Smart TVs)
3. Internet of Things Devices (e.g. consideration of potential for evidence storage)
4. Must include hands-on activities using devices mentioned above

Specializations

Digital Forensics (Specialization)
Secure Mobile Technology
Security Incident Analysis and Response

Related Knowledge Units

Device Forensics (2014)

Digital Communications (DCO)

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

Outcomes

To complete this KU, students should be able to:

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

Topics

1. Components of a digital communications system
2. Coding schemes
3. Digital Signaling
4. Spread Spectrum Signals
5. Multi-User Communication Access Techniques
    a. CDMA, TDMA, FDMA, SDMA, PDMA

Specializations

Network Security Engineering
Secure Mobile Technology
Secure Telecommunications

Related Knowledge Units

Digital Communications (2014)

Digital Forensics (DFS)

The intent of the Digital Forensics 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.

Outcomes

To complete this KU, students should be able to:

1. Discuss the rules, laws, policies, and procedures that affect digital forensics
2. Use one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.
3. 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

1. Legal Compliance
    a. Applicable Laws
    b. Affidavits
    c. How to Testify
    d. Case Law
    e. Chain of custody
2. Digital Investigations
    a. E-Discovery
    b. Authentication of Evidence
    c. Chain of Custody Procedures
    d. Metadata
    e. Root Cause Analysis
    f. Using Virtual Machines for Analysis

Specializations

Data Security Analysis
Digital Forensics (Specialization)
Network Security Administration (Specialization)
Network Security Engineering
Secure Mobile Technology
Secure Telecommunications
Security Incident Analysis and Response
System Security Administration

Related Knowledge Units

Digital Forensics (2014)

Embedded Systems (EBS)

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

Outcomes

To complete this KU, students should be able to:

1. Discuss embedded system architectures.
2. Compare and contrast the requirements and capabilities of embedded systems.
3. Examine real time issues such as concurrency and synchronization.
4. Apply real time resource management.
5. Trace how a real-time OS handles timing and resource challenges.

Topics

1. Microcontroller/embedded processor architectures
2. PLC's, Gate Arrays, and other common embedded devices
3. I/O, A/D, registers, and embedded hardware capabilities
4. Embedded devices communications
5. Interrupt handling and timing issues
6. Resource management in real time systems
7. Devices without operating systems
8. Real-time Operating Systems
9. Security issues imposed by limited resources
10. Programming languages and environments for embedded systems
    a. Tool chains
    b. Target operating systems and devices
    c. Cross compilers

Specializations

Industrial Control Systems-SCADA Security
Secure Embedded Systems

Related Knowledge Units

Embedded Systems (2014)

Forensic Accounting (FAC)

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

Outcomes

To complete this KU, students should be able to:

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

Topics

1. Investigative Accounting
2. Fraudulent Financial Reporting
3. Misappropriation of Assets
4. Indirect Methods of Reconstructing Income
5. Money Laundering
6. Transnational financial flows
7. Litigation services
8. Evidence Management
9. Economic Damages and Business Valuations

Specializations

Cyber Investigations

Related Knowledge Units

Forensic Accounting (2014)

Formal Methods (FMD)

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

Outcomes

1. Students should be able to apply formal security policy models to real world scenarios.

Topics

1. Concept of Formal Methods
2. Mathematical Logic
3. Applications
    a. Role in system design
    b. Role in software engineering
4. Limitations
5. Bell-LaPadula (as an example formal model)
6. Automated Reasoning Tools
7. System Modeling and Specification
8. Proofs and #

Specializations

Secure Software Development

Related Knowledge Units

Formal Methods (2014)

Fraud Prevention and Management (FPM)

The intent of the Fraud Prevention and Management 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.

Outcomes

To complete this KU, students should be able to:

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

Topics

1. Symptom Recognition
2. Data Driven Detection
3. Investigation of Theft
4. Concealment
5. Conversion Methods
6. Inquiry and Reporting
7. Financial, Revenue and Inventory
8. Liability and inadequate disclosure
9. Consumer fraud

Specializations

Cyber Investigations

Related Knowledge Units

Fraud Prevention and Management (2014)

Hardware Reverse Engineering (HRE)

The intent of the Hardware Reverse Engineering 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.

Outcomes

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

Topics

1. Principles of Reverse Engineering
2. Stimulus, Data Collection, Data Analysis
3. Specification development
4. Capability Enhancement / Modification Techniques
5. Detecting Modification
6. Stimulation Methods / Instrumentation (probing and measurement)
7. JTAG IEEE 1149.1
8. Defining and Enumerating Interfaces
9. Functional Decomposition

Specializations

None

Related Knowledge Units

Hardware Reverse Engineering (2014)

Hardware/Firmware Security (HFS)

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

Outcomes

To complete this KU, students should be able to:

1. Outline physical vulnerabilities of hardware devices.
2. Explain and make use of security capabilities implemented in hardware.
3. Describe how systems are initialized and how software is validated and loaded.
4. Describe the security role of intermediate software such as hardware abstraction layers or other forms of middleware.

Topics

1. Physical Vulnerabilities.
    a. Unused, unsecured communications channels
    b. Test pads and test paths
    c. Back doors, trojans, and hidden circuits
    d. Doping and Induced Faults
    e. Reverse Engineering
    f. Unauthorized memory access
2. Hardware side channel attacks
    a. Timing
    b. Power Analysis
    c. Electromagnetic
    d. RF analysis
    e. Hardware insertion (smartcards, USB, bus devices)
    f. Access through out-of-band management channels
3. Sourcing attacks
    a. Pirated, Fake, and Counterfeit Parts
    b. Supply chain disruption
4. Equipment Destruction Attacks
5. Hardware Security Components
    a. Verifiable device IDs
    b. Random Number Generators
    c. Boot ROM Digital Signatures
    d. Hardware-base encryption modules
    e. Security Co-processors/Controllers
    f. Encryption accelerators (SSL, etc.)
6. Physical Security Attributes
    a. Device validation
    b. Open and Accepted security algorithms
    c. Strong Random Number Generation
    d. Secure time source
    e. Standardized developer interface

   f. Clear documentation
   g. Key backup/Protection
   h. Tamper-resistance
   i. Scalability
7. Bootloader vulnerabilities
   a. Boot sector attacks
   b. Single User Mode
   c. Boot to non-secure OS's
   d. Boot loader reconfiguration
8. Microcode vulnerabilities
9. Firmware vulnerabilities
   a. Reflashing BIOS/PROMs
10. Security role of intermediate layers
   a. Hardware Abstraction Layer
   b. Virtualization Layers

Specializations

Industrial Control Systems-SCADA Security
Secure Embedded Systems
Secure Mobile Technology

Related Knowledge Units

Hardware/Firmware Security (2014)

Host Forensics (HOF)

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

Outcomes

To complete this KU, students should be able to:

1. Describe what can/cannot be retrieved from various Operating Systems,
2. Describe the methodologies used in host forensics.

Topics

More than one operating system should be demonstrated.

1. File Systems and File System Forensics
2. Hypervisor Analysis
3. Cryptanalysis
4. Rainbow Tables
5. Known File Filters (KFF)
6. Steganography
7. File Carving
8. Live System Investigations
9. Timeline Analysis
10. Include samples of hands-on activities

Examples of acceptable operating system specific Topics may include:

1. Registry Analysis, NTFS (Microsoft Windows)
2. Preference List Analysis, HFS+/AFS (Apple MacOS)
3. System configuration Analysis, EXT2/3/4 (Linux, e.g. /etc)

Specializations

Digital Forensics (Specialization)
Security Incident Analysis and Response
System Security Administration

Related Knowledge Units

Host Forensics (2014)

Suggested textbooks

Carrier, B., 2005. File system forensic analysis. Addison-Wesley Professional.

IA Architectures (IAA)

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

Outcomes

To complete this KU, students should be able to:

1. Examine a specific architecture and identify potential vulnerabilities.
2. Design a secure architecture for a given application.

Topics

1. Defense in Depth
2. DMZs
3. Proxy Servers
4. Composition and Security
5. Cascading
6. Emergent Properties
7. Dependencies
8. TCB Subsets
9. Enterprise Architectures / Security Architectures
10. Secure network design

Specializations

Data Security Analysis
Security Incident Analysis and Response
Security Policy Development and Compliance
System Security Administration
Systems Security Engineering

Related Knowledge Units

IA Architectures (2014)

IA Compliance (IAC)

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

Outcomes

To complete this KU, students should be able to:

1. Compare and contrast voluntary and mandatory compliance requirements.
2. Plan and conduct audits to determine compliance with policies, laws, regulations, and other standards.

Topics

1. Relationship between compliance and audit
2. Audit Types
    a. Internal
    b. External
3. Audit Purposes
    a. Compliance to specified requirements, specifications, policy, standards or laws
    b. Regulatory compliance
    c. Assessment of internal controls
4. Audit process
    a. Audit Charter
    b. Audit Baseline
    c. Audit Activities
    d. Audit Reporting,
        i. Results(Findings)
        ii. Recommendations
    e. Response
        i. Mitigation Strategy
5. Compliance Monitoring
    a. Compliance levels
6. Compliance Training

Specializations

Cyber Investigations
Data Management Systems Security
Data Security Analysis
Health Care Security
Security Policy Development and Compliance

Related Knowledge Units

IA Compliance (2014)

IA Standards (IAS)

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

Outcomes

To complete this KU, students should be able to:

1. Compare and contrast different types of standards including: laws, regulations, policies, voluntary, and framework-based standards.
2. Map the processes for the creation and/or changes to different types of standards.
3. Describe the impact of legal/regulatory standards on a given system.
4. Describe how standards may be applied and assessed for a sub-contractor or customer.
5. List and describe key provisions of common standards.

Topics

1. Laws
    a. HIPAA
    b. FERPA
    c. Sarbanes-Oxley
    d. FISMA
    e. Data breach disclosure laws
2. Regulations
3. NIST 800-53
    a. FDA 21 CFR part 820/806
    b. Rainbow Series
4. Commercial Standards
    a. PCI/DSS
5. Open Standards
    a. OWASP

Specializations

Health Care Security
Security Policy Development and Compliance
Systems Security Engineering (Specialization)

Related Knowledge Units

IA Standards (2014)

Suggested academic readings
The Rainbow Serieshttp://uh.edu/tech/cisre/resources/ia-resources/rainbow-series/

Independent/Directed Study/Research (IDR)

The intent of the Independent/Directed Study/Research Knowledge Unit is to provide credit for courses that address emerging issues related to information assurance and cyber defense.

Outcomes

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.)

Related Knowledge Units

Independent/Directed Study/Research (2014)

Industrial Control Systems (ICS)

The intent of the Industrial Control Systems 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.

Outcomes

To complete this KU, students should be able to:

1. Describe the use and application of PLCs in automation.
2. Describe the components and applications of industrial control systems.
3. Explain various control schemes and their differences.
4. Demonstrate the ability to understand, evaluate and implement security functionality across an industrial network.
5. Understand and compare the basics of the most used protocols.

Topics

1. SCADA Firewalls
2. Hardware Components
3. Programmable Logic Controllers (PLCs)
4. Protocols (MODBUS, PROFINET, DNP3, OPC, ICCP, SERIAL)
5. Networking (RS232/485, ZIGBEE, 900MHz, BlueTooth, X.25)
6. Types of ICSs (e.g., power distribution systems, manufacturing)
7. Models of ICS systems (time driven vs. event driven)
8. Common Vulnerabilities in Critical Infrastructure Systems
9. Ladder Logic

Specializations

Industrial Control Systems-SCADA Security

Related Knowledge Units

Industrial Control Systems (2014)

Introduction to Theory of Computation (ITC)

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

Outcomes

To complete this KU, students should be able to:

1. Describe the theory of abstract machines or automata and what can be computed with them.
2. Differentiate the characteristics of computable and non-computable functions.
3. Describe the concept of complexity and quantify the resources required for computation of basic problems.

Topics

1. Automata
2. Turing machines
3. Deterministic and non-deterministic finite automata
4. Formal language theory
5. Computability and non-computability
6. Turing computability
7. Analysis of Algorithms
8. Complexity measures
    a. time and storage
    b. communications
    c. numbers of processors
9. Big O notation
10. Best, worst, and average complexity
11. Upper and lower bounds on complexity
12. Classes of Complexity
    a. P and NP
    b. Intractability

Related Knowledge Units

Introduction to Theory of Computation (2014)

Intrusion Detection/Prevention Systems (IDS)

The intent of the Intrusion Detection/Prevention Systems (IDS) 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.

Outcomes

To complete this KU, students should be able to:

1. Detect, identify, resolve and document host or network intrusions.
2. Use tools and algorithms to detect various types of malware (keyloggers, rootkits) and unauthorized devices (rogue wireless access points) on a live network.
3. Configure IDS/IPS systems to reduce false positives and false negatives.
4. Deploy reactive measures to respond to detected intrusion profiles.

Topics

1. Deep Packet Inspection
2. Log File Analysis
3. Log Aggregation
4. Cross Log Comparison and Analysis
5. Anomaly Detection
    a. Establishing profiles
    b. Anomaly algorithms, such as:
        i. Statistical Techniques
        ii. Correlation Techniques
        iii. Fuzzy Logic Approaches
        iv. Artificial Intelligence
        v. Filtering Algorithms
        vi. Neural Networks
6. Misuse Detection (Signature Detection)
7. Specification-based Detection
8. Host-based Intrusion Detection and Prevention
9. Network-based Intrusion Detection and Prevention
    a. Stealth mode
10. Distributed Intrusion Detection
11. Hierarchical IDS's
12. Honeynets/Honeypots
13. Intrusion response
    a. Device Reconfiguration
    b. Notifications
        i. Logging
        ii. SNMP Trap
        iii. Email
        iv. Visual/Audio Alert
    c. Trace Recording
    d. Opening Application
    e. Session Interruption

f. Reach back

Specializations

Data Security Analysis
Industrial Control Systems-SCADA Security
Network Security Administration (Specialization)
Network Technology and Protocols
Security Incident Analysis and Response
System Security Administration

Related Knowledge Units

Networking Concepts Network Defense
Network Technology and Protocols
Advanced Network Technology and Protocols
Network Security Administration
Wireless Sensor Networks

Original Knowledge Unit

Intrusion Detection/Prevention Systems (2014)

Life-Cycle Security (LCS)

The intent of the Life-Cycle Security 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.

Outcomes

To complete this KU, students should be able to:

1. Describe the importance of secure software, and the programming practices, development processes and methodologies that lead to secure software.
2. List, describe the phases of the system life-cycle, and explain security related concerns at each phase.
3. List and describe the elements of a maturity model.

Topics

1. System Life-Cycle Phases and Issues
    a. Initiation
    b. Requirements
    c. Design
    d. Development
    e. Testing
    f. Deployment
    g. Operations and Maintenance
    h. Disposal
2. Vulnerability Mapping, Management, and Tractability
3. Threat modeling
4. Software Assurance Maturity Model
5. Role of Project/Program Management
6. Role of Process Management
7. Importance of Culture and Training
8. Development Processes and Paradigms
9. Configuration Management
10. Developmental Threats

Specializations

Health Care Security
Network Security Administration (Specialization)
Network Security Engineering
Secure Cloud Computing
Secure Embedded Systems
Secure Mobile Technology
Secure Software Development
Secure Telecommunications
Security Incident Analysis and Response
System Security Administration
Systems Security Engineering (Specialization)

Related Knowledge Units

Software Assurance
Security Risk Analysis
Secure Programming Practices
Software Security Analysis
Vulnerability Analysis
QA/Functional Testing

Original Knowledge Unit

Life-Cycle Security (2014)

Linux System Administration (LSA)

The intent of the Linux System Administration Knowledge Unit is to provide students with skill to perform basic operations involved in system administration of LINUX based systems.

Outcomes

To complete this KU, students should be able to apply the knowledge gained to successfully install and securely configure, operate and maintain a LINUX distro OS, to include:

1. Setting up user accounts
2. Configuring appropriate authentication policies
3. Configuring audit capabilities
4. Performing back-ups and restoring the system from a backup
5. Installing patches and updates
6. Reviewing security logs

Topics

1. OS Installation
2. User accounts management (Access controls, Password Policies, Authentications Methods, Group Policies)
3. Command Line Interfaces
4. Configuration Management
5. Updates and patches
6. Event Logging and Auditing (for performance and security)
7. Managing System Services
8. Virtualization
9. Backup and Restoring Data
10. File System Security
11. Network Configuration (port security)
12. Host (Workstation/Server) Intrusion Detection
13. Security Policy Development

Specializations

Data Management Systems Security
Data Security Analysis
Digital Forensics (Specialization)
Health Care Security
Industrial Control Systems-SCADA Security
Secure Cloud Computing
Security Incident Analysis and Response
Security Policy Development and Compliance
System Security Administration

Related Knowledge Units

System Administration (2014)

Low Level Programming (LLP)

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

Outcomes

To complete this KU, students should be able to:

1. Apply low level programming languages to implement complex programs such as internal operating system components and drivers to interface with and control hardware devices or to achieve other results (speed, size, efficiency, etc.).
2. Explain the risks and rewards that result from using low level programming.

Topics

1. Learn and apply a higher order language which allows low level access, such as C.
2. Learn and program in Assembly
3. Make appropriate and secure use of library functions
4. Correctly use pointers and pointer manipulation
5. Apply modularization in low level programs
6. Practice defensive programming techniques
7. Compile, assemble, and link object files to create working programs.
8. Outline how calls are made in assembly.

Specializations

Secure Embedded Systems
Secure Telecommunications
Systems Security Engineering (Specialization)

Related Knowledge Units

Low Level Programming (2014)

Media Forensics (MEF)

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

Outcomes

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

Topics

1. Drive Acquisition
2. Authentication of Evidence
    a. Verification and Validation
    b. Hashes
3. Metadata
4. Live vs. Static Acquisition
5. Sparse vs. Full Imaging
6. Slack Space
7. Hidden Files/clusters/partitions
8. (must include hands-on activities)

Specializations

Digital Forensics (Specialization)
Security Incident Analysis and Response

Related Knowledge Units

Media Forensics (2014)

Mobile Technologies (MOT)

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

Outcomes

To complete this KU, students should be able to:

1. Outline how mobile systems function to allow secure voice and data access.
2. 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.

Topics

1. 2G -> 3G -> 4G / LTE -> 5G
   a. Standards Heritage
   b. Core Architecture Evolution
2. Design Choices
3. Encryption
4. Mobile Use of SS7
5. RRC Signaling
6. Billing/Charging
7. Mobile Security

Specializations

Network Security Engineering
Secure Mobile Technology
Secure Telecommunications

Related Knowledge Units

Mobile Technologies (2014)

Network Forensics (NWF)

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

Outcomes

To complete this KU, students should be able to:

1. Describe the methodologies used in network forensics.
2. Analyze and decipher network traffic, identify anomalous or malicious activity, and provide a summary of the effects on the system.

Topics

1. Packet Capture and Analysis (Wifi, LAN)
2. Intrusion Detection and Prevention
3. Interlacing of device and network forensics
4. Log-file Analysis
5. Forensic Imaging and Analysis
6. (must include hands-on activities)

Specializations

Data Security Analysis
Digital Forensics (Specialization)
Network Security Administration (Specialization)
Network Security Engineering
Secure Mobile Technology
Secure Telecommunications
Security Incident Analysis and Response

Related Knowledge Units

Network Forensics (2014)

Suggested textbooks

Davidoff, S. and Ham, J., 2012. Network forensics: tracking hackers through cyberspace. Upper Saddle River: Prentice hall.

Network Security Administration (NSA)

The intent of the Network Security Administration Knowledge Unit is to provide students with the knowledge to administer and maintain a comprehensive enterprise security infrastructure.

Outcomes

To complete this KU, students should be able to:

1. Analyze problems, recommend solutions, products, and technologies to meet business objectives.
2. Recommend best security practices to achieve stated business objectives based on risk assumptions.
3. Actively protect information technology assets and infrastructure from external and internal threats.
4. Monitor systems for anomalies, proper updating, and patching.
5. Assist in incident responses for any breaches, intrusions, or theft.
6. Evaluate and perform planning, testing, and implementation of software and hardware deployed.

Topics

1. Coverage of mapping of business objectives to technology objectives and solutions.
2. Broad coverage of different security solutions and product categories and features.
3. Discussion of information security issues and conflicts between potential solutions.
4. Outline of cyber security best practices.
5. Applying network security policies.
6. Describe and explain risk posture, risk appetite.
7. Experience with a variety of network and systems monitoring tools.
8. Issue evaluation, response, and management.
9. Incident identification.
10. Incident response processes and management.
11. Deployment/upgrade processes.
12. User acceptance testing.
13. Blackout plans.
14. Maintenance windows and management.

Specializations

Network Security Administration (Specialization)
Network Security Engineering
Secure Cloud Computing
Secure Telecommunications
System Security Administration

Related Knowledge Units

Networking Concepts
Network Defense
Network Technology and Protocols

Advanced Network Technology and Protocols
Intrusion Detection/Prevention Systems
Wireless Sensor Networks

Original Knowledge Unit

Network Security Administration (2014)

Network Technology and Protocols (NTP)

The intent of the Network Technology and Protocols Knowledge Unit is to expand students' knowledge of networking to include an understanding common network protocols, how network components interact, and how networks evolve over time. The Knowledge Unit will also extend student experiences in using tools to monitor and analyze a network. Students expand their familiarity with network vulnerabilities.

Outcomes

To complete this KU, students should be able to:

1. Demonstrate an understanding of layer 2 networking (Ethernet).
2. Demonstrate an understanding of the structure and use of key networking protocols (IPv4 and IPv6).
3. Identify and describe a variety of common network vulnerabilities.
4. Identify and mitigate security concerns at layer 2 and layer 3 of a network.
5. Demonstrate the use of multiple tools to analyze and troubleshoot a network.
6. Explain the weaknesses of WEP and which weaknesses have been addressed and how.

Topics

To complete this KU, all Topics and sub-Topics must be completed

1. Network Switching (Ethernet)
    a. ARP and RARP
    b. Layer 2 security issues
2. IPv4 suite
    a. IPv4 Addressing
3. IPv6 suite
    a. IPv6 Addressing
4. Routing in IPv4 and v6.
    a. Routing tables and metrics
    b. Layer 3 security issues
    c. IPsec
5. Network naming
    a. DNS
    b. NetBIOS
6. Network Analysis/Troubleshooting
    a. Netflow

Specializations

Digital Forensics (Specialization)
Industrial Control Systems-SCADA Security
Network Security Administration (Specialization)
Network Security Engineering
Secure Cloud Computing
Secure Embedded Systems
Secure Mobile Technology

Secure Telecommunications
Security Incident Analysis and Response
System Security Administration
Systems Security Engineering (Specialization)

Related Knowledge Units

Networking Concepts
Network Defense
Advanced Network Technology and Protocols
Network Security Administration
Intrusion Detection/Prevention Systems
Wireless Sensor Networks

Original Knowledge Unit

Network Technology and Protocols (2014)

Suggested Textbooks

Fundamentals of Information Systems Security - ISBN-10: 128411645X

Operating Systems Hardening (OSH)

The intent of the Operating Systems Hardening 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.

Outcomes

To complete this KU, students should be able to:

1. Describe, for a given OS, the steps necessary for hardening the OS with respect to various applications.
2. 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

1. Secure Installation
2. Removing unnecessary components
3. File system maintenance (isolation of sensitive data)
4. User restrictions (access and authorizations)
5. User/Group/File Management
6. Password Standards and Requirements
7. Shutting Down Unnecessary/Unneeded Services
8. Closing Unnecessary/Unneeded Ports
9. Patch Management/Software Updates
10. Virtualization
11. Vulnerability Scanning

Specializations

Secure Cloud Computing
Secure Embedded Systems
Security Incident Analysis and Response
Security Policy Development and Compliance
System Security Administration
Systems Security Engineering (Specialization)

Related Knowledge Units

Operating Systems Hardening (2014)

Operating Systems Theory (OST)

The intent of the Operating Systems Theory 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.

Outcomes

1. Students should 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

1. Privilege States
2. Processes & Threads, Process/Thread Management
3. Memory Management, Virtual Memory
4. Inter-process Communications
5. Concurrency and Synchronization, Deadlocks
6. File Systems
7. Input / Output
8. Real-time operating systems/security issues
9. Distributed OS architectures & security issues
10. Race Conditions
11. Buffer Overflows
12. Virtualization
13. Clear Interface Semantics

Specializations

Digital Forensics (Specialization)
Secure Software Development

Related Knowledge Units

Operating Systems Theory (2014)

Suggested Textbooks

Operating System Concepts Essentials 2nd Ed, Author: SILBERSCHATZ
Wiley: ISBN-13: 978-1-118-80492-6

Penetration Testing (PTT)

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

Outcomes

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

Topics

1. Flaw Hypothesis Methodology
2. Other methodologies (e.g., OSSTMM)
3. Identifying flaws from documentation
4. Identifying flaws from source code analysis
5. Vulnerability Scanning
6. Understanding families of attacks
7. Understanding flaws that lead to vulnerabilities
8. Enumeration, foot printing
9. Attack Surface Discovery
10. Attack Vectors

Specializations

Network Security Administration (Specialization)
Network Security Engineering

Related Knowledge Units

Penetration Testing (2014)

Privacy (PRI)

The intent of the Privacy Knowledge Unit is to provide students with a understanding of privacy issues, tools, and practices.

Outcomes

To complete this KU, students should be able to:

1. Examine concepts of privacy.
2. Explore the effects the Internet has on privacy
3. Describe approaches individuals, organizations, and governments have taken to protect privacy.
4. Compare and contrast privacy policies and laws of different jurisdictions.

Topics

1. Personally Identifiable Information
2. Fair Information Practice Principles (FIPPs)
    a. Transparency
    b. Individual Participation
    c. Purpose Specification
    d. Data Minimization
    e. Use Limitation
    f. Data Quality and Integrity
    g. Security
    h. Accountability and Auditing
3. Privacy Impact Assessments
4. Anonymity and Pseudonymity
5. Privacy Policies, Laws and Regulations
6. Risks to Privacy
7. Tracking and Surveillance
8. Privacy tools
    a. Encryption
    b. VPNs
    c. Scramblers
9. Privacy Laws and legal basis

Specializations

Cyber Investigations
Security Policy Development and Compliance

QA/Functional Testing (QAT)

The intent of the QA/Functional Testing Knowledge Unit is to provide students with methods to assess how well a functional unit meets a requirement.

Outcomes

To complete this KU, students should be able to:

1. Develop effective tests in a structured, organized manner.
2. Perform security functional testing to demonstrate that security policies and mechanisms are completely and correctly implemented.

Topics

1. Testing methodologies (white, grey, black box testing)
2. Test coverage analysis
3. Automatic and manual generation of test inputs
4. Test execution
5. Validation of results

Specializations

Secure Embedded Systems
Secure Software Development
Systems Security Engineering (Specialization)

Related Knowledge Units

QA/Functional Testing (2014)

Radio Frequency Principles (RFP)

The intent of Radio Frequency (RF) Principles Knowledge Unit is to provide students with a basic understanding of radio frequency communications.

Outcomes

To complete this KU, students should be able to:

1. Identify methods for isolating RF emissions
2. Identify techniques for obfuscating RF transmissions
3. Discuss the tradeoffs associated with bandwidth data rate, modulation, complexity, acceptable BER, and signal spreading

Topics

1. Basics of electromagnetic radiation
2. Antennas
3. Information Modulation
4. Digital Modulation
5. Spectral representation
6. Bandwidth
7. BER
8. Eb/No vs. S/N
9. Limiting Access in RF
10. Propagation Principles

Specializations

Secure Mobile Technology
Secure Telecommunications

Related Knowledge Units

RF Principles (2014)

Secure Programming Practices (SPP)

The intent of the Secure Programming Practices 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.

Outcomes

To complete this KU, students should be able to:

1. Produce software components that satisfy their functional requirements without introducing vulnerabilities
2. Describe the characteristics of secure programming.
3. Understand the vulnerabilities inherent in different programming languages.
4. Examine vulnerabilities introduced through the use of libraries and how to mitigate those vulnerabilities.

Topics

1. Interpretation and realization of Security Requirements
2. Principles of Secure Programming
3. Robust Programming
4. Defensive Programming
    a. Input Validation, Type checking
    b. Cover all cases - use defaults to handle cases not explicitly covered
    c. Catch and handle exceptions at the lowest level possible
    d. Avoidance of risky coding constructs
    e. Avoid information leakage through error messages
    f. Apply security practices to classes
        i. Do not allow data changes by reference in external interfaces
        ii. Use the context to determine data access
        iii. Support verification in data updates
        iv. Authenticate when possible
5. Programming Flaws
    a. Buffer Overflows, Integer Errors
6. Static Analysis
7. Data Obfuscation
8. Data Protection
9. Secure Programming paradigms
    a. Pair programming
    b. Code reviews
    c. Test-driven development

Specializations

Secure Embedded Systems
Secure Mobile Technology
Secure Software Development

Related Knowledge Units

Life-Cycle Security
Software Assurance Security
Risk Analysis
Software Security Analysis
Vulnerability Analysis
QA/Functional Testing

Original Knowledge Unit

Secure Programming Practices (2014)

Software Assurance (SAS)

The intent of the Software Assurance 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.

Outcomes

To complete this KU, students should be able to:

1. Apply security design principles.
2. Describe how system design and architecture affects security.
3. Create a system design optimized to meet appropriate security requirements.
4. Apply modeling and vulnerability assessment to create a secure design.
5. Explain the importance of Design Reviews in creating secure systems.

Topics

1. Describe examples of the application of Security Principles:
    a. Separation (of domains)
    b. Isolation
    c. Encapsulation
    d. Least Privilege
    e. Simplicity (of design)
    f. Minimization (of implementation)
    g. Fail Safe Defaults / Fail Secure
    h. Modularity
    i. Layering
    j. Least Astonishment
    k. Open Design
    l. Usability
    m. Reduce attack surfaces
2. Compare and contrast the security of alternative designs
3. Review Secure Design Patterns
4. Evaluate the level of security required for system data.
5. Apply Life of Data - N-order Scope Map
6. Create an Audit Trail
7. Apply modeling techniques and vulnerability mapping to evaluate potential security issues.
8. Increase Resiliency
9. Design reviews

Specializations

Secure Software Development

Related Knowledge Units

Life-Cycle Security

Security Risk Analysis
Secure Programming Practices
Software Security Analysis
Vulnerability Analysis
QA/Functional Testing

Original Knowledge Unit

Software Assurance (2014)

Software Reverse Engineering (SRE)

The intent of the Software Reverse Engineering Knowledge Unit is to provide students with the capability to perform reverse engineering of executable code to determine its function and effects, or to discover details of the implementation.

Outcomes

1. Students should be able to use common software reverse engineering tools to safely perform static and dynamic analysis of software (or malware) of unknown origin for the purposes of understanding the software functionality and implementation.

Topics

1. Malware Analysis
2. Reverse Engineering Tools & Techniques
3. Sandboxing
4. Anti-reverse engineering techniques

Specializations

None

Related Knowledge Units

Software Reverse Engineering (2014)

Suggested textbooks

Practical Malware Analysis

Software Security Analysis (SSA)

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

Outcomes

To complete this KU, students should be able to:

1. Describe software security analysis tools and techniques.
2. Apply their knowledge to perform software security analysis, using common tools, against previously unknown software components.

Topics

1. Testing Methodologies
2. Source and Binary Code Analysis
3. Static and Dynamic Analysis Techniques
4. Sandboxing
5. Common analysis tools and methods

Specializations

Health Care Security
Secure Software Development

Related Knowledge Units

Software Security Analysis (2014)

Supply Chain Security (SCS)

The intent of the Supply Chain Security 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.

Outcomes

To complete this KU, students should be able to:

1. Describe the issues related to outsourcing hardware and/or software development and/or integration.
2. Describe methods to mitigate these issues, and the limitations of these methods.

Topics

1. Global Development
2. Off Shore Production
3. Transport and Logistics of IT Components
4. Evaluation of 3rd Party Development Practices
5. Understanding of the Capabilities and Limits of Software and Hardware Reverse Engineering

Specializations

Health Care Security
Secure Cloud Computing
Secure Mobile Technology
Security Policy Development and Compliance
System Security Administration
Systems Security Engineering (Specialization)

Related Knowledge Units

Supply Chain Security (2014)

Systems Certification and Accreditation (SCA)

The intent of the Systems Certification and Accreditation 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.

Outcomes

To complete this KU, students should be able to:

1. Describe the DoD system certification and accreditation processes.
2. Define certification and accreditation.

Topics

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

Specializations

Security Policy Development and Compliance
System Security Administration

Related Knowledge Units

Systems Certification and Accreditation (2014)

Systems Programming (SPG)

The intent of the Systems Programming 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, performance constrained, or within the deepest level of an operating system), typically in the C or assembly programming language which is designed to provide services to other software.

Outcomes

To complete this KU, students should be able to:

1. Develop programs which directly account for hardware and resource constraints of the specific systems on which they operate.
2. Outline and apply a layered approach to providing and accessing services using API's.
3. Implement new functions in an OS kernel or complex and sophisticated programs, such as a device driver, that can be embedded into an OS kernel.
4. Write programs that implement systems functions such as a network communications stack, a telnet client, or a basic file manager without the use of external libraries.

Topics

1. Hardware/software interfaces and interactions
2. Different types of systems programs
    a. Development environments
    b. Operating Systems
    c. Utilities
    d. Networking Functions
    e. Device Drivers
    f. Storage Frameworks
    g. Gaming engines
3. Layered services design
4. Providing and using Application Programming Interfaces (API's)
5. Programming to operating systems internal interfaces
6. Low level programming languages (C, Assembly, etc.)
7. Resource optimization
8. Resource management
9. Run time overhead minimization
10. Programming direct control of memory access and flow control
11. Managing memory in systems software
12. Security concerns in systems software
13. Monitoring and logging systems software

Specializations

Secure Mobile Technology
Secure Software Development
Systems Security Engineering (Specialization)

Related Knowledge Units

Systems Programming (2014)

Systems Security Engineering (SSE)

The intent of the Systems Security Engineering 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.

Outcomes

To complete this KU, students should be able to:

1. Analyze system components and determine how they will interact in a composed system.
2. Analyze a system design and determine if the design will meet the system security requirements.

Topics

1. Design of testing
2. Testing methodologies
3. Emergent Properties
4. Systems Engineering
5. System Integration
6. Make or Buy Analysis
7. Systems Security Analysis
8. Enterprise system components

Specializations

Data Security Analysis
Industrial Control Systems-SCADA Security
Secure Embedded Systems
Secure Software Development
Secure Telecommunications
System Security Administration
Systems Security Engineering (Specialization)

Related Knowledge Units

Systems Security Engineering (2014)

Virtualization Technologies (VTT)

The intent of the Virtualization Technologies 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.

Outcomes

To complete this KU, students should be able to:

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

Topics

1. Virtualization Architectures
2. Virtualization techniques for code execution
3. Memory management in virtual environments
4. Networking in virtual environments
5. Storage in virtual environments
6. Scheduling of virtual machines
7. Migration and snapshots
8. Virtual management layers
9. Digital Forensics in virtual environments

Specializations

Secure Cloud Computing
Systems Security Engineering (Specialization)

Related Knowledge Units

Virtualization Technologies (2014)

Vulnerability Analysis (VLA)

The intent of the Vulnerability Analysis 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.

Outcomes

To complete this KU, students should be able to:

1. Apply tools and techniques for identifying vulnerabilities.
2. Create and apply a vulnerability map of a system.
3. Apply techniques to trace a vulnerability to its root cause.
4. Propose and analyze countermeasures to mitigate vulnerabilities.
5. Explain the circumstances under which a vulnerability must be disclosed.

Topics

1. Definition of "vulnerability"
2. System modeling techniques
3. Vulnerability mapping.
4. Vulnerability characteristics and classification.
5. Taxonomy
    a. Buffer overflows, privilege escalation, rootkits
    b. Trojans/backdoors/viruses
    c. Return oriented programming
    d. Social Engineering Vulnerabilities
    e. Administrative Privileges and their effect on vulnerabilities
6. Root causes of vulnerabilities
7. Mitigation strategies
8. Analyze the expected and actual effectiveness of proposed countermeasures.
9. Explain when vulnerabilities must be disclosed.
10. Tools and techniques for identifying vulnerabilities

Specializations

Digital Forensics (Specialization)
Industrial Control Systems-SCADA Security
Network Security Administration (Specialization)
Network Security Engineering
Secure Cloud Computing
Secure Software Development
Security Incident Analysis and Response
System Security Administration

Related Knowledge Units

Life-Cycle Security
Software Assurance
Security Risk Analysis
Secure Programming Practices
Software Security Analysis
QA/Functional Testing

Original Knowledge Unit

Vulnerability Analysis (2014)

Web Application Security (WAS)

The intent of the Web Application Security Knowledge Unit is to provide students with an understanding of technology, tools, and practices associated with web applications.

Outcomes

To complete this KU, students should be able to:

1. Examine concepts of web application technologies and security issues associated with them.
2. Describe approaches used in the development and deployment of secure web applications
3. Explain how web applications are operated in a secure manner.

Topics

1. Web Application Technologies
    a. HTTP Protocol
    b. Encoding Schemes
    c. Web Application architectures
    d. AJAX
    e. XML and JSON
2. Server-Side Controls
3. Authentication
4. Session Management
5. Access Controls
6. Client-Side Controls
7. Input-Based Vulnerabilities
    a. SQL Injection
    b. Blind SQL Injection
    c. Cross-Site Scripting
    d. Cross-site request forgery
8. Function-Specific Input Vulnerabilities
9. Attacking Application Logic
10. Recent Attack Trends
11. Shared Hosting Vulnerabilities
12. Application Server Vulnerabilities

Specializations

Secure Software Development
Security Policy Development and Compliance

Windows System Administration (WSA)

The intent of the Windows System Administration Knowledge Unit is to provide students with skill to perform basic operations involved in system administration of Microsoft Windows based systems.

Outcomes

To complete this KU, students should be able to:

1. Set up user accounts.
2. Configure appropriate authentication policies.
3. Configure audit capabilities.
4. Perform back-ups.
5. Install patches and updates.
6. Review security logs, and restore the system from a backup.

Topics

1. OS Installation
2. User accounts management (Access controls, Password Policies, Authentications Methods, Group Policies)
3. Command Line Interfaces
4. Configuration Management
5. Updates and patches
6. Event Logging and Auditing (for performance and security)
7. Managing System Services
8. Virtualization
9. Backup and Restoring Data
10. File System Security
11. Network Configuration (port security)
12. Host (Workstation/Server) Intrusion Detection
13. Security Policy Development

Specializations

Data Management Systems Security
Digital Forensics (Specialization)
Health Care Security
Industrial Control Systems-SCADA Security
Secure Cloud Computing
Security Incident Analysis and Response
Security Policy Development and Compliance
System Security Administration

Related Knowledge Units

System Administration (2014)

Suggested textbooks

Installing and Configuring Windows Server 2012 R2 with MOAC Labs by Craig Zacker

Wireless Sensor Networks (WSN)

The intent of the Wireless Sensor Networks (WSN) Knowledge Unit is to provide students with a basic understanding of wireless sensor networks and the security issues associated with them.

Outcomes

To complete this KU, students should be able to:

1. Diagram and deploy a wireless sensor network.
2. Describe the challenges associated with wireless sensor networks, including coordination, energy efficiency, and self-organization.
3. Propose and analyze appropriate security measures for wireless sensor networks.

Topics

1. Managed vs. Ad-hoc network participation
2. Cross Layer Optimization
3. Network Architecture
    a. Mesh
    b. Structured
    c. Hierarchical
4. MAC approaches
    a. Coordination
    b. Self-organization
5. Routing Protocols
6. Membership Management
    a. Authentication Hash Tables
7. Security Issues
    a. Data Integrity
    b. Data Poisoning
    c. Resource Starvation
8. Encryption.
9. Energy Efficiency
    a. Power budget
    b. Energy Optimization
    c. Energy Harvesting
10. Radio Frequencies
    a. RF selection and management
    b. Interference

Specializations

Secure Mobile Technology

Related Knowledge Units

Networking Concepts
Network Defense

Network Technology and Protocols
Advanced Network Technology and Protocols
Network Security Administration

Original Knowledge Unit

Wireless Sensor Networks (2014)