National Centers of Academic Excellence in Cybersecurity (NCAE-C) – Cyber Defense (CAE-CD) Knowledge Units (KUs)

Contributors:
Annie Becker***, National Security Agency (NSA)
Zachary Blum, National Security Agency (NSA)
Kelli Burgin, Montreat College - CAE-CD
Anna Carlin, Fullerton College - CAE-CD
Bill Chu, UNC Charlotte - CAE-CD, CAE-R
Deanne Cranford-Wesley, North Carolina Central University - CAE-CD
Susan Frank, Suffolk County Community College - CAE-CD
Tirthankar Ghosh, University of New Haven - CAE-CO
Seth Hamman**, Cedarville University - CAE-CO
Randall Joyce, Murray State University - CAE-CD
Scott Keller, National Security Agency (NSA)
Anne Kohnke*, University of Detroit Mercy - CAE-CD
Yair Levy*, Nova Southeastern University - CAE-CD, CAE-R
Xiuwen Liu, Florida State University - CAE-CD, CAE-R
Theodore Manikas, Southern Methodist University – CAE-CD
Sean McBride, Idaho State University – CAE-CD
Stanley Mierzwa, Kean University - CAE-CD
Stephen Miller, CAE Peer Review National Center (CNC) & NCyTE - CAE-CD
Matthew Nagaishi, National Security Agency (NSA)
Michael Nowatkowski, Augusta University - CAE-CD
Anthony Pinto, University of West Florida - CAE-CD
Stu Steiner, Eastern Washington University - CAE-CD
Blair Taylor, Towson University - CAE-CD, CAE-CO
Michael Tu, Purdue University Northwest - CAE-CD
Renae Weathers***, National Security Agency (NSA)
Tobi West, Coastline College - CAE-CD
Gianluca Zanella, Augusta University – CAE-CD

*** - CAE PMO Lead
** - CAE KUs Lead
* - CAE-CD KUs WG Co-Chairs

20241209_2024_CAE-CD_KUs_Ver2024.06

This publication was partially supported by CAE Community at the California State University, San Bernardino (CSUSB), under National Security Agency (NSA) award number H98230-22-1-0316

Knowledge Units (KUs) Criterion Description

The Knowledge Units (KUs) criterion is the cornerstone of the Cyber Defense (CD)'s Program of Study (PoS) Validation. More than any other PoS Validation criteria, it provides the scope and rigor for the PoS curriculum and its targeted work roles as per the Department of Defense Cyber Workforce Framework (DCWF) (https://dodcio.defense.gov/Cyber-Workforce/DCWF/) or the NICE Framework (https://niccs.cisa.gov/workforce-development/nice-framework). The KUs, as a whole, are designed to produce graduates who meet the requirements set forth by the NCAE-C Community. The selection of a subset of KUs targets specific work roles identified by the academic institution for their Validated PoS. The NCAE-C program relies upon institutional accreditation for the sufficiency of program construction and maintenance. Courses, or other academic elements, should be institutionally approved per the institutional requirements for accreditation and aligned to the KUs. The PoS content as demonstrated by KU alignment is used to determine if the courses together as a whole constitute sufficient material in quantity and form. All CAE-CD programs need to cover the foundational, appropriate core (technical or non-technical), and required number of optional KUs per academic program type (Associate, Bachelors, Maters, or Doctoral) as indicated in the CAE-CD Requirements Document (see via: https://public.cyber.mil/ncae-c/documents-library/).

CAE-CD KUs Overview and Structure:

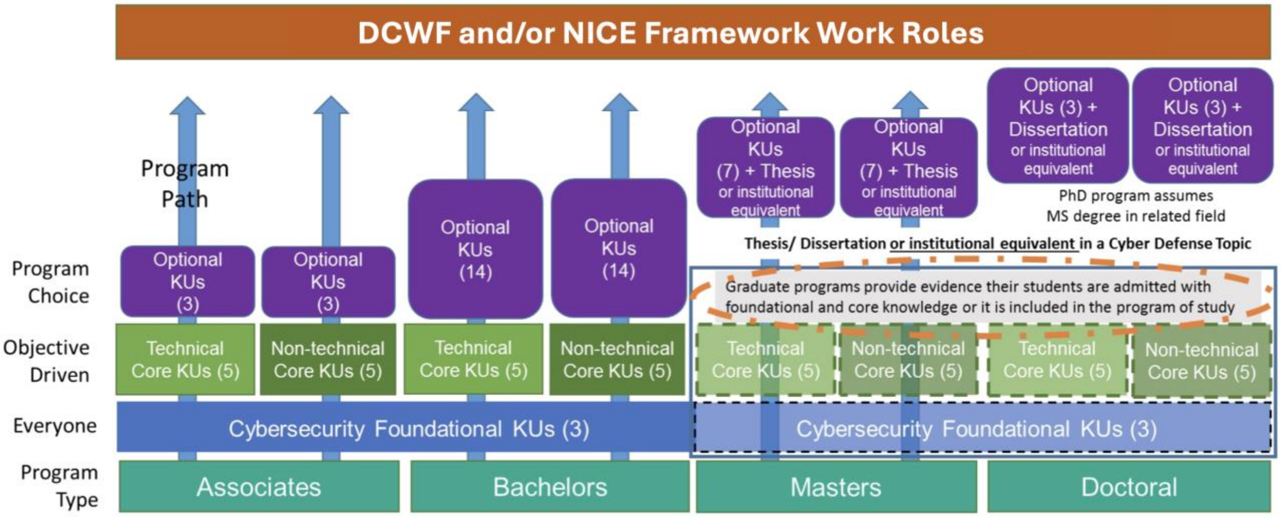
DCWF and/or NICE Framework Work Roles
Program Path
Program Choice
Objective Driven
Everyone
Program Type
Optional KUs (3)
Optional KUs (3)
Optional KUs (14)
Optional KUs (14)
Optional KUs (7) + Thesis or institutional equivalent
Optional KUs (7) + Thesis or institutional equivalent
Optional KUs (3) + 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

Figure 1. CAE-CD Knowledge Units Alignment Requirements Overview

(3 KUs) Foundational (all required): IT Systems Components (ISC), Cybersecurity Fundamentals (CSF), and Cybersecurity Principles (CSP)

(5 KUs) Core: KUs are required of all PoS. Individual programs choose to align to Technical or Non-Technical Core KUs depending on the nature of their PoS. Certificate, Associate, and Bachelor degree programs are required to align courses in the PoS to either the Technical or Non-Technical KUs. Graduate programs may either align to these KUs or may provide detailed documentation on how the institution verifies that students have met these KUs. For example, the institution may document a system in place that allows for checking of prior courses and/or other experiences of entering graduate students to demonstrate the Foundational and Core KUs or require them to take courses and/or other experiences to achieve the Foundational and/or Core KUs lacking before entering or during the program.

The five technical **core** KUs are:

- Basic Scripting and Programming (BSP)
- Basic Networking (BNW)
- Network Defense (NDF)
- Basic Cryptography (BCY)
- Operating Systems Concepts (OSC)

The five non-technical **core** KUs are:

- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Program Management (SPM)
- Security Risk Analysis (SRA)
- Cybersecurity Planning and Management (CPM)

Optional KUs (60 total): The required subset of additional KUs 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 maybe used as optional KUs.).

Aligning Courses to KUs

Every KU contains learning outcomes and topics. KU Outcomes will be shown (as a set) to provide guidance on the coverage for the course learning outcomes. The majority of the KU topics must be addressed in the aligned courses. KU topics are deliberately broad so schools can apply their discretion and subject matter expertise. More specific guidance is available upon request. There are no fixed requirements for the number of credit hours or semester weeks needed to cover a KU, but the KU learning outcomes help to define the appropriate depth of coverage. The KU Description provides further guidance but does not define strict requirements. While it is not required that every learning outcome be explicitly assessed as written, applicant schools should be able to defend their coverage of the learning outcomes. A KU should not be aligned to elective or optional course(s), as all students are required to take all courses indicated in the KU alignment documentation. A KU may be covered by one or more courses, however, a course should not be aligned to an excessive number of KUs given the challenge of so many KU Outcomes coverage with a single course. Programs should not align multiple courses to a KU purely to show the strength of coverage--there is no such thing as 110% coverage; either a KU is covered or it is not. When multiple courses are aligned to a KU, it is assumed that all of them partially cover the KU and that together they fully cover the KU. If there are multiple courses that cover a KU, then schools should align only the minimal set or the single course with the primary coverage. However, four or more courses aligned to a single KU may be more of an indication of week KU coverage than strength because it risks diluting the KU. Furthermore, a single course can fully and partially cover more than one KU (aside from graduate Optional KUs aligned to thesis course(s) or a capstone project course).

Hands-on Activities

Cyber Defense may combine theoretical knowledge with applied competencies. Students learn the knowledge and skills needed in order to competently perform the work role(s) tasks assigned to the validated PoS. Therefore, a considerable volume of hands-on labs and other competency-building assignments are needed for cyber defense programs. It is expected that students graduating from a CAE-CD-validated PoS will have the knowledge associated with the aligned work roles for that PoS and be able to perform most, if not all, tasks associated with the selected work role(s) from either the DCWF and/or NICE Framework.

Graduate Programs

Graduate programs may align KUs to prerequisite courses that are required for admittance into the program but are not taught in the graduate PoS itself. For additional details about KU alignment and program level specifics, please see Section 1e of the CAE-CD Requirements Document via: https://public.cyber.mil/ncae-c/documents-library/.

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. Example: The intent of this knowledge unit is to provide students with a [basic/intermediate/advanced] awareness, knowledge, skills of [details].

Outcomes: A description of student-based outcomes associated with the knowledge unit. To the highest degree possible, use of the Bloom's Taxonomy verbs (https://ccecc.acm.org/assessment/blooms) and Bloom's Computing verbs (https://ccecc.acm.org/assessment/blooms-for-computing) for KU outcomes are applied.

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. To complete each KU, an alignment to a minimum of 75% of the topics and sub-topics is required. The format of the KU 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 that clearly define elements within the KU.

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

Most Related DCWF and/or NICE Framework Work Role(s): A connection to DCWF and/or the NICE Framework at the work role(s) level (DCWF: https://dodcio.defense.gov/Cyber-Workforce/DCWF/; NICE Framework: https://niccs.cisa.gov/workforce-development/nice-framework). List of the top five most relevant DCWF and/or NICE Framework Work Role(s) related to this KU.

The 2024 CAE Cyber Defense (CAE-CD) Knowledge Units

CAE-CD Foundational Knowledge Units

Cybersecurity Fundamentals (CSF)
Cybersecurity Principles (CSP)
IT Systems Components (ISC)

The foundational knowledge units are required of all programs seeking CAE-CD PoS Validation. For associate and baccalaureate programs, the foundational knowledge units will be aligned as part of the PoS Validation process. For Graduate level programs, the institution will need to define how they meet the foundational knowledge when it is considered a prerequisite to the graduate program.

Foundational - Cybersecurity Fundamentals (CSF)

The intent of the Cybersecurity Fundamentals (CSF) Knowledge Unit is to provide students with a basic understanding of the fundamental concepts and vocabulary within the vast cybersecurity discipline. Students must be able to describe the current cybersecurity threat landscape, including the various motivations, objectives, and threats. This KU reinforces adversarial thinking and the need for cybersecurity. Students must also be able to describe the goals of cybersecurity, how risk management informs the approach to cybersecurity, and the principles and best practices of cybersecurity.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Define the fundamental principles of cybersecurity.
2. Describe the goals of cybersecurity.
3. Describe potential objectives of cyber attackers and their motivations.
4. Describe various types of cyber attacks.
5. Describe various common vulnerability types and evaluate their severity.
6. Describe common mechanisms used to protect against cyber attacks.
7. Describe cyber defense tools, methods and components.
8. Apply cyber defense methods to prepare a system to repel attacks and provide system security.
9. Describe appropriate measures to be taken should a system compromise occur.
10. Discuss current events in cybersecurity.

Topics

1. Cybersecurity principles
2. Threats and Adversaries (threat actors, malware, natural phenomena, and human factors)
3. Vulnerability Management
4. Basic Risk Management and Assessment (Risk, Threats, Vulnerabilities, Risk Mitigation, Residual Risk, Risk Acceptance, Risk Transference, Risk Appetite)
5. The Cybersecurity/McCumber Cube (Confidentiality, Integrity, and Availability (CIA) Triad, Information States, Security Controls)
6. Cyber Kill Chain, MITRE ATT&CK, and ATLAS Frameworks
7. Attack methods for different vulnerability types`
8. Security Life-Cycle
9. Applications of Cryptography and PKI
10. Data Security (e.g., in transmission, at rest, in processing)
11. Security Models (e.g., Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
12. Access Control Models (e.g., MAC, DAC, RBAC, Lattice)
13. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
14. Malware
15. Session Management

16. Exception Management
17. Security Mechanisms (e.g., Identification/Authentication, Audit)
18. Authentication, authorization, and accounting (AAA) and access control
19. Malicious activity detection/forms of attack
20. Security Governance, Policies, Controls and Appropriate Countermeasures (include Disaster Recover, Business Continuity, and Incident Response Policies and concepts)
21. Key Legal issues associated with cybersecurity and privacy (HIPAA, HITECH, SOX, FERPA, GLBA, COPPA, FISMA, GDPR, court rulings on-going)
22. Ethics (e.g., ethics associated with cybersecurity profession)
23. Cybersecurity best practices
24. Current events in cybersecurity
25. Cybersecurity awareness

Vocabulary

Advanced Persistent Threat (APT); Cybersecurity Fundamentals; Threat Landscape; Adversarial Thinking; Risk Management; Cybersecurity Principles; Cyber Attacks; Vulnerabilities; Cyber Defense; Access Control; Confidentiality, Integrity, Availability (CIA); Security Models; Legal Issues in Cybersecurity

Related Knowledge Units:

Cybersecurity Principles (CSP); IT Systems Components (ISC); Policy, Legal, Ethics, and Compliance (PLE)

Most Related DCWF and/or NICE Framework Work Role(s)

Defensive Cybersecurity; Cybersecurity Policy and Planning; Cybersecurity Instruction; Infrastructure Support; Insider Threat Analysis

Foundational- Cybersecurity Principles (CSP)

The purpose of the Cybersecurity Principles (CSP) Knowledge Unit is to equip students with basic security design fundamentals that enable them to build systems that can be trusted.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Differentiate and discuss 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 and apply 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 (e.g., CIA Triad, risks, threats, vulnerabilities, assets, security controls, security event detection, governance)
2. Principles of system and software design
3. Separation of domains and duties
4. Adequate Security
5. Isolation (e.g., Compartmentalize/Segmentation)
6. Encapsulation (e.g., Data protection in Object Oriented Programming)
7. Modularity
8. Organizational and system resilience (e.g., Hardened)
9. Security by design.
10. Accountability.
11. Simplicity of design (e.g., Economy of Mechanism)
12. Minimization of implementation (e.g., Least Common Mechanism)
13. Open Design
14. Complete Mediation
15. Layering (e.g., Defense in depth)
16. Least Privilege
17. Leverage Existing Components
18. Fail Safe Defaults/Fail Secure
19. Least Astonishment (e.g., Psychological Acceptability)
20. Minimize Trust Surface (e.g., Reluctance to trust, Zero Trust)
21. Usability and Management
22. Trust relationships
23. Ethics in Cybersecurity

Vocabulary
Asset; CIA Triad; Encapsulation; Governance; Isolation; Modularity; Open Systems Interconnect (OSI) and Transmission Control Protocol/Internet Protocol (TCP/ IP) Models (Segments, Packets, Frames); Risk Appetite, risk management; Security Control; Security Event Detection; Separation of Duties; Secure System, Threat, Trust, Trusted System, Trustworthy, Vulnerability

Related Knowledge Units:
Cybersecurity Fundamentals (CSF); Basic Networking (BNW); Basic Scripting and Programming (BSP); Cybersecurity Ethics (CSE); Basic Cyber Operations (BCO)

Most Related DCWF and/or NICE Framework Work Role(s)
Communications Security (COMSEC) Management; Executive Cybersecurity Leadership; Systems Security Management; Secure Software Development; Insider Threat Analysis

Foundational - IT Systems Components (ISC)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Differentiate and diagram the various hardware components of modern computing environments and their individual functions.
2. Characterize the networks that interconnect computing components.
3. Describe the various IT activities and roles involved in managing computing systems.
4. Understand system and software architectures.
5. Understand basic security issues in modern computing environments.
6. Describe how software is managed within an organization.
7. Properly apply the vocabulary associated with cybersecurity.

Topics

1. Endpoint protection (e.g., Workstations, laptops, tablets, servers, appliances, mobile devices, peripheral devices (Printers, scanners, external storage), wearable devices)
2. Storage Devices (e.g., external storage drives, filesystems, shared file servers, databases)
3. System Architectures (e.g., enterprise, cloud, SaaS/PaaS/IaaS, etc.) and enabling technologies (e.g., containers, virtualization)
4. Managed services alternative environments (e.g., Supervisory Control and Data Acquisition (SCADA), real-time systems, critical infrastructures)
5. Configuration Management
6. Networks (Internet, LANs, wireless, WANs, CANs, Internet of Things, Automotive, and Smart cities)
7. Networking Equipment (e.g., routers, switches, firewalls, and network cables)
8. Network mapping (identification and enumeration of network components)
9. Network Security Components (Data Loss Prevention, VPNs, Firewalls, monitors, intrusion detection systems)
10. Intrusion Detection and Prevention Systems, Incident Response
11. Managed Services
12. IT Management and Monitoring (e.g., system monitoring tools, configuration management tools, and backup/recovery tools)
13. Software (e.g., operating systems, applications, and virtualization software)
14. Software Security (secure coding principles, software issues by type)
15. Configuration Management
16. System and application software updates patching (e.g., patch management)
17. Vulnerability Scanning (e.g., Vulnerability Windows, zero-day to patch availability)
18. Physical and environmental security concerns
19. Internet of Things (IoT)
20. Cyber Defense Partnerships (e.g., Federal, State, Local, Industry)

21. IT organizational structure

Vocabulary

Bring Your Own Device (BYOD); Configuration Management; Endpoint Protection; Infrastructure-as-a-Service (IaaS); IT Management and Monitoring; Networks; Networking Equipment; Network Security Components; Network Attached Storage (NAS); Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS); Software Security; Storage Area Network (SAN); Storage Devices; System Architectures; Universal Serial Bus (USB); Zero-day vulnerability; Zero-day exploits; Zero-day attacks

Related Knowledge Units

Cybersecurity Fundamentals (CSF); Basic Networking (BNW)

Most Related DCWF and/or NICE Framework Work Role(s)

Software Security Assessment; Systems Requirements Planning; Incident Response; Executive Cyber Leader; Cyber Instructional Curriculum Developer

CAE-CD Technical Core KUs

Basic Cryptography (BCY)
Basic Networking (BNW)
Basic Scripting and Programming (BSP)
Network Defense (NDF)
Operating Systems Concepts (OSC)

For each program at the associate or baccalaureate level identified as a technical program (by the school), a set of technical core knowledge units needs to be chosen to support the PoS Validation requirements. The five knowledge units listed above constitute the set of Technical core which apply to all programs of study aligned with technical cybersecurity work roles.

Technical Core - Basic Cryptography (BCY)

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

KU Learning Outcomes

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

1. Identify the elements of a cryptographic system.
2. Describe the differences between symmetric and asymmetric algorithms.
3. Describe which cryptographic protocols, tools, and techniques are appropriate for a given situation.
4. Describe how crypto can be used, its strengths and weaknesses, modes, and issues that must be addressed before implementation (e.g., key management).

Topics

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

c. Case Studies (Heartbleed, Pass-the-hash, algorithm downgrades, etc.)

Vocabulary
Advanced Encryption Standard (AES); Asymmetric Cryptography; Cryptographic Attacks; Cryptographic Failures; Cryptographic Modes; Cryptographic Protocols; Cryptographic Standards; Cryptography; Data Encryption Standard (DES); Digital Signatures; Hash Functions; Key Management; Public Key Infrastructure (PKI); Symmetric Cryptography

Related Knowledge Units
Advanced Cryptography (ACR)

Most Related DCWF and/or NICE Framework Work Role(s)
Software Security Assessment; Secure Software Development; Infrastructure Support; Security Architect; Research and Development Specialist

Technical Core - Basic Networking (BNW)

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

KU Learning Outcomes

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

1. Describe and explain the fundamental concepts, technologies, components and issues related to communications and data networks.
2. Apply networking concepts to design a basic network architecture given a specific need and set of hosts/clients.
3. Apply and demonstrate knowledge of networking concepts by tracking and identifying the data packets involved in a simple TCP connection (or perform a trace of such a connection).
4. Apply and demonstrate use of a network monitoring tool to observe the flow of packets (e.g., WireShark).
5. Perform and examine results of network mapping (i.e., enumeration and identification of network components) (e.g., Nmap).
6. Describe common network vulnerabilities.

Topics

1. Networking models (e.g., OSI and TCP/IP)
2. Internet and World Wide Web
3. Network media (e.g., wired, optical, and wireless)
4. Network Architectures and topologies (e.g., PAN, LAN/WAN, DMZ, Enclaves, VLAN, NAT, subnetting, supernetting, bus, star, partial and full mesh, peer-to-peer, client-server)
5. Common Network Devices and their role in the network (e.g., Routers, Switches, clients and servers, Wireless Access Points, VPNs, Firewalls (hardware, software, virtual), All-in-One Appliances)
6. Network Protocols introduction (e.g., IP, TCP, UDP, ICMP)
7. Network Services and protocols introduction (e.g., DNS, NTP, VLAN, DHCP, etc.)
8. Network Applications and protocols introduction (e.g., SMTP, HTTP, VoIP, SSH, etc.)
9. Use of basic network administration tools (e.g., PING, Traceroute, SNMP)
10. Overview of Network Security Issues (e.g., Zero Trust, Defense-in-depth, SIEM/SOAR, Best Practices)
11. Log analysis (e.g., traffic, threat prevention, audit, event, session, Geo-location, user activity, system, compliance)
12. Basic business continuity and disaster recovery (e.g., basics of DRP, BCP, IRP)

Vocabulary

Business Continuity: Data Packet Analysis: Disaster Recovery: Network Administration: Network Architecture: Network Devices: Network Monitoring: Network Protocols: Network Security: Network Services: Network Topology: Network Vulnerabilities

Related Knowledge Units

Network Defense (NDF); Network Technology and Protocols (NTP); Advanced Network Technology and Protocols (ANT); Network Security Administration (NSA); Intrusion Detection/Prevention Systems (IDS); Wireless Sensor Networks (WSN)

Most Related DCWF and/or NICE Framework Work Role(s)

Insider Threat Analysis; Vulnerability Analysis; Software Developer; Authorizing Official/Designating Representative; Enterprise Architecture

Technical Core - Basic Scripting and Programming (BSP)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Write and execute simple scripts to automate system administration tasks.
2. Write and execute programs in a high-level language using basic programming constructs and concepts
3. Write and execute simple linear and looping scripts.
4. Write and execute simple and compound conditions within a programming language or similar environment (e.g., scripts, macros, SQL).
5. Implement basic security practices in scripting, including bounds checking and input validation.
6. Demonstrate conceptual understanding and practical use of regular programming or scripting expressions.

Topics

1. Basic security concepts
2. Permissions (e.g., Linux, Windows, MacOS), bounds checking, input validation, type checking and parameter validation
3. Fundamental concepts and basic implementation of regular expressions
4. Fundamental data structures and algorithms
5. Boolean logic/operations (e.g., AND / OR / XOR / NOT)
6. Scripting language on both Windows and Linux (e.g. PERL, Python, BASH, JAVA, VB Scripting, Powershell)
7. Integrated Development Environment (IDE), Compilers/Interpreters
8. Properly apply basic programming constructs and concepts including:
    a. Variables and types (e.g., int, float, char, etc.)
    b. Strings, arrays, structures
    c. Sequential and parallel execution
    d. Assignments (e.g., :=, =, ++, --, etc.)
    e. Decisions and branching (e.g., if, if ... else, elseif, switch, case, etc.)
    f. Loops (e.g., for, while, repeat, etc.)
    g. Functions, procedures, and calls
    h. Debugging techniques
    i. Console and file I/O
    j. Libraries

Vocabulary
Algorithms; Automation; Boolean Logic; Bounds Checking; Data Structures; Input Validation; Integrated Development Environment (IDE); Programming; Programming Constructs; Regular Expressions; Scripting; Security

Related Knowledge Units
Algorithms (ALG); Digital Forensics (DFS); Penetration Testing (PTT); Software Assurance (SAS); Secure Programming Practices (SPP)

Most Related DCWF and/or NICE Framework Work Role(s)
Enterprise Architecture; Executive Cyber Leader; Data Operations Specialist; Technical Support Specialist; Secure Systems Development

Technical Core - Network Defense (NDF)

The intent of the Network Defense (NDF) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

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

Topics

1. Concepts of network defense, such as:
    a. Defense-in-Depth
    b. Network attacks and exploitation
    c. Network Hardening
    d. Minimizing Exposure (e.g., Attack Surface and Vectors)
    e. MITREs D3FEND Matrix
2. Network defense/monitoring tools:
    a. Implementing Firewalls
    b. DMZs / Proxy Servers
    c. VPNs
    d. Decoys (e.g., Honeypots and Honeynets)
    e. Implementing IDS/IPS
    f. Traffic signature analysis
    g. Network anomaly detection
3. Network Operations
    a. Network Security Monitoring (e.g., NOCs, SOCs)
    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
5. Security Incident and Event Management (SIEM)
    a. Log analysis
    b. Visualization of anomalies

Vocabulary

Defense-in-Depth; Firewalls; IDS/IPS; Log Analysis; Minimizing Exposure; MITRE's D3FEND Matrix; Network Access Control; Network Attacks; Network Defense; Network Hardening; Network

Operations Center (NOC); Network Security Monitoring; Security Incident and Event Management (SIEM); Security Operations Center (SOC)

Related Knowledge Units

Basic Networking (BNW); Network Technology and Protocols (NTP); Advanced Network Technology and Protocols (ANT); Network Security Administration (NSA); Intrusion Detection/Prevention Systems (IDS); Wireless Sensor Networks

Most Related DCWF and/or NICE Framework Work Role(s)

Systems Requirements Planning; Incident Response; Infrastructure Support; Vulnerability Analysis; All-Source Analysis

Technical Core - Operating Systems Concepts (OSC)

The intent of this Operating Systems Concepts (OSC) 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.

KU Learning Outcomes

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

1. Describe and discuss the role and basic functions of an operating system.
2. Describe and discuss how operating systems interact with hardware and software applications.
3. Identify and describe basic security issues of operating systems.
4. Install, configure, and harden operating systems in a virtual environment.

Topics

1. Installation and configuration of common OSes (e.g., Linux distros, Windows)
2. Privileged and non-privileged states
3. Application processes and threads
4. Memory (e.g., real, virtual, and management)
5. Files systems, log files
6. Virtualization/hypervisors
7. Fundamental security design principles as applied to an OS (e.g., System Hardening, Domain separation, process isolation, resource encapsulation, least privilege)
8. Access controls (e.g., models and mechanisms)
9. Domain separation, process isolation, resource encapsulation, least privilege

Vocabulary

Configuration; File Systems; Hardware; Hypervisor; Installation; Memory Management; Non-Privileged States; Operating System; Privileged States; Security; Software; Virtualization

Related Knowledge Units

Operating Systems Hardening (OSH); Operating Systems Theory (OST)

Most Related DCWF and/or NICE Framework Work Role(s)

Data Operations Specialist; Enterprise Architecture; Exploitation Analyst; Software Developer; Product Support Manager

CAE-CD Non-Technical Core KUs

Cyber Threats (CTH)
Cybersecurity Planning and Management (CPM)
Policy, Legal, Ethics, and Compliance (PLE)
Security Program Management (SPM)
Security Risk Analysis (SRA)

For each program at the associate or baccalaureate level identified as a non-technical program (by the school), a set of non-technical core knowledge units must be chosen to support the PoS Validation requirements. The five knowledge units listed above constitute the set of Non-Technical core which apply for all programs of study aligned to relevant cybersecurity work roles.

Non-Technical Core - Cyber Threats (CTH)

The intent of the Cyber Threats (CTH) Knowledge Unit is to provide students with basic information about the malicious acts that aim to damage data, steal data, or disrupt digital operations in general that may be present in the cyber realm.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk.
2. Adequately communicate, rate in importance, and describe different types of cyber-attacks and their characteristics.
3. Evaluate threat intelligence to determine if a given attack/attacker/vulnerability combination is a threat to a given organization.
4. Explain and discuss how defending against cyber threats is critical for protecting systems, networks, and data from harm.

Topics

1. Motivations and Techniques
2. The Adversary Model (e.g., resources, capabilities, intent, motivation, risk aversion, access)
3. Types of Attacks and the vulnerabilities that enable them
    a. Brute force attack
    b. Password guessing / cracking
    c. Malware: Backdoors / trojans / viruses / wireless attacks
    d. Sniffing / spoofing / session hijacking / MiTM
    e. Denial of Service (DoS) / Distributed Denial of Service (DDoS)
    f. BOTs / Botnets
    g. Buffer Overflow
    h. Zero-day exploits
    i. Persistence
4. History of attacks
5. Indicators of compromise
6. Events that indicate an attack is/has happened
7. Attack timing (within x minutes of being attached to the net)
8. Attack surfaces / vectors, and trees
9. Hardware attacks
10. Covert Channels
11. Social Engineering
12. Tactics, Techniques, and Procedures (TTPs)
13. Threat actors
    a. Insider threat
    b. Script kiddies
    c. Advanced Persistent Threat (APT) Groups

14. Threat Information Sources (e.g., Common Vulnerabilities and Exposures (CVEs), CISA's Known Exploited Vulnerabilities, CERT, MITRE ATT&CK/ATLAS, OWASP Top 10 Web App Security Threats)
15. Open Source Intelligence (OSINT)

Vocabulary

Advanced Persistent Threats (APTs); Adversary Model; Common Vulnerabilities and Exposures (CVEs); Cyber Threats; Cyberattacks; Indicators of Compromise; Malware; Open Source Intelligence (OSINT); Social Engineering; Threat Actors; Threat Intelligence; Vulnerabilities

Related Knowledge Units

Security Program Management (SPM); Security Risk Analysis (SRA); Cyber Crime (CCR); Policy, Legal, Ethics and Compliance (PLE)

Most Related DCWF and/or NICE Framework Work Role(s)

Target Analysis; Secure Software Development; Defensive Cybersecurity; Incident Response; Vulnerability Analysis

Non-Technical Core - Cybersecurity Planning and Management (CPM)

The intent of the Cybersecurity Planning and Management (CPM) Knowledge Unit is to equip students with the knowledge and skills needed to strategically develop, implement, effectively communicate, and oversee policies and procedures that protect an organization’s information systems from cyber threats, strengthen data security, integrity, and availability while aligning cybersecurity initiatives with the organization's goals and regulatory obligations.

KU Learning Outcomes

To complete this KU, students will 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 security 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, and financial implications, of personnel in planning and managing security, including:
    a. Board of Directors
    a. Senior Management
    b. Chief Information Security Officer (CISO)
    c. IT Management (i.e., CIO, CTO, IT Director, etc.)
    d. Functional Area Management
    e. Information Security personnel
    f. End users
5. Discuss potential virtualization security risks and mitigation strategies.
6. Develop policies, processes, and procedures in relation to regulations, internationally recognized standards, and/or business requirements (such as Criminal Justice Information Services (CJIS) requirements for public service systems).

Topics

1. Broad coverage of the cybersecurity Common Body of Knowledge (CBK) as related to planning and management
2. Examples of Operational, Technical, and Strategic Planning and Management
3. C-Level Functions which impact cybersecurity
4. Making cybersecurity a strategic essential part of the core organizational strategy
5. Requirements and plans for Business Continuity / Disaster Recovery
6. Policies, processes, and procedures for incident response
7. Protection of intellectual property
8. Implementation of access controls
9. Patch and change control management
10. Risk Assessment and Management

11. Cybersecurity Policies and Procedures
12. Security Education, Training, and Awareness (SETA)
13. Compliance and Regulatory Requirements
14. Security Architecture and Design
15. Vendor and Third-Party Risk Management
16. Threat Intelligence and Analysis
17. Cybersecurity Metrics and Reporting

Vocabulary

Access Controls; Business Continuity; Compliance; Cybersecurity Planning and Management; Disaster Recovery; Incident Response; Intellectual Property; Patch Management; Risk Assessment; Security Architecture; Security Policies; Threat Intelligence

Related Knowledge Units

Security Program Management (SPM); Policy, Legal, Ethics and Compliance (PLE); Cyber Threats (CTH)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Legal Advice; Systems Authorization; All-Source Analysis; Executive Cyber Leader; Communications Security (COMSEC) Management

Non-Technical Core - Policy, Legal, Ethics, and Compliance (PLE)

The purpose of the Policy, Legal, Ethics, and Compliance (PLE) Knowledge Unit is to provide students with an understanding of both the technical and nontechnical qualities of information governance to ensure that organizations protect data, maintain trust, and operate within legal and ethical frameworks.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Identify and recall key applicable laws, regulations, and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data.
2. Describe the responsibilities related to the handling of data as it pertains to legal, ethical and/or agency auditing issues.
3. Describe and differentiate how the type of legal dispute (e.g., civil, criminal, private) affects the evidence used to resolve legal disputes.
4. Explain the importance of compliance with legal and ethical standards in cybersecurity.
5. Explain the challenges and dilemmas that cybersecurity professionals face in both legal and ethical situations.
6. Apply legal, ethical principles, and ethical decision-making to real-world situations in cybersecurity (i.e., case studies).

Topics

1. Purpose of policies
2. Types of policies (e.g., Information Security Policy, Acceptable Use Policy (AUP), Data Protection Policy, Incident Response Policy)
3. Key legal concepts (e.g., Data Protection Laws, Intellectual Property Laws, Cybercrime Laws, Contract Law)
4. Federal Laws and Authorities
   a. Computer Security Act
   b. Sarbanes – Oxley Act
   c. Gramm – Leach – Bliley Act
   d. Privacy (COPPA) HIPAA / FERPA
   e. USA Patriot Act
   f. Americans with Disabilities Act, Section 508
   g. Maturity Models (e.g., Cybersecurity Maturity Model Certification (CMMC))
   h. Other Federal laws and regulations
5. State, US and international standards / jurisdictions (e.g. GDPR)
6. Ethical principles (e.g., Confidentiality, Integrity, Accountability, Fairness)
7. Compliance areas (e.g., Regulatory Compliance, Internal Compliance, Audit and Assessment)
8. Payment Card Industry Data Security Standard (PCI DSS)

9. BYOD issues
10. Health Information Technology for Economic and Clinical Health Act (HITECH) (breach notifications)
11. Basic Intellectual Property Concepts
    a. Copyrights, Patents, and Trademarks
    b. Trade Secrets and Their Protection (e.g. Non-Disclosure Agreements (NDAs))
    c. Software/System User Agreements
12. Compliance
    a. Identification of Requirements
    b. Tracking and Reporting Compliance
    c. Compliance Audits and Assessments
13. Ethics
    a. Ethical Behaviors and Codes of Conduct
    b. Conflicts of Interest and Their Management
    c. Whistleblowing and Reporting Mechanisms

Vocabulary
Accountability; Audit; Compliance; Compliance Standards; Confidentiality; Cybercrime; Data Protection; Ethics; Integrity; Intellectual Property; Legal; Policy

Related Knowledge Units
Cybersecurity Principles (CSP); Cybersecurity Planning and Management (CPM); Cybersecurity Ethics (CSE); Security Program Management (SPM); Basic Cyber Operations (BCO); Forensic Accounting (FAC); Cyber Threats (CTH); Cyber Crime (CCR)

Most Related DCWF and/or NICE Framework Work Role(s)
Security Control Assessment; Secure Systems Development; Information Systems Security Developer; Product Manager; Data Analyst

Non-Technical Core - Security Program Management (SPM)

The intent of the Security Program Management (SPM) Knowledge Unit is to provide students with the knowledge necessary to define and implement a cybersecurity program for the protection of an organization’s systems and data.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Apply knowledge to identify goals, objectives and performance metrics and to develop a security program.
2. Apply knowledge to effectively manage a cybersecurity program.
3. Assess the effectiveness of a cybersecurity program.
4. Articulate the effectiveness of a cybersecurity program using applicable soft or nontechnical skills aligned with an administrative function.

Topics

1. Goals and objectives of a security program
2. Measuring the effectiveness of a security program (i.e., 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 Education, Training and Awareness (SETA)
8. Routine cybersecurity and information security risk assessments
9. 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. Business Continuity and Crisis Management
    j. Certification and Accreditation
10. Automation

Vocabulary

Security Organization; Security Program Management (SPM); Security Policies; Security Baselining; Cybersecurity Program; Goals and Objectives; Performance Metrics; Program

Monitoring and Control; Security Education, Training and Awareness (SETA); Risk Assessments; Incident Response Program; Business Continuity and Crisis Management

Related Knowledge Units
Cybersecurity Planning and Management (CPM); Systems Certification and Accreditation (SCA); Cybersecurity Fundamentals (CSF)

Most Related DCWF and/or NICE Framework Work Role(s)
Executive Cybersecurity Leadership; Secure Project Management; Systems Security Management; Enterprise Architecture; Systems Requirements Planning

Non-Technical Core - Security Risk Analysis (SRA)

The intent of the Security Risk Analysis (SRA) 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 system and recommend mitigations to identified risks.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe and explain how risk relates to a system security policy and governance.
2. Describe various risk analysis methodologies.
3. Evaluate and categorize risk with respect to technology, processes, individuals, the enterprise, and recommend appropriate responses.
4. Identify and select the optimal risk analysis methodology based on needs, advantages and disadvantages.
5. Annotate and apply standards, frameworks, legal requirements, and institutional (public/private) policy when conducting a risk assessment.

Topics

1. Risk Assessment/Analysis Methodologies
2. Risk Measurement and Evaluation Methodologies
3. Risk Management Models
4. Risk Management Processes (i.e., Identification (asset, threat, controls, consequences, and vulnerabilities; Estimation (methodology, assessment consequences, incident likelihood, risk), Evaluation, etc.)
5. Security Controls
6. Risk Mitigation Economics
7. Risk Transference/Acceptance/Mitigation
8. Following documented risk frameworks
9. Communication, documentation, and logging of cybersecurity risk
10. Standards, frameworks, legal requirements (e.g., NIST 800-53, CMMC 2.0, Privacy (COPPA) HIPAA / FERPA)

Vocabulary

Communication; Governance; Legal Requirements; Risk Analysis; Risk Assessment; Risk Frameworks; Risk Management; Risk Methodology; Risk Mitigation; Security Controls; Security Policy; Standards

Related Knowledge Units

Systems Certification and Accreditation (SCA); Foundational - Cybersecurity Fundamentals (CSF)

Most Related DCWF and/or NICE Framework Work Role(s)

Enterprise Architecture; Secure Systems Development; Systems Requirements Planning; Incident Response; Vulnerability Analysis

CAE-CD Optional Knowledge Units

Programs must document their programs of study using knowledge units. The categories of knowledge units that form the base of the program are *foundational* (used in all programs), and *core* (either Technical or Non-Technical). The remainder of the knowledge units are called optional KUs. 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 maybe used as optional KUs and if Non-Technical core is chosen, then Technical core maybe used as optional KUs.)

The following are the Optional Knowledge Units:

Advanced Algorithms (AAL)
Advanced Cryptography (ACR)
Advanced Network Technology and Protocols (ANT)
Algorithms (ALG)
Analog Telecommunications (ATC)
Basic Cyber Operations (BCO)
Business Continuity and Disaster Recovery (BCD)
Cloud Computing (CCO)
Cyber Crime (CCR)
Cyber-Physical Systems (CPS)
Cybersecurity Ethics (CSE)
Data Administration (DBA)
Data Structures (DST)
Database Management Systems (DMS)
Databases (DAT)
Device Forensics (DVF)
Digital Communications (DCO)
Digital Forensics (DFS)
Embedded Systems (EBS)
Forensics Accounting (FAC)
Formal Methods (FMD)
Fraud Prevention and Management (FPM)
Hardware Reverse Engineering (HRE)
Hardware/Firmware Security (HFS)
Host Forensics (HOF)
IA Architecture (IAA)
IA Compliance (IAC)
IA Standards (IAS)
Independent/Directed Study/Research (Emerging Topics) (IDR)
Industrial Control Systems (ICS)
Introduction to Theory of Computation (ITC)
Intrusion Detection/Prevention Systems (IDS)
Life-Cycle Security (LCS)
Low Level Programming (LLP)
Media Forensics (MEF)
Mobile Technologies (MOT)
Network Forensics (NWF)
Network Security Administration (NSA)
Network Technology and Protocols (NTP)
Operating Systems Hardening (OSH)
Operating Systems Theory (OST)
Operating System Administration (OSA)
Pre-OS Boot Environment (PBE)
Penetration Testing (PTT)
Privacy (PRI)
QA/Functional Testing (QAT)
Radio Frequency Principles (RFP)
Secure Programming Practices (SPP)
Software Assurance (SAS)
Software Reverse Engineering (SRE)
Software Security Analysis (SSA)
Supply Chain Security (SCS)
Systems Certification and Accreditation (SCA)
Systems Programming (SPG)
Systems Security Engineering (SSE)
Threat Intelligence (THI)
Virtualization Technologies (VVT)
Vulnerability Analysis (VLA)
Web Application Security (WAS)
Wireless Sensor Networks (WSN)

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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Understand and be able to implement the algorithms listed in the topics below.

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

Vocabulary

Algorithm Analysis; Algorithm Implementation; Algorithm Selection; Artificial Intelligence Algorithms; Bloom Filters; Coding; Compression; Data Analysis; Dynamic Programming; MapReduce; Markov Chain Monte Carlo; Naive Bayes

Related Knowledge Units

Algorithms (ALG)

Most Related DCWF and/or NICE Framework Work Role(s)

Communications Security (COMSEC) Management; Insider Threat Analysis; Information Systems Security Developer; Software Test and Evaluation Specialist; Software/Cloud Architect

Advanced Cryptography (ACR)

The intent of the Advanced Cryptography (ACR) Knowledge Unit is to provide students with knowledge of cryptographic algorithms, protocols, and their uses in the protection of information in various states (at rest, in processing, and/or in transit).

KU Learning Outcomes

To complete this KU, students will be able to:

1. Explain how various cryptographic algorithms and protocols work.
2. Evaluate security mechanisms based on cryptography.
3. Explain the application of cryptography in SSL, virtual private networks, secure storage, and other security applications.
4. Evaluate a cryptosystem and explain its vulnerability to errors or attacks.

Topics

1. Number Theory
2. Probability and Statistics
3. Understanding of the major algorithms (e.g., AES, 3DES/TDEA, RSA, ECC, SHA)
4. Suite B Algorithms
5. Understanding of the families of attacks (e.g., differential, man-in-the-middle, linear, etc.)
6. Hashing and Signatures
7. Key Management
8. Modes and appropriate uses
9. Classical Cryptanalysis (i.e., Konheim)
10. Identity-based Cryptography
11. Digital Signatures
12. Virtual Private Networks
13. Quantum Key Cryptography
14. Homomorphic encryption - advances and usage

Vocabulary

Cryptanalysis; Cryptographic Algorithms; Cryptographic Protocols; Data at Rest; Data in Processing; Data in Transit; Information Security; Key Management; Secure Storage; Security Mechanisms; SSL; Virtual Private Networks

Related Knowledge Units

Algorithms (ALG); Basic Cryptography (BCY)

Most Related DCWF and/or NICE Framework Work Role(s)

Communications Security (COMSEC) Management; Vulnerability Analysis; Information Systems Security Developer; Cyber Defense Incident Responder/Incident Response; Cyberspace Operations

Advanced Network Technology and Protocols (ANT)

The intent of the Advanced Network Technology and Protocols (ANT) 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 (VoIP).

KU Learning Outcomes

To complete this KU, students will be able to:

1. Identify and describe 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

1. Advanced Routing algorithms and protocols
   a. BGP
   b. OSPF
   c. MPLS
   d. Static and dynamic routing
   e. Route metrics
   f. Distance vector vs link state
2. Ethernet Switching (e.g., Spanning Tree Protocol, VLANs, Trunks, Link Aggregation, POE, port mirroring)
3. Wireless (e.g., WLAN topology, antennas, frequencies, channels, standards, security issues)
4. Remote Access (e.g., VPN, site-to-site vs client-to-site, standards, protocols, RDP)
5. Principles, protocols, and implications of software-defined networking
6. IPv6 Networking Suite including IPv6 security issues
7. Quality of Service
8. Network Services
9. Social Network implementation and security issues.
10. Voice over IP (VoIP)
11. Multicasting
12. Advanced Network Security Topics
    a. Secure DNS
    b. Network Address Translation
    c. Deep Packet Inspection
    d. Transport Layer Security
13. Troubleshooting (e.g., methodologies, cabling issues, wireless issues, general network issues)

Vocabulary

Advanced Routing Protocols; BGP; Ethernet Switching; IPv6; MPLS; Network Security; OSPF; Quality of Service (QoS); Remote Access; Software Defined Networking (SDN); Troubleshooting; Wireless Networking

Related Knowledge Units

Basic Networking (BNW); Network Defense (NDF); Network Technology and Protocols (NTP); Network Security Administration (NSA); Intrusion Detection/Prevention Systems (IDS); Wireless Sensor Networks (WSN)

Most Related DCWF and/or NICE Framework Work Role(s)

Network Operations; System Administrator; Research and Development Specialist; Communications Security (COMSEC) Management; Security Control Assessment

Algorithms (ALG)

The intent of the Algorithms (ALG) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Understand and be able to implement the algorithms listed in the topics below.

Topics

To complete this KU, all Topics must be completed:

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

Vocabulary

Algorithm Analysis; Average Case; Best Case; Computational Complexity; Greedy Algorithm; Iterative; Optimization; Recursion; Searching; Sorting; String Matching; Worst Case

Related Knowledge Units

Advanced Algorithms (AAL); Advanced Cryptography (ACR); Basic Cryptography (BCY)

Most Related DCWF and/or NICE Framework Work Role(s)

Software Developer; Software/Cloud Architect; Communications Security (COMSEC) Management; Systems Testing and Evaluation; Information Systems Security Developer

Analog Telecommunications (ATC)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe the basic concepts of modern analog communications systems and illustrate concepts using block diagrams.
2. Understand and 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

Vocabulary

Analog Communication Systems; Architecture; Bandwidth; Blocking; Call Arrival Models; Grade of Service; Interference Issues; Modulation; Noise; Signal-to-Noise Ratio; Signaling Methods; Switching; Trunks

Related Knowledge Units

Industrial Control Systems (ICS)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Curriculum Development; Program Manager; Cyber Operations Planner; AI Test and Evaluation Specialist; Knowledge Manager

Business Continuity and Disaster Recovery (BCD)

The intent of the Business Continuity and Disaster Recovery (BCD) Knowledge Unit is to prepare students to maintain business continuity and support organizational resilience. This KU covers the principles and practices necessary to develop, implement, and manage business continuity plans and disaster recovery strategies. Students learn to identify potential risks, create contingency plans, and establish protocols to maintain critical business functions during and after a disaster. The goal is to equip students with the skills to minimize downtime, protect data integrity, and maintain organizational resilience in the face of various threats.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Identify key components of a Business Continuity and Disaster Recovery (BCDR) plan, including risk assessment, business impact analysis, and recovery strategies.
2. Explain the differences between BCDR and describe how each contributes to organizational resilience.
3. Implement a basic BCDR plan for a small business, ensuring all critical processes and data are covered.
4. Analyze potential risks and vulnerabilities in an organization's current BCDR plan, and suggest improvements to enhance its effectiveness.
5. Evaluate the effectiveness of a BCDR plan through testing and simulation exercises, and recommend adjustments based on the outcomes.

Topics

1. Introduction to BCDR
   a. Definition and Importance
   b. Key Concepts: Business Continuity vs. Disaster Recovery
2. Risk Assessment and Business Impact Analysis (BIA)
   a. Identifying Potential Risks
   b. Assessing Impact on Business Operations
   c. Prioritizing Critical Business Functions
3. Business Continuity Planning (BCP)
   a. Developing a Business Continuity Plan
   b. Strategies for Maintaining Operations
   c. Communication Plans and Stakeholder Engagement
4. Disaster Recovery Planning (DRP)
   a. Developing a Disaster Recovery Plan
   b. IT Systems and Data Recovery
   c. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
5. Implementation and Testing
   a. Plan Implementation
   b. Regular Testing and Drills

    c. Updating and Maintaining Plans
6. Crisis Management and Response
    a. Incident Response Procedures
    b. Emergency Response Teams
    c. Communication During a Crisis
7. Regulatory and Compliance Requirements
    a. Relevant Laws and Regulations
    b. Industry Standards and Best Practices
8. Training and Awareness
    a. Employee Training Programs
    b. Awareness Campaigns
    c. Roles and Responsibilities
9. Continuous Improvement
    a. Post-Incident Review
    b. Lessons Learned
    c. Plan Updates and Enhancements

Vocabulary

Business Continuity Management (BCM); Business Continuity Planning (BCP); Business Impact Analysis (BIA); Crisis Management and Response; Disaster Recovery Planning (DRP); Disaster Recovery Strategies; Incident Response and Emergency Management; Organizational Resilience; Recovery Time Objective (RTO) and Recovery Point Objective (RPO); Risk Assessment

Related Knowledge Units

Cybersecurity Fundamentals (CSF); Cybersecurity Principles (CSP); Cybersecurity Planning and Management (CPM); Policy, Legal, Ethics, and Compliance (PLE); Security Program Management (SPM); Security Risk Analysis (SRA); IA Compliance (IAC)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Defense Infrastructure Support Specialist; IT Project Manager; Cyber Policy and Strategy Planner; Continuity of Operations Specialist; Cyber Incident Responder

Basic Cyber Operations (BCO)

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

KU Learning Outcomes

To complete this KU, students will 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.
5. Use attack frameworks to assess adversary behavior and motives for cyber operations.

Topics

1. Legal Authorities and Ethics
2. Stages of a Cyber Operation (and details of each phase)
    a. Target Identification
    b. Reconnaissance
    c. Gaining Access
    d. Hiding Presence
    e. Establishing Persistence
    f. Execution
    g. Assessment
3. Basic Process Modeling
4. Validating Procedures
5. Handling failures to follow procedures
6. Case studies of actual cyber operations
7. MITRE ATT&CK/ATLAS
8. Creating and validating security procedures
9. Threat intelligence
10. Process Feedback
11. Case studies of actual cyber operations

Vocabulary

Assessment; Cyber Operations; Ethics; Execution; Gaining Access; Hiding Presence; Legal Authorities; MITRE ATT&CK; Reconnaissance; Target Identification; Threat Intelligence

Related Knowledge Units

Network Forensics (NWF); Penetration Testing (PTT); Vulnerability Analysis (VLA); Web Application Security (WAS)

Most Related DCWF and/or NICE Framework Work Role(s)

Defensive Cybersecurity; All-Source Collection Requirements Management; All-Source Analyst; DevSecOps Specialist; Insider Threat Analysis

Cloud Computing (CCO)

The intent of the Cloud Computing (CCO) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Compare cloud computing to traditional computing.
2. List each type of service/model of cloud computing.
3. Explain cloud security (e.g., attacks, mitigations, overall vulnerability).
4. Describe the challenges of securing cloud assets and apply strategies to improve cloud security.

Topics

1. Virtualization platforms
2. Cloud Services (e.g., SaaS, PaaS, DaaS, IaaS, FaaS)
3. Scalability
4. Service Oriented Architectures
5. Service Level Agreements (SLAs)
6. Deployment Models (e.g., private, public, community, hybrid)
7. Cloud security (e.g., data protection, identity and access management, compliance, governance, and incident response)
8. Common cloud security tools and services
9. Best practices in cloud computing cybersecurity
10. Storage
11. Identity and Access Management (IAM) in cloud systems
12. Resilience and Disaster recovery
13. Forensics/IR Implications of cloud use
14. Legal/Privacy/Regulatory/Compliance Issues

Vocabulary

Cloud Computing; Cloud Security; Cloud Services (SaaS, PaaS, DaaS, IaaS, FaaS); Data Protection; Deployment Models (Private, Public, Community, Hybrid); Forensics/Incident Response; Identity and Access Management (IAM); Legal/Privacy/Regulatory/Compliance; Resilience and Disaster Recovery; Scalability; Service Level Agreements (SLAs); Virtualization

Related Knowledge Units

Virtualization Technologies (VTT); IA Architecture (IAA)

Most Related DCWF and/or NICE Framework Work Role(s)

Security Control Assessment; Communications Security (COMSEC) Management; Software Security Assessment; COMSEC Manager; Cyber Defense Infrastructure Support Specialist

Cyber Crime (CCR)

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

KU Learning Outcomes

To complete this KU, students will 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.
3. Examine case studies of Internet cybercrime methods and potential protections.

Topics

1. Cyber Crime Types
    a. Social Engineering (e.g., Phishing, Vishing, SMiShing, Impersonation)
    b. Hacking
    c. Intrusions
    d. Malware (e.g., Ransomware, Trojans)
    e. Espionage
    f. Intellectual Property Theft
    g. Fraud and Financial Crime
    h. Child Exploitation
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
9. Ethical codes and societal norms
    a. Rights of others
    b. Respect and principles of community
    c. Resource use, allocation, and abuse
    d. Cybersecurity and social responsibility
10. Common tactics used in cyber crime (e.g., malware, botnets, exploit kits, dark web)
11. Impact of cyber crime (e.g., financial loss, reputation damage, legal consequences, operational disruption)

Vocabulary

Cyberbullying; Cyber Laws; Cybercrime; Cybersecurity; Cyberstalking; Cyber Terrorism; Espionage; Hacking; Identity Theft; Intellectual Property Theft; Malware; Social Engineering

Related Knowledge Units
Cyber Threats (CTH); Policy, Legal, Ethics, and Compliance (PLE)

Most Related DCWF and/or NICE Framework Work Role(s)
Secure Software Development; Secure Systems Development; Knowledge Management; Defensive Cybersecurity; Infrastructure Support

Cyber-Physical Systems (CPS)

The intent of the Cyber-Physical Systems (CPS) Knowledge Unit is to provide students with a basic understanding of the fundamental concepts, principles, and practices in designing, developing, and deploying CPS.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe the integration of computational and physical processes, including the role of sensors, actuators, and control systems in CPS.
2. Implement strategies for ensuring the safety, security, and reliability of CPS, particularly in critical applications such as healthcare, transportation, and industrial automation.
3. Analyze and evaluate CPS applications in various industries, such as smart grids, autonomous vehicles, and smart cities.

Topics

1. Architecture and Design (e.g., system design, modeling, and simulation)
2. Security and Privacy of CPSs including threats, vulnerabilities, risk assessment, and mitigation strategies
3. Real-time Systems (e.g., scheduling, synchronization, and timing analysis)
4. Networked Systems (e.g., communication protocols, network architecture, and distributed systems)
5. Embedded Systems (e.g., microcontrollers, embedded software, and hardware-software integration)
6. Sensor and Actuator Systems (e.g., sensor fusion, actuator control, and feedback mechanisms)
7. Control Systems (e.g., control theory, stability analysis, and optimization techniques)
8. Human-Machine Interface (e.g., user interface design, human factors, and usability)
9. Internet of Things (IoT) (e.g., IoT architectures, protocols, and applications)
10. Safety and Reliability (e.g., hazard analysis, fault tolerance, and system reliability)
11. Standards and Regulations (e.g., industry standards, regulatory requirements, and compliance)
12. Physical Security Information Management (PSIM) Systems
13. Security of Unmanned Aerial Vehicle (UAV)/drones including security of drone platforms, communications, evidence artifacts, and supply chain in the design and construction

Vocabulary

Actuator Control; Applications; Compliance; Control Theory; Cyber-Physical Systems (CPS); Embedded Systems (EBS); Fault Tolerance; Feedback Mechanisms; Hardware/Firmware Security (HFS); Hazard Analysis; Human Factors; Human-Machine Interface; Industrial Control Systems (ICS); Industry Standards; Internet of Things (IoT); IoT Architectures; Mitigation Strategies; Modeling and Simulation; Networked Systems; Optimization Techniques; Protocols; Regulatory

Requirements; Risk Assessment; Safety and Reliability; Security and Privacy; Sensor Fusion; Scheduling; Stability Analysis; Standards and Regulations; System Design; System Reliability; User Interface Design; Usability

Related Knowledge Units

Embedded Systems (EBS); Hardware/Firmware Security (HFS); Industrial Control Systems (ICS)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Defense Infrastructure Support Specialist; Systems Security Analyst; Industrial Control Systems (ICS) Security Specialist; Cyber Operator; Network Operations Specialist

Cybersecurity Ethics (CSE)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Explain how ethical foundations are applied to situations arising from the interconnected world.
2. Examine diverse and global ethical dilemmas.
3. Describe the role of cybersecurity in supporting and encouraging ethics, as well as where cybersecurity practices can cause ethical conflicts.
4. Identify and recall key ethical principles and frameworks relevant to cybersecurity.
5. Examine and differentiate between various ethical issues and conflicts in cybersecurity.
6. Assess the effectiveness of different ethical decision-making approaches in cybersecurity.

Topics

1. Ethical Codes and Frameworks
2. Ethics and Cyberspace
3. Ethical Issues
    a. Property
    b. Availability
    c. Rights of others
    d. Respect and principles of community
    e. Resource use, allocation, and abuse
    f. Censorship
4. Ethics-based decision tools
5. Cybersecurity and social responsibility
6. Ethical Foundations in Cybersecurity
7. Common Ethical Dilemmas in Cybersecurity
8. Ethical Decision-Making Tools
9. Role of Cybersecurity in Promoting Ethics
10. Impact of Cybersecurity Practices on Society

Vocabulary

Availability; Censorship; Community Principles; Cyber Ethics; Cybersecurity Principles; Ethical Conflicts; Ethical Decision Making; Ethical Dilemmas; Ethical Frameworks; Property Rights; Resource Allocation; Social Responsibility

Related Knowledge Units

Policy, Legal, Ethics, and Compliance (PLE); Cybersecurity Principles (CSP)

Most Related DCWF and/or NICE Framework Work Role(s)
AI Risk and Ethics Specialist; Systems Authorization; Incident Response; Exploitation Analyst; Cyber Defense Infrastructure Support Specialist

Data Administration (DBA)

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

KU Learning Outcomes

To complete this KU, students will 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 (e.g., 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. Internal and external data policies
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

Vocabulary
Data Accessibility; Data Archival; Data Classification; Data Governance; Data Lifecycle; Data Management; Data Ownership; Data Quality; Data Security; Data Storage; Data Stewardship; Data Utility

Related Knowledge Units
Databases (DAT); Database Management Systems (DMS)

Most Related DCWF and/or NICE Framework Work Role(s)
Systems Administration; Partner Integration Planning; Knowledge Manager; Data Scientist; AI Test and Evaluation Specialist

Data Structures (DST)

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

KU Learning Outcomes

To complete this KU, students will 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 (e.g., 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
14. Graphs
15. Backtracking

Vocabulary

Abstract Data Types; Array; Data Formats; Data Structures; Double Linked List; Hash Table; Heap; Linked List; Queue; Stack; Tree; Vector

Related Knowledge Units

Basic Scripting and Programming (BSP); Databases (DAT)

Most Related DCWF and/or NICE Framework Work Role(s)

DevSecOps Specialist; Systems Testing and Evaluation; Program Manager; AI Risk and Ethics Specialist; Data Analysis

Database Management Systems (DMS)

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

KU Learning Outcomes

To complete this KU, students will 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 (e.g. user creation/deletion, permissions and access controls)
5. Database concepts (e.g. Indexing, Inference, Aggregation, Polyinstantiation)
6. Database Security
    a. How to protect data (e.g., confidentiality, integrity and availability in a DBMS context)
    b. Vulnerabilities (e.g., SQL injection)

Vocabulary

Access Controls; Data Definition Language (DDL); Data Integrity; Data Manipulation Language (DML); Database Administration; Database Management System (DBMS); Database Security; Distributed Database; Hierarchical Database; Relational Database; SQL; SQL Injection

Related Knowledge Units
Databases (DAT); Data Administration (DBA)

Most Related DCWF and/or NICE Framework Work Role(s)
Data Analysis; Database Administration; Program Manager; Database Administrator; Data Architect

Databases (DAT)

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

KU Learning Outcomes

To complete this KU, students will 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

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 (e.g., 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 (e.g., DAC, MAC, RBAC, Clark-Wilson)

Vocabulary

Access Control; Client; Data Security; Database, Database Server; DBMS; Distributed Database; Encryption; Hashing; Inference; Injection; NoSQL Database; Query; Relational Database; Server, SQL; Tables

Related Knowledge Units

Database Management Systems (DMS); Data Administration (DBA); Data Structures (DST)

Most Related DCWF and/or NICE Framework Work Role(s)

Database Administration; Systems Requirements Planner; Data Operations Specialist; AI Test and Evaluation Specialist; Knowledge Management

Device Forensics (DVF)

The intent of the Device Forensics (DVF) Knowledge Unit is to provide students with the ability to apply forensics techniques to investigate and analyze mobile, tablets, and wearable devices, including forensic recovery, analysis, and preservation of data from mobile devices.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe methods for data acquisition and extraction, analysis of widespread, mobile, tablets, and wearable devices.
2. Perform physical and logical extractions, handle data acquisition tools, and understand the challenges of dealing with locked or encrypted devices.
3. Explain the legal issues related to mobile, tablets, and wearable devices to conduct forensic analyses.

Topics

1. Device acquisition and evidence extraction tools and procedures (e.g., obtaining, collecting, and documenting)
2. Mobile Device Operating Systems
3. Sim and SD Card information
4. Device Encryption and Recovery
5. Mobile Device Analysis (e.g. smart phones, tablets)
6. Embedded Systems (e.g. GPS, games consoles, Smart TVs)
7. Internet of Things Devices and IoT Apps on mobile devices (e.g. consideration of potential for evidence storage)
8. Legal and ethical considerations of mobile device forensics
9. Mobile device forensic tools

Vocabulary

Analysis; Data Acquisition; Encryption; Extraction; Forensic Recovery; Internet of Things Devices; Legal Issues; Mobile Device Operating Systems; Mobile Devices; Preservation; Tablets; Wearable Devices

Related Knowledge Units

Digital Forensics (DFS); Media Forensics (MEF)

Most Related DCWF and/or NICE Framework Work Role(s)

Data Operations Specialist; Digital Forensics; Product Designer (User Interface/UI); Cybercrime Investigation; Digital Evidence Analysis

Digital Communications (DCO)

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

KU Learning Outcomes

To complete this KU, students will 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 (e.g., CDMA, TDMA, FDMA, SDMA, PDMA)

Vocabulary

Code-Division Multiple Access (CDMA); Coding Schemes; Current State of the Art; Digital Communications; Digital Signaling; Frequency-Division Multiple Access (FDMA); Modulation Techniques; Pattern-Division Multiple Access (PDMA); Spread Spectrum Signals; Subsystems; Time Division Multiple Access (TDMA); Space-Division Multiple Access (SDMA)

Related Knowledge Units

IA Architectures (IAA); Analog Telecommunications (ATC)

Most Related DCWF and/or NICE Framework Work Role(s)

Privacy Compliance Manager; Cybersecurity Curriculum Development; Cyber Crime Investigator; Cyber Defense Forensics Analyst; Systems Testing and Evaluation

Digital Forensics (DFS)

The intent of the Digital Forensics (DFS) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Discuss the rules, laws, policies, and procedures that affect digital forensics.
2. Identify and describe the steps of the digital forensics' investigation lifecycle.
3. Describe methods for the acquisition/analysis of various compute devices.
4. Use one or more common DF tools, such as Autopsy, Cellebrite, EnCase, FTK, ProDiscover, Magnet Axiom, OpenText, ProDiscover, SleuthKit, and/or X-Ways.
5. Perform memory extraction from mobile, embedded, and/or IoT devices.

Topics

1. Legal Compliance
    a. Applicable Laws
    b. Affidavits
    c. How to Testify
    d. Case Law
    e. Chain of custody
    f. Rule of Evidence
    g. Search Warrant
2. Digital Investigations
    a. E-Discovery
    b. Authentication of Evidence
    c. Chain of Custody Procedures
    d. Root Cause Analysis
3. Evidence acquisition
4. Create Forensic Images
5. Operating System Artifacts
6. Document Artifacts
7. E-mail Artifacts
8. Data Carving
9. Device Memory Extraction
    a. Device acquisition tools and procedures (e.g., obtaining, collecting, and documenting)
    b. Types of Devices (e.g., Mobile, Embedded, IoT, etc)
10. Key Components of Digital Forensics (e.g., evidence collection, data recovery, analysis, forensic imaging, forensic tools and software, legal considerations, reporting, presentation of evidence)
11. Preservation of digital evidence (e.g. use of Faraday Bags)
12. Digital Forensics Lifecycle (e.g., identification, preservation, collection, examination, analysis, documentation, presentation, review)

13. Use of free open source and commercial software tools and techniques for forensics acquisition, discovery, analysis, and reporting
14. Create Forensic Reports

Vocabulary

Digital Forensics (DF); Legal Compliance; Digital Investigations; Evidence Acquisition; Forensic Imaging; Operating System Artifacts; Data Carving; Device Memory Extraction; Digital Forensics Lifecycle; Forensic Tools; Forensic Reports; Chain of Custody

Related Knowledge Units

Basic Cryptography (BCY); Cybersecurity Ethics (CSE); Device Forensics (DVF); Host Forensics (HOF); Media Forensics (MEF); Operating Systems Concepts (OSC)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Curriculum Development; Digital Evidence Analysis; Technology Research and Development; Digital Forensics; Forensics Analyst

Embedded Systems (EBS)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Identify and describe the fundamental components and architecture of embedded systems, including microcontrollers, sensors, and actuators.
2. Explain the constraints and challenges associated with developing applications for embedded devices, such as concurrency, synchronization, limited memory, processing power, and energy consumption
3. Develop and implement basic embedded real-time resource management system applications using appropriate programming languages and tools, ensuring compliance with device constraints.
4. Evaluate the performance and efficiency of embedded system applications, identifying potential bottlenecks and areas for optimization.
5. Design, develop and prototype embedded system solutions that address specific real-world problems, integrating hardware and software components effectively.

Topics

1. Introduction to Embedded Systems
    a. Definition and Characteristics
    b. Examples and Applications
    c. Differences between Embedded Systems and General-Purpose Computers
2. Embedded System Components (e.g., Hardware and Software)
3. Embedded System Design and Development
4. Microcontroller/embedded processor architectures
5. PLC's, Gate Arrays, and other common programmable logic devices
6. I/O, A/D, registers, sensors, actuators, and embedded hardware components
7. Memory (e.g., RAM, ROM, Flash)
8. Embedded devices communications
9. Interrupt handling and timing issues
10. Resource management in real time systems
11. Devices without operating systems
12. Real-Time Operating Systems (RTOS)
13. Security in Embedded Systems
14. Security issues imposed by limited resources
15. Programming languages and environments for embedded systems
    a. Tool chains
    b. Target operating systems and devices
    c. Cross compilers

Vocabulary

Actuators; Embedded Programming Languages; Embedded System Design; Embedded Systems; Interrupt Handling; Memory Management (RAM, ROM, Flash); Microcontrollers; Real-Time Operating Systems (RTOS); Real-Time Systems; Resource Management; Security in Embedded Systems; Sensors

Related Knowledge Units
Basic Networking (BNW); Cybersecurity Principles (CSP); Operating Systems Concepts (OSC); Hardware/Firmware Security (HFS); Hardware Reverse Engineering (HRE); Industrial Control Systems (ICS); Systems Programming (SPG)

Most Related DCWF and/or NICE Framework Work Role(s)
Software Test and Evaluation Specialist; Cybersecurity Architecture; System Testing and Evaluation Specialist; Systems Requirements Planning; Product Support Manager

Forensic Accounting (FAC)

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

KU Learning Outcomes

To complete this KU, students will 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

Vocabulary

Business Valuation; Concealed Revenue; Damages; Detection Techniques; Evidence Management; Financial Statement Fraud; Forensic Accounting; Investigative Accounting; Litigation Support; Loss Calculation; Money Laundering; Prevention and Detection

Related Knowledge Units

Cyber Crime (CCR); Digital Forensics (DFS); Network Forensics (NWF); Policy, Legal, Ethics, and Compliance (PLE)

Most Related DCWF and/or NICE Framework Work Role(s)

Data Officer; AI Risk and Ethics Specialist; Data Analysis; Partner Integration Planning; Product Designer User Interface (UI)

Formal Methods (FMD)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Apply formal cybersecurity policy models to real world scenarios.
2. Describe the use of mathematical logic in the design of securing systems.

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

Vocabulary

Algorithms; Automated Reasoning Tools; Bell-LaPadula Model; Cryptography; Cybersecurity Policy Models; Formal Methods (FMD); Mathematical Logic; Proofs; Specification; System Design; System Modeling; Software Engineering

Related Knowledge Units

Algorithms (ALG); Advanced Algorithms (AAL); Basic Cryptography (BCY); Advanced Cryptography (ACR)

Most Related DCWF and/or NICE Framework Work Role(s)

Executive Cyber Leader; Data Scientist; Executive Cybersecurity Leadership; Software Security Assessment; Cyber Instructor

Fraud Prevention and Management (FPM)

The intent of the Fraud Prevention and Management (FPM) Knowledge Unit is to provide students with the necessary knowledge to develop plans and processes for a holistic approach to preventing and mitigating the variety of cybercrime and cyber-related fraud throughout the system lifecycle.

KU Learning Outcomes

To complete this KU, students will 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.
7. Recognize the importance of public and private partnerships, through law enforcement and industry, for the benefit of fraud awareness.

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
10. Nation-state adversaries

Vocabulary

Consumer Fraud; Cybercrime; Data Driven Detection; Financial Statement Fraud; Fraud Detection; Fraud Prevention; Fraud Triangle; Investigation; Legal and Ethical Requirements; Nation-State Adversaries; Public-Private Partnerships; Record Keeping

Related Knowledge Units

Cyber Crime (CCR); Forensic Accounting (FAC)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Legal Advice; Cyber Crime Investigator; Cyber Defense Forensics Analyst; Executive Cybersecurity Leadership; Security Control Assessment

Hardware Reverse Engineering (HRE)

The intent of the Hardware Reverse Engineering (HRE) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. 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

Vocabulary

Data Collection; Functionality; Hardware Components; Instrumentation; Inputs; Measuring; Modification; Outputs; Probing; Reverse Engineering; Stored Data; Stimulation

Related Knowledge Units

Hardware/Firmware Security (HFS); Systems Security Engineering (SSE)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Defense Analyst; Systems Testing and Evaluation; Technical Support; Cyber Operations Planner; Technical Support Specialist

Hardware/Firmware Security (HFS)

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

KU Learning Outcomes

To complete this KU, students will 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.
5. Discuss how hardware and firmware security technologies can be combined to layer defenses.

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.)
    g. Trusted Platform Module (TPM)

    h. UEFI Secure Boot (e.g., PEI, SEC, DXE, BDS, Bootloader phases)

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
    e. UEFI Secure Boot bypasses (e.g., BLACKLOTUS, BOOTHOLE)
8. Microcode vulnerabilities
9. Firmware vulnerabilities (e.g., Reflashing BIOS/PROMs)
10. Security role of intermediate layers
    a. Hardware Abstraction Layer
    b. Virtualization Layers

Vocabulary

Bootloader Vulnerabilities; Equipment Destruction Attacks; Firmware Vulnerabilities; Hardware Side Channel Attacks; Hardware Security Components; Hardware/Firmware Security; Microcode Vulnerabilities; Physical Security Attributes; Physical Vulnerabilities; Security Role of Intermediate Layers; Sourcing Attacks; Trusted Platform Module (TPM)

Related Knowledge Units

Basic Cryptography (BCY); Cyber Threats (CTH); Embedded Systems (EBS); Hardware Reverse Engineering (HRE); Life-Cycle Security (LCS); Low Level Programming (LLP); Supply Chain Security (SCS); Systems Programming (SPG); Systems Security Engineering (SSE)

Most Related DCWF and/or NICE Framework Work Role(s)

Software Security Assessment; COMSEC Manager; Target Network Analysis; Cyber Defense Incident Responder; Cybersecurity Curriculum Development

Host Forensics (HOF)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Discuss the forensic investigation process
2. Describe what can/cannot be retrieved from various Operating Systems.
3. Describe the methodologies used in host forensics.
4. Perform live system investigation and provide host forensics report.

Topics

1. Forensic investigation process
2. File Systems and File System Forensics
3. Hypervisor Analysis
4. Cryptanalysis
5. Rainbow Tables
6. Known File Filters (KFF)
7. Steganography
8. File Carving
9. Live System Investigations (e.g., artifacts from forensic tool usage on a host)
10. Log and Timeline Analysis
11. Host application forensics analysis

Examples of acceptable operating system specific Topics may include:

1. Registry Analysis, FAT/NTFS/GPT, Microsoft Office Forensics, Web Browser Forensics (Microsoft Windows)
2. Preference List Analysis, HFS+/AFS (Apple MacOS)
3. System configuration Analysis, EXT2/3/4 (Linux)

Vocabulary

Cryptanalysis; File Carving; File System Forensics; Forensic Investigation Process; Host Application Forensics; Hypervisor Analysis; Known File Filters; Live System Investigations; Log and Timeline Analysis; Rainbow Tables; Registry Analysis; Steganography

Related Knowledge Units

Device Forensics (DVF); Digital Forensics (DFS); Independent/Directed Study/Research (IDR); Media Forensics (MEF); Network Forensics (NWF)

Most Related DCWF and/or NICE Framework Work Role(s)

Digital Forensics; Insider Threat Analysis; Forensics Analyst; Cyber Instructor; Technology Research and Development

IA Architectures (IAA)

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

KU Learning Outcomes

To complete this KU, students will 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. TCB Subsets
6. Enterprise Architectures / Security Architectures
7. Secure network design
8. Discuss the forensic investigation process
9. Discuss the forensic investigation process

Vocabulary

Composition and Security; Data Protection; Defense-in-Depth; DMZ (Demilitarized Zone); Enterprise Architecture; Forensic Investigation; Information System Security; Proxy Server; Secure Network Design; Security Architecture; TCB (Trusted Computing Base); Vulnerability Assessment

Related Knowledge Units

Cloud Computing (CCO)

Most Related DCWF and/or NICE Framework Work Role(s)

Communications Security (COMSEC) Management; Insider Threat Analysis; Target Network Analysis; Cyber Instructor; IT Investment Portfolio Manager

IA Compliance (IAC)

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

KU Learning Outcomes

To complete this KU, students will 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

Vocabulary

Audit; Audit Activities; Audit Baseline; Audit Charter; Audit Reporting; Compliance; External Audit; Findings; Internal Audit; Mitigation Strategy; Recommendations; Regulatory Compliance

Related Knowledge Units

Cybersecurity Planning and Management (CPM); Policy, Legal, Ethics, and Compliance (PLE); QA/Functional Testing (QAT)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Legal Advice; Cybersecurity Architecture; IT Program Auditor; Secure Project Management; Systems Authorization

IA Standards (IAS)

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

KU Learning Outcomes

To complete this KU, students will 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 (e.g. PCI/DSS)
5. Open Standards (e.g. OWASP)

Vocabulary

FERPA; FISMA; Framework-based Standards; HIPAA; Information Security Standards; Laws; NIST 800-53; PCI/DSS; Policies; Regulations; Sarbanes-Oxley; Voluntary Standards

Related Knowledge Units

QA/Functional Testing (QAT)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Legal Advice; Executive Cyber Leader; Enterprise Architect; DevSecOps Specialist; AI/ML Specialist

Industrial Control Systems (ICS)

The intent of the Industrial Control Systems (ICS) Knowledge Unit is to provide students with an understanding of the basics of industrial control systems, including Supervisory Control and Data Acquisition (SCADA) systems, their architecture, components, communication protocols, as well as their vulnerabilities and security challenges. Students will learn about the basics of ICS and SCADA security best practices environments, including their role in operating critical infrastructure, their key differences from information systems, their common vulnerabilities, and approaches to advancing their resilience.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Identify and recall the fundamental components and architecture of ICS and SCADA systems.
2. Describe the use and application of Programmable Logic Controllers (PLCs) in automation.
3. Describe approaches to address common weaknesses while considering unique ICS characteristics and requirements.
4. Apply knowledge of ICS and SCADA systems to identify potential vulnerabilities and threats.
5. Explain how ICS environments differ from traditional information system environments.
6. Explain how security models are being used to guide ICS and SCADA systems security.

Topics

1. Industrial operations ecosystem
   a. Industry sectors
   b. Professional roles and responsibilities in industrial environments
   c. Process types
   d. Industrial lifecycles
   e. Workplace safety
2. Instrumentation and control systems
   a. Supervisory Control and Data Acquisition (SCADA) Systems
   b. Types of ICSs (e.g., power distribution systems, manufacturing)
   c. Models of ICS systems (e.g., time-driven vs. event-driven)
   d. Sensors and actuators
   e. Controllers (Programmable Logic Controllers (PLC), Remote Terminal Units (RTUs), Distributed Control Systems (DCS))
   f. Controller programming (ladder diagram, function block, structured text, sequential function chart)
   g. Human-Machine Interfaces (HMIs) in ICS and SCADA systems
3. Process equipment
   a. Hardware components of ICS and SCADA systems (e.g. Motors, valves, pumps, compressors, generators, boilers, and reactors)
4. Industrial control networking and communications

    a. ICS and SCADA systems protocols and networking (e.g., Ethernet/IP, MODBUS, PROFINET, DNP3, OPC, ICCP, HART)
    b. Other ICS communications technologies (e.g. serial, RS232/485, ZIGBEE, 900MHz, Bluetooth, X.25)

5. Process safety and reliability (e.g., causes of safety risk, hazards assessment, impact analysis)
6. Industrial cybersecurity guidance and regulations
    a. Regulatory, compliance, and industry standards and guidelines (e.g., NIST, IEC 62443) requirements for ICS and SCADA systems
    b. ICS Network Security Architectures (e.g., Purdue Enterprise Reference Architecture, Converged Plantwide Ethernet, levels, zones, cells, conduits)
7. Common weaknesses affecting ICS environments
    a. ICS and SCADA security challenges
    b. Common vulnerabilities in critical infrastructure, ICS, and SCADA systems
    c. Threats and attack vectors affecting ICS environments
8. ICS events and incidents response/recovery
9. ICS cybersecurity defensive techniques (e.g., network segmentation, anomaly detection, device hardening, engineered controls)

Vocabulary
Production Operations; Critical Infrastructure; Industrial Processes; Industry Sectors; Facilities; Engineering Documentation; Piping and Instrument Diagrams; Industrial Control Systems; Control Rooms; Control Enclosures; Operator Interfaces; Engineering Computers; Controllers; Input/Output; Sensors and Transmitters; Control Logic; Process Equipment; Reference Architectures; Signals and Protocols; IEC 62443; NIST SP 800-82; Physical Consequences; Positive Control; Cyber-Informed Engineering; Process Hazards Assessment; Fail-Safes

Related Knowledge Units
Business Continuity and Disaster Recovery (BCD), Cyber-Physical Systems (CPS), Embedded Systems (EBS), Life-Cycle Security (LCS)

Most Related DCWF and/or NICE Framework Work Role(s)
Cybersecurity Curriculum Development; Information Systems Security Manager; Operational Technology (OT) Cybersecurity Engineering Work Role; Control Systems Security Specialist; Vulnerability Assessment Analyst; Cybersecurity Instruction; Technology Research and Development

Independent/Directed Study/Research (IDR)

The intent of the Independent/Directed Study/Research (IDR) Knowledge Unit (KU) is to provide credit for courses that address emerging issues related to Information security and Cyber Defense. This KU can only be used for one aligned course and must adequately provide evidence of Cyber Defense topics addressed.

KU Learning Outcomes

To be determined by the academic unit offering the KU-aligned course covering this KU.

Topics

Courses focused on emerging technologies and their security relevant issues or new Tools, Techniques, and Methods related to Cyber Defense. This "wild-card" Knowledge Unit allows an applicant school to submit a Cyber Defense course for credit towards satisfying the academic requirements for PoS Validation. Only one course may be aligned for credit. It will be up to the review committee to validate if the course is worthy of credit.

Related Knowledge Units

None

Introduction to Theory of Computation (ITC)

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

KU Learning Outcomes

To complete this KU, students will 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

Vocabulary

Automata; Big O Notation; Complexity; Computability; Deterministic Finite Automata; Formal Language Theory; Non-Computability; Non-Deterministic Finite Automata; Non-Deterministic Polynomial Time (NP); Polynomial Time (P); Turing Computability; Turing Machines

Related Knowledge Units

Formal Methods (FMD); Operating Systems Theory (OST)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Intelligence Planner, All Source Analyst, AI Risk and Ethics Specialist, AI/ML Specialist, Systems Security Analyst

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, preventing, and analyzing vulnerabilities and threats and taking steps to mitigate associated risks, including early detection of cyber intrusions.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Detect, identify, resolve and document host or network intrusions.
2. Apply cyber threat intelligence and MITRE ATT&CK framework to achieve early detection of cyber intrusions.
3. Apply tools and algorithms to detect various anomalous activity, types of malware, and unauthorized devices on a network.
4. Leverage baseline activity to configure IDS/IPS and maximize efficiency (e.g., reduce false positives and false negatives).
5. Apply open-source data to enrich and analyze logs using techniques such as data visualization, event correlation, and anomaly detection.
6. Deploy and test mitigation responses to detected intrusion profiles.
7. Apply proactive techniques to prevent unwanted activities in networks and systems.

Topics

1. Kill Chain
2. MITRE ATT&CK/ATLAS frameworks
    a. Tactics Techniques and Procedures (TTPs)
    b. Manifestations of attacks
    c. Detection methods
3. Deep Packet Inspection
4. Log File Analysis (e.g., endpoint, access, DNS, netflow, HTTP, SMTP, SSL/TLS, application)
5. Telemetry data
6. Log Aggregation
7. Log enrichment using open data sources
8. Cross Log Comparison and Analysis
9. Anomaly Detection (e.g. Establishing profiles)
10. Anomaly algorithms
    a. Statistical Techniques
    b. Correlation Techniques
    c. Fuzzy Logic Approaches
    d. Artificial Intelligence
    e. Filtering Algorithms
    f. Neural Networks
11. Heuristic (signature) Detection
12. Specification-based Detection
13. Host-based Intrusion Detection and Prevention
    a. Behavioral Detection (file and process)

14. Network-based Intrusion Detection and Prevention
    a. Stealth mode
15. Distributed Intrusion Detection
16. Hierarchical IDSs
17. Cyber threat intelligence
18. Honeynets/Honeypots
19. Intrusion response
    a. Device Reconfiguration
    b. Notifications (e.g. Logging, SNMP Trap, Email, Visual/Audio Alert)
    c. Trace Recording
    d. Opening Application
    e. Session Interruption
    f. Reach back

Vocabulary

Anomaly Detection; Cyber Threat Intelligence; Distributed Intrusion Detection; Heuristic Detection; Host-based Intrusion Detection/Prevention; Honeynets/Honeypots; Intrusion Detection/Prevention Systems (IDS/IPS); Intrusion Response; Log Analysis; MITRE ATT&CK Framework; Network-based Intrusion Detection/Prevention; Specification-based Detection

Related Knowledge Units

Basic Networking (BNW); Network Defense (NDF); Network Technology and Protocols (NTP); Advanced Network Technology and Protocols (ANT); Network Security Administration (NSA); Wireless Sensor Networks (WSN)

Most Related DCWF and/or NICE Framework Work Role(s)

Defensive Cybersecurity, Incident Response, Forensics Analyst, Cyber Operations Planner, Communications Security (COMSEC) Management

Life-Cycle Security (LCS)

The intent of the Life-Cycle Security (LCS) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe the importance of secure software, programming best-practices, and the development processes and methodologies that lead to secure software.
2. List and 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

Vocabulary

Configuration Management; Developmental Threats; Life-Cycle Security (LCS); Maturity Model; Process Management; Project/Program Management; Secure Software; Software Assurance (SAS); Software Assurance Maturity Model; System Life-Cycle; Threat Modeling; Vulnerability Mapping

Related Knowledge Units

Software Assurance (SAS); Security Risk Analysis (SRA); Secure Programming Practices (SPP); Software Security Analysis (SSA); Vulnerability Analysis (VLA); QA/Functional Testing (QAT)

Most Related DCWF and/or NICE Framework Work Role(s)

Systems Requirements Planning, Software Test and Evaluation Specialist, AI Risk and Ethics Specialist, Software Security Assessment, Product Support Manager

Low Level Programming (LLP)

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

KU Learning Outcomes

To complete this KU, students will 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 (e.g., speed, size, efficiency, etc.).
2. Explain the risks and advantages that result from using low level programming.

Topics

1. Higher level language which allows low level access, such as C
2. Assembly
3. Secure use of library functions
4. Pointers and pointer manipulation
5. Modularization in low level programs
6. Defensive programming techniques
7. Compiling, assembling, and linking object files to create working programs
8. Assembly calls

Vocabulary

Assembly Calls; Assembly Language; Assembling; C Programming Language; Compiling; Defensive Programming; Linking; Low Level Programming (LLP); Modularization; Operating Systems Concepts (OSC); Pointers and Pointer Manipulation; Secure Library Functions

Related Knowledge Units

Operating Systems Concepts (OSC); Software Reverse Engineering (SRE); Software Security Analysis (SSA)

Most Related DCWF and/or NICE Framework Work Role(s)

Secure Software Development, Software Developer, DevSecOps Specialist, Data Officer, Digital Evidence Analysis

Media Forensics (MEF)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe methods and approaches for forensic analysis on specified media.
2. Apply forensics techniques to investigate and analyze a particular media in context.
3. Explain methods and approaches for forensics acquisition on specified media.

Topics

1. Media 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

Vocabulary

Authentication of Evidence; Full Imaging; Hashes; Hidden Files/Clusters/Partitions; Live Acquisition; Media Acquisition; Metadata; Slack Space; Sparse Imaging; Static Acquisition; Validation; Verification

Related Knowledge Units

Digital Forensics (DFS); Device Forensics (DVF); Host Forensics (HOF); Network Forensics (NWF)

Most Related DCWF and/or NICE Framework Work Role(s)

Digital Forensics, Digital Evidence Analysis, Forensics Analyst, Multi-Disciplined Language Analysis, Cyber Intelligence Planner

Mobile Technologies (MOT)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Understand and explain 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

Vocabulary

2G, 3G, 4G, 5G; Billing/Charging; Core Architecture Evolution; Encryption; Mobile Device Connectivity; Mobile Security; Mobile Systems; Network Infrastructure; RRC Signaling; Secure Voice and Data Access; SS7; Standards Heritage

Related Knowledge Units

Cloud Computing (CCO); Digital Communications (DCO); Device Forensics (DVF)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Workforce Developer and Manager, IT Program Auditor, DevSecOps Specialist, Cyber Instructional Curriculum Developer, Product Support Manager

Network Forensics (NWF)

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

KU Learning Outcomes

To complete this KU, students will 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.
3. Use tools that can share and automate network detection of malicious activity.

Topics

1. Packet Capture and Analysis (Wifi, LAN)
2. Network based security incidents investigation
3. Interlacing of device and network forensics
4. Log-file Analysis
5. Forensic Imaging and Analysis
6. Security Information and Event Management (SIEM)
7. Yara and Sigma rules for detection
8. MITRE ATT&CK/ATLAS frameworks
9. Cyber threat intelligence

Vocabulary

Anomalous Activity; Cyber Threat Intelligence; Forensic Imaging; Log File Analysis; Malicious Activity; MITRE ATT&CK/ATLAS Frameworks; Network Forensics; Network Traffic Analysis; Packet Capture; Security Incident Investigation; Security Information and Event Management (SIEM); Yara and Sigma Rules

Related Knowledge Units

Digital Forensics (DFS); Cyber Threat Hunting (CTH); Host Forensics (HOF); Digital Forensics (DFS); Device Forensics (DVF)

Most Related DCWF and/or NICE Framework Work Role(s)

Digital Forensics, Incident Response, Infrastructure Support, Cyber Defense Incident Responder, Data Analysis

Network Security Administration (NSA)

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

KU Learning Outcomes

To complete this KU, students will 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.
7. Discuss cybersecurity architecture, frameworks, and models to best meet the organization's business objectives.

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 cybersecurity 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

Vocabulary

Data Loss Prevention (DLP); Firewalls & Intrusion Detection/Prevention; Incident Response; Network Segmentation; Risk Assessment; Security Architecture; Security Auditing; Security Awareness & Training; Security Monitoring & Logging; Security Policies & Standards; Threat Modeling; Vulnerability Management

Related Knowledge Units
Basic Networking (BNW); Network Defense (NDF); Network Technology and Protocols (NTP); Advanced Network Technology and Protocols (ANT); Intrusion Detection/Prevention Systems (IDS); Wireless Sensor Networks (WSN)

Most Related DCWF and/or NICE Framework Work Role(s)
Cybersecurity Architecture, Secure Systems Development, Network Operations, Vulnerability Analysis, Cyber Crime Investigator

Network Technology and Protocols (NTP)

The intent of the Network Technology and Protocols (NTP) Knowledge Unit is to expand students' knowledge of networking to include an understanding of 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Demonstrate an understanding of layer 2 networking (Data Link layer).
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 (Network layer) of a network.
5. Demonstrate the use of multiple tools to analyze and troubleshoot wired and wireless networks.
6. Explain the weaknesses of WEP and which weaknesses have been addressed and how.

Topics

1. Network Switching (Ethernet)
    a. ARP and RARP
    b. OSI Model, Layer 2 and Layer 3 security issues
2. IPv4 suite and IPv4 Addressing
3. IPv6 suite and 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 (e.g. Netflow)
7. Protocol and packet analysis tools like Wireshark

Vocabulary

ARP; DNS; IPv4; IPv6; Layer 2 Security; Layer 3 Security; Network Analysis; Network Protocols; Network Security; Routing; Troubleshooting; Wireshark

Related Knowledge Units

Basic Networking (BNW); Network Defense (NDF); Advanced Network Technology and Protocols (ANT); Network Security Administration (NSA); Intrusion Detection/Prevention Systems (IDS); Wireless Sensor Networks (WSN)

Most Related DCWF and/or NICE Framework Work Role(s)

Data Operations Specialist, Defensive Cybersecurity, Cyber Policy and Strategy Planner, Enterprise Architect, AI/ML Specialist

Operating Systems Administration (OSA)

The intent of the Operating Systems Administration (OSA) Knowledge Unit is to provide students with skills to perform basic operations involved in system administration of operating systems.

KU Learning Outcomes

To complete this KU, students will be able to:

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

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
14. Host firewall and endpoint protection configuration

Vocabulary

Audit Capabilities; Authentication Policies; Backups; Command Line Interfaces; Configuration Management; Event Logging; Patches; Security Logs; Security Policy Development; System Restore; Updates; User Accounts

Related Knowledge Units

Operating Systems Hardening (OSH); Operating Systems Theory (OST); Pre-OS Boot Environment (PBE)

Most Related DCWF and/or NICE Framework Work Role(s)

Systems Administration, Program Manager, Cyber Defense Analyst, AI Adoption Specialist, Enterprise Architecture

Operating Systems Hardening (OSH)

The intent of the Operating Systems Hardening (OSH) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe, for a given OS, the steps necessary for hardening the OS and reduce the attack surface area.
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.
3. Leverage built-in OS capabilities and/or third-party applications to increase defensive posture.

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
12. Host Firewall Configuration
13. Secure Boot
14. Drive Encryption

Vocabulary

Attack Surface Reduction; Component Removal; File System Isolation; Host Firewall Configuration; Operating System Hardening (OSH); Patch Management; Password Policy; Port Management; Secure Installation; Service Management; User Access Control; Vulnerability Scanning

Related Knowledge Units

Operating Systems Administration (OSA); Operating Systems Theory (OST); Pre-OS Boot Environment (PBE)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Crime Investigator, Software Developer, Data Analyst, Cybersecurity Curriculum Development, System Administrator

Operating Systems Theory (OST)

The intent of the Operating Systems Theory (OST) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Understand operating systems theory and implementation.
2. 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
14. Zero-trust architecture
15. Micro segmentation and isolated environments

Vocabulary

Concurrency and Synchronization; Deadlocks; Distributed OS Architectures; File Systems; Input/Output; Inter-process Communications; Memory Management; Operating Systems Theory; Processes & Threads; Privilege States; Real-time Operating Systems; Virtual Memory

Related Knowledge Units

Operating Systems Administration (OSA); Operating Systems Hardening (OSH); Pre-OS Boot Environment (PBE)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Architecture, Software Security Assessment, Digital Evidence Analysis, Security Control Assessor, Communications Security (COMSEC) Management

Pre-OS Boot Environment (PBE)

The intent of the Pre-OS Boot Environment (PBE) Knowledge Unit is to provide students with an understanding of an entire ecosystem below the operating system including tools that interact with firmware within the OS environment and firmware capabilities to verify image integrity and boot integrity.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe the different stages of a boot environment before the Operating System loads.
2. Describe what capabilities exist to verify a device is loading a secure image or application.
3. Demonstrate the ability to turn off and turn on sub-components of a system within the BIOS/UEFI menu.

Topics

1. Chain of Trust and Root of Trust
2. Boot Integrity / Measured Boot
3. BIOS/UEFI and UEFI Customization
4. Secure Boot / Trusted Boot
5. Trusted Platform Module (TPM) and Trusted Computing Group (TCG)
6. Disabling/Enabling peripherals in BIOS/UEFI

Vocabulary

BIOS/UEFI; Boot Integrity; Chain of Trust; Measured Boot; Peripheral Disabling/Enabling; Pre-OS Boot Environment (PBE); Root of Trust; Secure Boot; Trusted Boot; Trusted Computing Group (TCG); Trusted Platform Module (TPM); UEFI Customization

Related Knowledge Units

Operating Systems Administration (OSA); Operating Systems Hardening (OSH); Operating Systems Theory (OST)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Intelligence Planner, Security Control Assessor, Product Designer User Interface (UI), Secure Systems Development, Cyber Operations Planner

Penetration Testing (PTT)

The intent of the Penetration Testing (PTT) Knowledge Unit is to provide students with methods and frameworks to discover ways of exploiting vulnerabilities and exploit them to gain access to a system. This is done within the legal and ethical confines of best practices in ethical hacking. Students will also learn ways to responsibly report vulnerabilities and countermeasures to the appropriate clients or companies (i.e. Bug Bounties).

KU Learning Outcomes

To complete this KU, students will be able to:

1. Plan, organize and perform penetration testing on a simple network.
2. Analyze security vulnerabilities of systems and networks.
3. Discuss post-exploitation techniques.
4. Describe how to use attack frameworks to identify attack surfaces for penetration testing.
5. Create a professional penetration testing report with results and findings.
6. Devise remediation and mitigation strategies to defend against attackers and threats.
7. Assess ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with those requirements.
8. Compare and contrast various network security assessment and hacking tools.

Topics

1. Penetration Test Methodologies and Frameworks (e.g., Flaw Hypothesis Methodology, OSSTMM)
2. Identifying vulnerabilities from documentation and source code analysis
3. Vulnerability Scanning
4. Understanding families of attacks
5. Understanding flaws that lead to vulnerabilities
6. Enumeration, foot printing
7. Attack Surface Discovery
8. Attack Vectors
9. Attack Frameworks (e.g., MITRE ATT&CK/ATLAS)
10. Exploitation and post-exploitation techniques
11. Ethical usage of penetration testing
12. Professional penetration testing reports
13. Penetration Testing Tools and Scripts (e.g., Metasploit, Kali Linux, etc.)
14. Open Source Intelligence (OSINT)
15. Passive/Active Reconnaissance

Vocabulary

Attack Frameworks; Attack Surface Discovery; Attack Vectors; Cybersecurity Ethics; Ethical Hacking; Exploitation Techniques; MITRE ATT&CK; OSINT (Open-Source Intelligence); Penetration Testing; Remediation Strategies; Vulnerability Analysis; Vulnerability Scanning

Related Knowledge Units

Network Defense (NDF); Vulnerability Analysis (VLA); Cybersecurity Ethics (CSE)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Architecture, Secure Systems Development, Defensive Cybersecurity, Incident Response, All-Source Collection Requirements Management

Privacy (PRI)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Examine concepts of privacy and confidentiality.
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 (PII)
2. Electronic Protected Health Information (ePHI)
3. 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
4. Privacy Impact Assessments
5. Anonymity and Pseudonymity
6. Privacy Policies, Laws and Regulations (e.g., GDPR and State laws)
7. Risks to Privacy
8. Tracking and Surveillance
9. Privacy tools
    a. Encryption
    b. VPNs
    c. Scramblers

Vocabulary

Anonymity; Confidentiality; ePHI (Electronic Protected Health Information); Encryption; FIPPs (Fair Information Practice Principles); GDPR (General Data Protection Regulation); PII (Personally Identifiable Information); Privacy; Privacy Impact Assessments; Pseudonymity; Surveillance; Tracking

Related Knowledge Units

Cybersecurity Principles (CSP); Policy, Legal, Ethics, and Compliance (PLE); Cybersecurity Ethics (CSE)

Most Related DCWF and/or NICE Framework Work Role(s)
Cyber Legal Advisor, Cybersecurity Legal Advice, Forensics Analyst, Privacy Compliance Manager, Multi-Disciplined Language Analyst

QA/Functional Testing (QAT)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Develop effective tests in a structured, organized manner.
2. Perform functional testing to demonstrate that security policies and software requirements are met.

Topics

1. Testing methodologies (e.g., unit testing, integration testing, system testing, acceptance testing, performance testing, security testing, white box, grey box, black box)
2. Test coverage analysis
3. Automatic and manual generation of test inputs
4. Test execution
5. Validation of results
6. Documentation of test results

Vocabulary

Acceptance Testing; Black Box; Functional Testing; Grey Box; Integration Testing; Performance Testing; Security Testing; System Testing; Test Coverage Analysis; Test Execution; Unit Testing; White Box

Related Knowledge Units

Life-Cycle Security (LCS); Software Assurance Security (SAS); Security Risk Analysis (SRA); Software Security Analysis (SSA); Vulnerability Analysis (VLA)

Most Related DCWF and/or NICE Framework Work Role(s)

Systems Security Management, Software Security Assessment, Cybersecurity Curriculum Development, Systems Testing and Evaluation, Secure Software Assessor

Radio Frequency Principles (RFP)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Understand and identify methods for isolating RF emissions.
2. Understand and 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

Vocabulary

Antennas; Bandwidth; BER (Bit Error Rate); Digital Modulation; Eb/No (Energy per bit to Noise power spectral density ratio); Information Modulation; Radio Frequency (RF) Electromagnetic Radiation; RF Emissions; RF Transmissions; S/N (Signal-to-Noise Ratio); Spectral Representation

Related Knowledge Units

Digital Communications (DCO); Wireless Sensor Networks (WSN)

Most Related DCWF and/or NICE Framework Work Role(s)

All-Source Collection Manager, Cyberspace Operations, Exploitation Analysis, Forensics Analyst, Cyber Policy and Strategy Planner

Secure Programming Practices (SPP)

The intent of the Secure Programming Practices (SPP) 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.

KU Learning Outcomes

To complete this KU, students will 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. Differentiate between memory safe and memory unsafe languages.
5. 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, and Bounds 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
5. Apply security practices to classes
    a. Don't allow external interfaces data changes by reference
    b. Use context to determine data access
    c. Support data updates verification
    d. Authenticate
6. Programming Flaws
    a. Buffer Overflows, Integer Errors
    b. Input Validation
    c. API Abuse
    d. Security Features
    e. Time and State
    f. Errors
    g. Code Quality
    h. Encapsulation
    i. Environment
7. Static Analysis
8. Data Obfuscation
9. Data Protection
10. Web Application Threats

11. Secure Programming paradigms
    a. Pair programming
    b. Code reviews
    c. Test-driven development

Vocabulary
Buffer Overflows; Data Obfuscation; Data Protection; Defensive Programming; Input Validation; Integer Errors; Memory Safety; Secure Programming Practices; Secure Programming Paradigms; Static Analysis; Vulnerabilities; Web Application Threats

Related Knowledge Units
Life-Cycle Security (LCS); Software Assurance Security (SAS); Security Risk Analysis (SRA); Software Security Analysis (SSA); Vulnerability Analysis (VLA); QA/Functional Testing (QAT)

Most Related DCWF and/or NICE Framework Work Role(s)
Cyber Crime Investigator, Cybersecurity Curriculum Development, Technical Support Specialist, Database Administrator, Information Systems Security Developer

Software Assurance (SAS)

The intent of the Software Assurance (SAS) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Apply secure-by-design principles.
2. Describe how system design and architecture affect 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

Vocabulary

Audit Trail; Design Reviews; Life of Data - N-order Scope Map; Modeling; Resiliency; Secure-by-design; Secure Design Patterns; Security Principles (e.g., Separation, Isolation, Encapsulation, Least Privilege); Security Requirements; Software Assurance (SAS); System Design and Architecture; Vulnerability Assessment

Related Knowledge Units

Life-Cycle Security (LCS); Security Risk Analysis (SRA); Secure Programming Practices (SPP); Software Security Analysis (SSA); Vulnerability Analysis (VLA); QA/Functional Testing (QAT)

Most Related DCWF and/or NICE Framework Work Role(s)

Cyber Intelligence Planner, System Administrator, Research and Development Specialist, AI Test and Evaluation Specialist, Cybersecurity Architecture

Software Reverse Engineering (SRE)

The intent of the Software Reverse Engineering (SRE) Knowledge Unit is to provide students with the capability to perform reverse engineering of executable code by following triage process using comment software reverse engineering tools to safely determine its function and effects, or to discover details of the implementation.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Apply common software reverse engineering tools to safely perform static and dynamic analysis of software of unknown origin for the purposes of understanding the software functionality and implementation.
2. Analyze malware using static, dynamic, code, and/or memory analysis techniques.

Topics

1. Reverse Engineering Tools and Techniques
   a Static analysis techniques and methodology
   b Dynamic analysis techniques and methodology
2. Sandboxing
3. Anti-reverse engineering techniques
4. Commercial software packers
5. Code disassembly
6. Memory Analysis tools

Vocabulary

Anti-Reverse Engineering; Code Disassembly; Commercial Software Packers; Dynamic Analysis; Implementation Details; Malware Analysis; Memory Analysis; Sandboxing; Software Functionality; Software Reverse Engineering (SRE); Static Analysis; Triage Process

Related Knowledge Units

Life-Cycle Security (LCS); Software Security Analysis (SSA); Vulnerability Analysis (VLA)

Most Related DCWF and/or NICE Framework Work Role(s)

Secure Software Development, Digital Forensics, Cyber Defense Forensics Analyst, Software Security Assessment, Defensive Cybersecurity

Software Security Analysis (SSA)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe software security analysis tools and techniques.
2. Apply 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

Vocabulary

Binary Code Analysis; Common Analysis Tools; Dynamic Analysis; Life-Cycle Security (LCS); QA/Functional Testing (QAT); Sandboxing; Software Reverse Engineering (SRE); Software Security Analysis (SSA); Source Code Analysis; Static Analysis; Testing Methodologies; Vulnerability Analysis (VLA)

Related Knowledge Units

Software Reverse Engineering (SRE); Life-Cycle Security (LCS); QA/Functional Testing (QAT); Vulnerability Analysis (VLA)

Most Related DCWF and/or NICE Framework Work Role(s)

Systems Security Management, Vulnerability Analysis, Technology Research and Development, Systems Security Analysis, Software Developer

Supply Chain Security (SCS)

The intent of the Supply Chain Security (SCS) 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.

KU Learning Outcomes

To complete this KU, students will 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. Offshore Production
3. Transport and Logistics of IT Components
4. Evaluation of 3rd-Party Development Practices
5. Cybersecurity risk in supply chain
6. Understanding of the Capabilities and Limits of Software and Hardware Reverse Engineering

Vocabulary

Cybersecurity Risk; Global Development; Hardware Development; Mitigation Strategies; Offshore Production; Outsourcing; Reverse Engineering; Security Issues; Software Development; Supply Chain Security (SCS); Third-Party Components; Transport and Logistics

Related Knowledge Units

Cybersecurity Planning and Management (CPM); Security Risk Analysis (SRA); Policy, Legal, Ethics, and Compliance (PLE); Security Program Management (SPM)

Most Related DCWF and/or NICE Framework Work Role(s)

Systems Security Analysis, Threat Analysis, AI Test and Evaluation Specialist, Secure Project Management, Enterprise Architecture

Systems Certification and Accreditation (SCA)

The intent of the Systems Certification and Accreditation (SCA) 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.

KU Learning Outcomes

To complete this KU, students will 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)

Vocabulary

Accreditation; Certification; Certification Boards and Panels; Components of the C&A Process; DoD Policies and Directives; DoD System Certification and Accreditation Processes; IA Compliance (IAC); NIST Risk Management Framework (SP800-37); Policy, Legal, Ethics, and Compliance (PLE); QA/Functional Testing (QAT); Roles/Players; Systems Certification and Accreditation (SCA)

Related Knowledge Units

IA Compliance (IAC); QA/Functional Testing (QAT); Policy, Legal, Ethics, and Compliance (PLE); Security Program Management (SPM)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Architecture, Systems Requirements Planning, Exploitation Analyst, All-Source Analyst, AI Test and Evaluation Specialist

Systems Programming (SPG)

The intent of the Systems Programming (SPG) 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.

KU Learning Outcomes

To complete this KU, students will 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. Develop 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 (e.g., C, Assembly)
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

Vocabulary

Application Programming Interfaces (APIs); Device Drivers; Hardware/software interfaces; Layered services design; Low-level programming languages; Memory management; Monitoring and logging; Operating Systems; Resource optimization; Runtime overhead minimization; Security concerns; Systems programs

Related Knowledge Units
Secure Programming Practices (SPP); Software Assurance (SAS); Software Security Analysis (SSA); Systems Certification and Accreditation (SCA); Systems Security Engineering (SSE)

Most Related DCWF and/or NICE Framework Work Role(s)
Security Control Assessor, Software Developer, AI Risk and Ethics Specialist, Software/Cloud Architect, AI Test and Evaluation Specialist

Systems Security Engineering (SSE)

The intent of the Systems Security Engineering (SSE) 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 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.

KU Learning Outcomes

To complete this KU, students will 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

Vocabulary

Emergent Properties; Make or Buy Analysis; Requirements Identification; System Components; System Design; System Implementation; System Life-cycle; System Operation/Maintenance; System Testing; Systems Integration; Systems Security Analysis; Systems Security Engineering (SSE)

Related Knowledge Units

Secure Programming Practices (SPP); Software Assurance (SAS); Software Security Analysis (SSA); Systems Certification and Accreditation (SCA); Systems Programming (SPG)

Most Related DCWF and/or NICE Framework Work Role(s)

Enterprise Architecture, Communications Security (COMSEC) Management, Secure Project Management, Secure Software Development, Secure Systems Development

Threat Intelligence (THI)

The intent of the Threat Intelligence (THI) Knowledge Unit is to provide students with the fundamentals and the use of threat hunting and tools, vulnerability assessment, incident analysis, incident response, forensics, and investigations of a cyber incidences.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Identify threat tactics and methodologies.
2. Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.
3. Apply signature development to perform packet-level analysis using appropriate tools.
4. Demonstrate ability to apply incident response and handling methodologies.
5. Demonstrate familiarity with legal and regulatory requirements with regard to incident handling.
6. Apply anomaly detection techniques to perform proactive threat hunting.
7. Apply appropriate threat packaging techniques to prepare and share threat reports.

Topics

1. Threat intelligence sources
2. Open-Source Threat Intelligence (OSINT)
3. Threat intelligence tools
4. Threat sharing standards
5. Threat intelligence at strategic, operational and tactical levels
6. Incident response fundamentals
7. Incident detection
8. Incident analysis and forensics
9. Incident handling and management
10. Legal and regulatory requirements

Vocabulary

Event Correlation; Forensics; Incident Analysis; Incident Response; Intrusion Detection; Legal and Regulatory Requirements; Open-Source Threat Intelligence (OSINT); Packet-Level Analysis; Signature Development; Threat Hunting; Threat Intelligence; Vulnerability Assessment

Related Knowledge Units

Cyber Crime (CCR); Digital Forensics (DFS); Policy, Legal, Ethics, and Compliance (PLE); Security Risk Analysis (SRA)

Most Related DCWF and/or NICE Framework Work Role(s)

Digital Forensics, Infrastructure Support, Insider Threat Analysis, Information Systems Security Developer, Data Analyst

Virtualization Technologies (VTT)

The intent of the Virtualization Technologies (VTT) 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.

KU Learning Outcomes

To complete this KU, students will be able to:

1. Describe the fundamental concepts of virtualization.
2. Compare and contrast the different virtualization architectures.
3. Discuss potential virtualization security risks and mitigation strategies.

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 and containers
7. Migration and snapshots
8. Virtual management layers
9. Digital Forensics in virtual environments
10. Security Risks and Considerations (e.g., VM Sprawl, Malware, VM Sandbox Escape)

Vocabulary

Digital Forensics (in virtual environments); Guest; Host; Hypervisor; Virtual Machine (VM); Virtual Network; Virtual Storage; Virtualization; Virtualization Architectures (e.g., Full, Para, Hosted); Virtualization Security; VM Escape; VM Sprawl

Related Knowledge Units

Cloud Computing (CCO); IA Architectures (IAA); Network Security Administration (NSA); Operating Systems Theory (OST)

Most Related DCWF and/or NICE Framework Work Role(s)

Cybersecurity Curriculum Development, System Administrator, Systems Developer, Security Control Assessor, Cyber Operations Planner

Vulnerability Analysis (VLA)

The intent of the Vulnerability Analysis (VLA) Knowledge Unit is to provide students with a thorough understanding of system vulnerabilities, including 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.

KU Learning Outcomes

To complete this KU, students will 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. Application/ software vulnerability
    b. Missconfigurations
    c. Buffer overflows, privilege escalation, rootkits
    d. Supply chain vulnerability
    e. Trojans/backdoors/viruses
    f. Social Engineering Vulnerabilities
    g. 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

Vocabulary

Application/Software Vulnerability; Buffer Overflows; Misconfigurations; Privilege Escalation; Rootkits; Social Engineering Vulnerabilities; Supply Chain Vulnerability; Taxonomy; Trojans/Backdoors/Viruses; Vulnerability Analysis (VLA); Vulnerability Characteristics; Vulnerability Mapping

Related Knowledge Units

Intrusion Detection/Prevention Systems (IDS); Life-Cycle Security (LCS); Penetration Testing (PTT); Software Assurance (SAS); Security Risk Analysis (SRA); Secure Programming Practices (SPP); Software Security Analysis (SSA); QA/Functional Testing (QAT); Threat Intelligence (THI)

Most Related DCWF and/or NICE Framework Work Role(s)

Security Control Assessment, Vulnerability Analysis, Research and Development Specialist, Secure Systems Development, Defensive Cybersecurity

Web Application Security (WAS)

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

KU Learning Outcomes

To complete this KU, students will be able to:

1. Examine concepts of web application technologies and associated security issues.
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

Vocabulary

Access Controls; AJAX; Authentication; Cross-Site Scripting (XSS); Encoding Schemes; HTTP Protocol; JSON; Session Management; SQL Injection; Web Application Architectures; Web Application Security (WAS); XML

Most Related DCWF and/or NICE Framework Work Role(s)

Software Security Assessment, Product Support Manager, Cybersecurity Architecture, Cyber Operations Planner, Security Control Assessor

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 their associated security issues.

KU Learning Outcomes

To complete this KU, students will 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. Analyze and propose 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

Vocabulary

Anti-Reverse Engineering Techniques; Code Disassembly; Dynamic Analysis; Implementation Details; Malware Analysis; Memory Analysis; Reverse Engineering Tools; Sandboxing; Software Functionality; Software Reverse Engineering (SRE); Static Analysis; Triage Process

Related Knowledge Units

Basic Networking (BNW); Network Defense (NDF); Network Technology and Protocols (NTP); Advanced Network Technology and Protocols (ANT); Network Security Administration (NSA); Radio Frequency Principles (RFP)

Most Related DCWF and/or NICE Framework Work Role(s)
Cybersecurity Architecture, IT Investment Portfolio Manager, Data Steward, Secure Software Development, Software Security Assessment