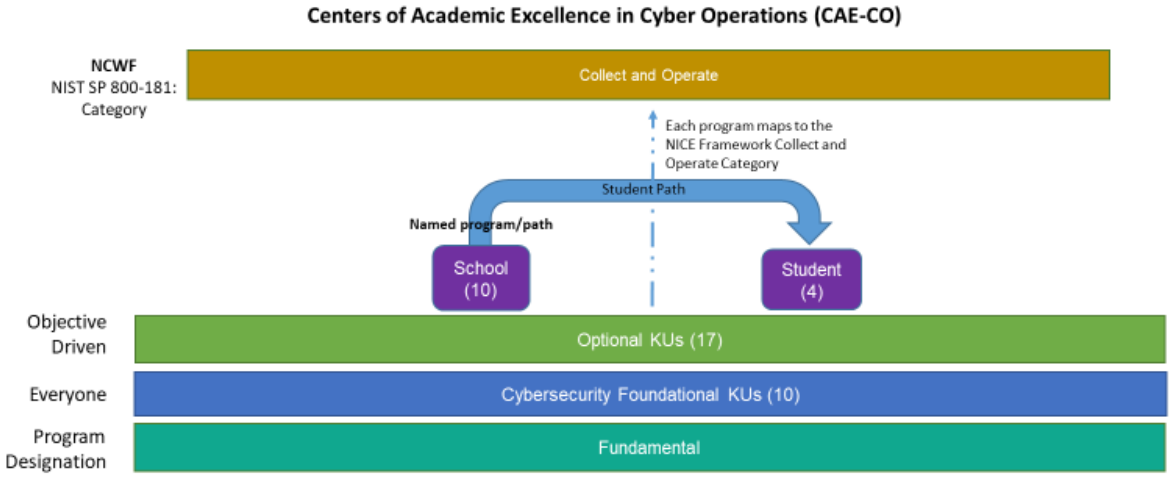
2021 CAE Cyber Operations (CAE-CO) Knowledge Units

Knowledge Unit Usage Notional Structure....3
Model KU Structure....4
Mandatory KU's....5
Mandatory- Low Level Programming Languages (LLP) (must include programming assignments to demonstrate that students are capable of the desired outcomes)....6
Mandatory- Software Reverse Engineering (SRE) (must include hands-on lab exercises)....7
Mandatory- Operating System Theory (OST)....8
Mandatory- Networking (must include hands-on lab exercises)....9
Mandatory- Cellular and Mobile Technologies....10
Mandatory- Discrete Math and Algorithms....11
Mandatory- Overview of Cyber Defense (must include hands-on lab exercises)....12
Mandatory- Security Fundamental Principles....13
Mandatory- Vulnerabilities....14
Mandatory- Legal and Ethics....15
Optional KU's....17
Optional- Programmable Logic (must include hands-on lab exercises)....18
Optional- Wireless Security (must include hands-on exercises)....19
Optional- Virtualization -> should be Virtualization (must include hands-on lab exercises)....20
Optional- Cloud Security/ Cloud Computing (CCO)....21
Optional- Risk Management of Information Systems....22
Optional- Computer Architecture (includes Logic Design)....23
Optional- Microcontroller Design (must include hands-on lab exercises)....24
Optional- Software Security Analysis (SSA) (must include hands-on lab exercises)....25
Optional- Secure Software Development (Building Secure Software) (must include hands-on lab exercises)....26
Optional- Embedded Systems (EBS) (must include hands-on lab exercises)....27
Optional- Digital Forensics (DFS) (must include hands-on lab exercises)....28
Optional- Systems Programming (SPG) (must include hands-on lab exercises)....29
Optional- Applied Cryptography....30
Optional- Industrial Control System (ICS)....31
Optional- User Experience (UX)/Human Computer Interface (HCI) Security....32
Optional- Offensive Cyber Operations....33
Optional- Hardware Reverse Engineering (HRE) (must include hands-on lab exercises)....34

Knowledge Unit Usage Notional Structure



Knowledge Units (KU):
Foundational: Low Level Programming, Software Reverse Engineering, Operating System Theory, Networking, Cellular and Mobile, Discrete Math and Algorithms, Overview of Cyber Defense, Security Fundamental Principles, Vulnerabilities, Legal and Ethics
Optional: Programmable Logic, Wireless Security, Virtualization, Cloud Security/Cloud Computing, Risk Management of Information Systems, Computer Architecture (includes Logic Design),Microcontroller Design, Software Security Analysis, Secure Software Development (Building Secure Software), Embedded Systems, Digital Forensics, Systems Programming, Applied Cryptography, Industrial Control Systems, User Experience (UX) Human Computer Interface (HCI) Security, Offensive Cyber Operations, Hardware Reverse Engineering

Model KU Structure

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

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

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

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

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

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

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

Mandatory KU's

Criterion 1 of the criteria for Measurement specifically addresses the academic requirements for the CAE-Cyber Operations Fundamental program. The academic requirements are based on Knowledge Units (KUs) (single or multiple courses, or course modules within single or multiple courses).

The program must include KUs covering 100% of the mandatory academic content and a minimum of 10 of the 17 optional academic content.

Students meeting the academic criteria for the institution's cyber operations program must complete coursework to meet all ten of the mandatory KUs and at least four of the optional KUs offered by the institution.

The Outcomes listed in each KU description are examples of the level of depth cyber operations students must demonstrate to meet the requirement.

Mandatory- Low Level Programming Languages (LLP) (must include programming assignments to demonstrate that students are capable of the desired outcomes)

Low level programming allows programmers to construct programs that interact with a system without the layers of abstraction that are provided by many high level languages. Proficiency in low-level programming languages is required to perform key roles in the cyber operations field (e.g., forensics, malware analysis, exploit development).

Outcomes

To complete this KU, students should be able to:

1. After completing the course content mapped to this knowledge unit, students will be able to develop low level programs with the required complexity and sophistication to implement exploits for discovered vulnerabilities.
2. Students will be able to write complex programs such as ones that implement a simple network stack. (C Language Programming)
3. Students will be able to write a functional, stand-alone assembly language program, such as a simple telnet client, with no help from external libraries. (Assembly Language Programming)

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. C Programming
2. Assembly Language Programming (for x86, ARM, MIPS, or PowerPC)

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Software Reverse Engineering (SRE) (must include hands-on lab exercises)

The discipline of reverse engineering provides the ability to deduce the design of a software component, to determine how something works (i.e., recover the software specification), discover data used by software, and to aid in the analysis of software via disassembly and/or decompilation. The ability to understand software of unknown origin or software for which source code is unavailable is a critical skill within the cyber operations field. Use cases include malware analysis and auditing of closed source software.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to use the tools mentioned above to safely perform static and dynamic analysis of software (or malware) of potentially unknown origin, including obfuscated malware, to fully understand the software's functionality.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Reverse engineering techniques
2. Reverse engineering for software specification recovery
3. Reverse engineering for malware analysis
4. Reverse engineering communications (to uncover communications protocols)
5. Deobfuscation of obfuscated code
6. Common tools for reverse engineering including but not limited to:
    - Disassemblers (e.g., IdaPro)
    - Debuggers (e.g., gdb, OllyDbg, WinDbg)
    - Virtualization-based sandbox environments (e.g., VMware, Xen)
    - Process and file activity monitors (e.g., ProcMon)
    - Network activity monitors (e.g., Wireshark, tcpdump, TcpView)

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Operating System Theory (OST)

Operating systems (OS) provide the platform on which running software acquires and uses computing resources. Operating systems are responsible for working with the underlying hardware to provide the baseline security capabilities of a system. Understanding the underlying theory of operating system design is critical to cyber operations as operating systems control the operation of a computer and the allocation of associated resources.

Outcomes

To complete this KU, students should be able to:

1. Students will have a thorough understanding of operating systems theory and implementation. They will be able to understand operating system internals to the level that they could design and implement simple architectural changes to an existing OS.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Privileged vs. non-privileged states; and transitions between them (domain switching)
2. Concurrency and synchronization (e.g., semaphores and locks)
3. Processes and threads, process/thread management, synchronization, inter-process communications
4. Memory management, virtual memory, hierarchical memory schemes
5. Uni-processor and multi-processor interface and support
6. CPU Scheduling
7. File Systems
8. IO issues (e.g., buffering, queuing, sharing, management)
9. Distributed OS issues (client/server, message passing, remote procedure calls, clustering)

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Networking (must include hands-on lab exercises)

Computer and communications networks are the very environment in which cyber operations are conducted. An understanding of these networks is essential to any discussion of cyber operations activities.

Outcomes

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

1. Students will have a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones. They will have a thorough knowledge of the major network protocols that enable communications and data transfer.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Routing, network, and application protocols including:
   - TCP/IP (versions 4 and 6)
   - ARP, BGP, SSL/TLS
   - DNS
   - SMTP
   - HTTP
2. Network architectures
3. Network security
4. Wireless network technologies
5. Network traffic analysis
6. Protocol analysis (examining component-to-component communication to determine the protocol being used and what it is doing)
7. Network mapping techniques (active and passive)

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Cellular and Mobile Technologies

As more communications are conducted via mobile and cellular technologies, these technologies have become critical (and continue to become more critical) to cyber operations. It is important for those involved in cyber operations to understand how data is processed and transmitted using these ubiquitous devices.

Outcomes

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

1. Students will be able to describe user associations and routing in a cellular/mobile network, interaction of elements within the cellular/mobile core, and end-to-end delivery of a packet and/or signal and what happens with the hand-off at each step along the communications path. They will be able to explain differences in core architecture between different generations of cellular and mobile network technologies.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Overview of smart phone technologies
2. Overview of embedded operating systems (e.g., iOS, Android)
3. Wireless technologies (mobile: GSM, WCDMA, CDMA2000, LTE; and Internet: 802.11b/g/n)
4. Infrastructure components (e.g., fiber optic network, evolved packet core, PLMN)
5. Mobile protocols (SS7, RR, MM, CC)
6. Mobile logical channel descriptions (BCCH, SDCCH, RACH, AGCH, etc.)
7. Mobile registration procedures
8. Mobile encryptions standards
9. Mobile identifiers (IMSI, IMEI, MSISDN, ESN, Global Title, E.164)
10. Mobile and Location-based Services

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Discrete Math and Algorithms

In order for cyber operators to make educated choices when provided with an array of algorithms and approaches to solving a particular problem, there are essential underlying concepts drawn from discrete mathematics, algorithms analysis, and finite automaton with which they should be familiar.

Outcomes

To complete this KU, students should be able to:

1. Given an algorithm, a student will be able to determine the complexity of the algorithm and cases in which the algorithm would/would not provide a reasonable approach for solving a problem.
2. Students will understand how variability affects outcomes, how to identify anomalous events, and how to identify the meaning of anomalous events.
3. Students will understand how automata are used to describe computing machines and computation, and the notion that some things are computable and some are not. They will understand the connection between automata and computer languages and describe the hierarchy of language from regular expression to context free.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Searching and sorting algorithms
2. Complexity theory
3. Regular expressions
4. Computability
5. Mathematical foundations for cryptography
6. Entropy

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Overview of Cyber Defense (must include hands-on lab exercises)

Cyber operations encompass both offensive and defensive operations. Defensive operations are essential in protecting our systems and associated digital assets. Understanding how defense compliments offense is essential in a well-rounded cyber operations program.

Outcomes

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

1. Students will have a sound understanding of the technologies and methods utilized to defend systems and networks. They will be able to describe, evaluate, and operate a defensive network architecture employing multiple layers of protection using technologies appropriate to meet mission security goals.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Identification of reconnaissance operations
2. Anomaly/intrusion detection
3. Anomaly identification
4. Identification of command and control operations
5. Identification of data exfiltration activities
6. Identifying malicious code based on signatures, behavior and artifacts
7. Network security techniques and components (e.g., firewalls, IDS, etc.)
8. Cryptography (include PKI cryptography) and its uses in cybersecurity
9. Malicious activity detection
10. System security architectures and concepts
11. Defense in depth
12. Trust relationships
13. Distributed/Cloud
14. Virtualization

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Security Fundamental Principles (i.e., "First Principles")

The first fundamental security design principles are the foundation upon which security mechanisms (e.g., access control) can be reliably built. They are also the foundation upon which security policies can be reliably implemented. When followed, the first principles enable the implementation of sound security mechanisms and systems. When not completely followed, the risk that an exploitable vulnerability may exist is increased. A solid understanding of these principles is critical to successful performance in the cyber operations domain.

Outcomes

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

1. Students will possess a thorough understanding of the fundamental principles underlying cyber security, how these principles interrelate and are typically employed to achieve assured solutions, the mechanisms that may be built from or due to these principles.
2. Given a particular scenario, students will be able to identify which fundamental security design principles are in play, how they interrelate and methods in which they should be applied to develop systems worthy of trust.
3. Students will understand how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. General Fundamental design principles including:
   Simplicity
   Open Design
   Design for Iteration
   Least Astonishment
2. Security Design Principles including:
   Minimize Secrets
   Complete Mediation
   Fail-safe Defaults
   Least Privilege
   Economy of Mechanism
   Minimize Common Mechanism
   Isolation, Separation and Encapsulation
3. Methods for Reducing Complexity including:
   Abstraction
   Modularity
   Layering
   Hierarchy

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Vulnerabilities

Vulnerabilities are not random events, but follow a pattern. Understanding the pattern of vulnerabilities and attacks can allow one to better understand protection, risk mitigation, and identify vulnerabilities in new contexts. Vulnerability analysis and it's relation to exploit development are core skills for one involved in cyber operations.

Outcomes

To complete this KU, students should be able to:

1. Students will possess a thorough understanding of the various types of vulnerabilities (design and/or implementation weaknesses), their underlying causes, their identifying characteristics, the ways in which they are exploited, and potential mitigation strategies. They will also know how to apply fundamental security design principles during system design, development and implementation to minimize vulnerabilities.
2. Students will understand how a vulnerability in a given context may be applied to alternative contexts and to adapt vulnerabilities so that lessons from them can be applied to alternative contexts.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Vulnerability taxonomies such as CVE, CWE, OSVDB, and CAPEC
2. Buffer overflows
3. Privilege escalation attacks
4. Input validation issues
5. Password weaknesses
6. Trust relationships
7. Race conditions
8. Numeric over/underflows
9. User-space vs. kernel-space vulnerabilities
10. Local vs. remote access

NICE Framework Categories

Collect and Operate (CO)

Mandatory- Legal and Ethics

People working in cyber operations must comply with many laws, regulations, directives and policies. Cyber operations professionals should fully understand the extent and limitations of their authorities to ensure operations in cyberspace are in compliance with U.S. law. In addition, cyber operators must have knowledge of cyber ethics for both understanding and applying moral reasoning models to address current and emerging ethical dilemmas on an individual and society.

Outcomes

To complete this KU, students should be able to:

1. Given a cyber operations scenario, students will be able to explain the authorities applicable to the scenario.
2. Students will be able to provide a high-level explanation of the legal issues governing the authorized conduct of cyber operations and the use of related tools, techniques, technology, and data.
3. Students will be able to evaluate the relationship between ethics and law, describe civil disobedience and its relation to ethical hacking, describe criminal penalties related to unethical hacking, and apply the notion of Grey Areas to describing situations where law has not yet caught up to technological innovation.
4. Students will be able to describe steps for carrying out ethical penetration testing, describe 'ethical hacking' principles and conditions, distinguish between ethical and unethical hacking, and distinguish between nuisance hacking, activist hacking, criminal hacking, and acts of war.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. International Law
   Jus ad bellum
      United Nations Charter
   Jus in bello
      Hague Conventions
      Geneva Conventions
2. U.S. Laws
   Constitution
      Article I (Legislative Branch)
      Article II (Presidency)
      Article III (Judiciary)
      Amendment 4 (Search and Seizure)
      Article 14 (Due Process)
   Statutory Laws
   Title 10 (Armed Forces)
   Title 50 (War and National Defense)
   Title 18 (Crimes)
      18 SC 1030 (Computer Fraud and Abuse Act)
      18 SC 2510-22 Electronic Communications Privacy Act
      18 SC 2701-12 Stored Communications Act
      18 USC 1831-32 Economic Espionage Acts

3. Cyber Ethics
   Professional Ethics and Codes of Conduct
   Social Responsibility
   Ethical Hacking

NICE Framework Categories

Collect and Operate (CO)

Optional KU's

At least 10 of the following 17 optional knowledge units must exist in the institutions curriculum and be available to all students during their required course of study. For students to qualify for recognition of completing the cyber operations program they must take courses that meet at least 4 of the institution's mapped 10+ Optional KUs.

Optional- Programmable Logic (must include hands-on lab exercises)

In digital electronic systems, logic devices provide specific functions, including device-to-device interfacing, data communication, signal processing, data display, timing and control operations, and several other system functions. Logic devices can be fixed, or programmable using a logic language. The advantage of a programmable logic device (PLD) is the ability to use a programmable logic language to implement a design into a PLD and immediately test it in a live circuit.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to specify digital device behavior using programmable logic language. They will be able to design, synthesize, simulate, and implement logic on an actual programmable logic device. For instance, students will be able to perform parallel computational tasks such as taking multiple cipher cores and running them in parallel to perform password cracking attacks.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Hardware design/programming languages (e.g. VHSIC Hardware Design Language (VHDL), Verilog, OpenCL)
2. Programmable logic devices (Programmable Logic Controllers (PLC), Fully Programmable Gate Arrays (FPGA))

Optional- Wireless Security (must include hands-on exercises)

Wireless systems are essential to enabling mobile users. However, a significant impact in security can result from the use of wireless or the improper configuration of wireless security due to the erratic nature of the wireless environment. The dynamic and inconsistent connectivity of wireless requires unique approaches to networking in everything from user identification and authentication to message integrity and cipher synchronization.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to describe the unique security and operational attributes in the wireless environment and their effects on network communications. They will be able to identify the unique security implications of these effects and how to mitigate security issues associated with them.
2. Students will be able to describe and demonstrate the vulnerabilities with ineffective mechanisms for securing or hiding 802.11 traffic.
3. Students will be able to understand, describe, and implement a secure wireless network that uses modern encryption and enforces the proper authentication of users.
4. Students will be able to compare and contrast mechanisms for association and authentication with a GSM BSC and a UMTS RNC.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. A comparison of security implementations in different wireless technologies (e.g., 2G/3G/4G/Wi-Fi/Bluetooth/RFID)
2. Confidentiality, integrity and availability policy enforcement considerations in wireless networks
3. Enumeration issues and methods to limit exposing and identifying cellular, enterprise, device and personal wireless identifiers (e.g. WLAN and cellular beacons, System Information Reports, TMSI)
4. Security protocols used in wireless communications and how each addresses issues of authentication, integrity, and confidentiality (e.g. COMP128, UIA, TKIP, CCMP, SSP, E1)
5. Availability issues in wireless and nuances in different denial-of-service attacks (e.g. energy jamming, carrier sense exploitation, RACH flooding, access management protocol exploitation)
6. Security issues in hardware and software architectures of wireless devices
7. Common ciphers, their implementations, advantages and disadvantages for use in securing wireless networks
    - Stream ciphers (e.g. E0, RC4, A5, SNOW, ZUC)
    - Block ciphers (e.g. Kasumi, SAFER, AES)

Optional- Virtualization - > should be Virtualization (must include hands-on lab exercises)

Virtualization technology has rapidly spread to become a core feature of enterprise environments, and is also deeply integrated into many server, client, and mobile platforms. It is also widely used in IT development, research, and testing environments. Virtualization is also a key technology in cyber security. As such a deep technical understanding of the capabilities and limitations of modern approaches to virtualization is critical to cyber operations.

Outcomes

To complete this KU, students should be able to:

1. Students will understand and be able to describe the technical mechanisms by which virtualization is implemented in a variety of environments, and their implications for cyber operations.
2. Students will be able to enumerate and describe the various interfaces between the hypervisors, VMs, physical and virtual hardware, management tools, networking, storage, and external environments.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Type I and Type II architectures.
2. Virtualization Principles including efficiency, resource control and equivalence
3. Virtualization techniques for code execution, including trap and emulate, binary translation, paravirtualization, and hardware-supported virtualization (e.g., Intel VMX).
4. Management of memory in virtualized systems, including hardware supported memory management (e.g. EPT/SLAT), memory deduplication, and isolation of VM hypervisor and memory spaces
5. Techniques for allocating storage (e.g., hard drives) to Virtual Machines, and the associated capabilities (e.g., snapshots).
6. Techniques for associating hardware (virtual or physical) with virtual machines, including hardware-supported methods (e.g., SR-IOV) and device emulation.
7. Techniques for providing advanced virtualization capabilities, such as live-migration and live-failover.
8. Internal and External Interfaces provided by virtualized platforms for management, monitoring, and internal communication/synchronization.
9. Snapshots, migration, failover

Note: Education focused on simply using VMs or virtualization platforms/tools (such as vSphere, HyperV, or VirtualBox) for efficiency purposes (e.g. server consolidation) is not sufficient to address this KU.

Optional- Cloud Security/ Cloud Computing (CCO)

Cloud resources are commonly used for a wide variety of use cases, including the provision of enterprise services, data processing and analysis, development and testing, and a wide variety of consumer focused services. As such it is important that the students have a clear understanding of the variety, complexity, and capabilities of modern cloud platforms. Cloud computing has implications for cyber operations not only as a potential target, but also as an extensive resource to bring relatively cheap computing power to solve problems (e.g. cracking passwords) which would have been more difficult pre-cloud.

Outcomes

To complete this KU, students should be able to:

1. Students will understand and be able to describe a variety of cloud service models and deployment modes, and select appropriate service models and delivery modes for a variety of potential workloads, including enumerating the security tradeoffs associated with their selections.
2. Students will be able to develop and deploy a workload in an appropriate cloud environment, including addressing issues associated with deployment, configuration, management, scalability, and security.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Cloud infrastructure components and the interfaces they expose. This should include public/consumer facing interfaces (such as public management APIs) and internal interfaces (such as those to provide automated backup, failover, and accounting)
2. Essential Characteristics of Cloud Platforms and an understanding of the technologies that enable these characteristics
3. Common Service models
4. Common Deployment Modes (e.g. public cloud, private cloud, hybrid cloud) and the associated tradeoffs (e.g. privacy/scalability/resilience)
5. Cloud infrastructure components and the interfaces they expose. This should include public/consumer facing interfaces (such as public management APIs), and internal interfaces (such as those to provide automated backup, failover, and accounting)
6. Techniques for deploying and scaling cloud resources (such as Puppet/Chef)
7. Security implication of cloud resources, including issues associated with shared resources and multi-tenancy, the extension of trust to include the cloud provider, and approaches to mitigating these issues
8. Developing, deploying, and managing applications on cloud resources, which should include hand-on exercises that utilize real cloud services

Recommended Resource for this KU: NIST 800-145

Optional- Risk Management of Information Systems

Risk Management of Information Systems is a critical topic area which forms the basis for applying information system security principles to an operational environment. Risk Management decisions are the embodiment of the organization's security culture and values as demonstrated through the willingness to commit resources to information system security capabilities.

Given the significant and growing danger of cyber security threats, it is imperative that all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to identify, measure (quantitative and qualitative), and mitigate key information technology risks.
2. Students will also be able to describe each of the tasks associated with risk framing, assessment, response and monitoring.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Risk Models (e.g. NIST SP 800-39 Managing Information Security Risk)
2. Risk Processes (e.g. NIST SP 800-37 Risk Management Framework)

Optional- Computer Architecture (includes Logic Design)

This knowledge unit ensures students understand the components that comprise a computing system and possess the ability to assess processor design and organization alternatives as they impact functionality and performance of a system.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to define devices of electronic digital circuits and describe how these components are interconnected. They will be able to integrate individual components into a more complex digital system and understand the data path through a CPU.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Organization of computer and processor architectures
2. Instruction set design alternatives
3. Processor implementation
4. Memory system hierarchy
5. Buses
6. I/O systems
7. Factors affecting performance

Optional- Microcontroller Design (must include hands-on lab exercises)

A microcontroller (or MCU, short for microcontroller unit) is a small, simple computer on a single integrated circuit containing a processor core, limited memory, and programmable input/output peripherals and sensors. Microcontrollers are typically inexpensive and have little or no interface for human interaction. They are typically programmed for a fixed function with little or no change over their lifecycle.

Outcomes

To complete this KU, students should be able to:

1. Students are knowledgeable of the concepts, methods, techniques, technologies, requirements, and development tools commonly used in the design and implementation of microcontroller applications. They will be able to develop or make a substantial modification to a simple microcontroller-based system and identify the cyber concerns associated with such a system.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Typical instruction sets and architectures
2. Common programming environments for microcontrollers
3. How the real-time requirements and simple architecture of the typical microcontroller require special programming considerations
4. Cyber considerations and issues related to microcontrollers and the larger systems they are typically integrated into

Optional- Software Security Analysis (SSA) (must include hands-on lab exercises)

This knowledge unit ensures that students will possess the ability to analyze software for the presence of weaknesses that may lead to exploitable vulnerabilities in operational systems.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to perform analysis of existing source code for functional correctness. Through the application of testing methodologies, students should be able to build test cases that demonstrate the existence of vulnerabilities. For example, students could apply industry standard tools that analyze software for security vulnerabilities.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Source code analysis
2. Binary code analysis
3. Static code analysis techniques
4. Dynamic code analysis techniques
5. Testing methodologies (Black Box/White Box/Fuzz)

Optional- Secure Software Development (Building Secure Software) (must include hands-on lab exercises)

This knowledge unit ensures that students know how to write robust, secure software. These methods taught in this class should lead to software that maintains the Confidentiality, Integrity and Availability of the software and data.

Outcomes

To complete this KU, students should be able to:

1. Students should be able to demonstrate that they understand the techniques specifying program behavior, the classes of well-known defects, and how they manifest themselves in various languages.
2. Students will understand how poor coding affects security and can identify common coding errors. Students will demonstrate that they are capable of authoring programs that are free from defects and can document their code with clear and succinct explanations, so other people can enhance and maintain the developed code.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Secure programming principles and practices
2. Constructive techniques (What process might provide for "good code.")

Optional- Embedded Systems (EBS) (must include hands-on lab exercises)

An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It includes a microprocessor, memory, and peripherals either packaged as an SOC or as separate components within the device. It is embedded as part of a complete device often including hardware and mechanical parts. It typically has more robust user interaction than a microcontroller. The embedded system's function typically changes very little, if at all, over the lifecycle of an instance of the system. Examples of embedded systems would include a wireless router or military weapons systems.

Outcomes

To complete this KU, students should be able to:

1. Students are knowledgeable of the concepts, methods, techniques, technologies, requirements, and development tools commonly used in the design and implementation of embedded systems. They will be able to develop or make a substantial modification to a simple embedded system and identify the cyber concerns associated with such an embedded system.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Typical instruction sets and architectures
2. Common operating systems and programming environments for embedded systems
3. How the real-time requirements typical of embedded systems require differences in the OS & applications
4. Cyber considerations and issues related to embedded systems

Optional- Digital Forensics (DFS) (must include hands-on lab exercises)

Digital forensics is the recovery and investigation of material found in various cyber environments (e.g. networks, memory, operating systems, etc.). The focus of this KU is on the digital forensics process and technology (tools and techniques) not the legal aspect (such as chain of custody or preparing evidence for court).

Outcomes

To complete this KU, students should be able to:

1. Students will be able to understand a user's activity, determine the manner in which an operating system or application has been subverted, recover "deleted" and/or intentionally hidden information from various types of media, and demonstrate proficiency with handling a large number of different kinds of devices.
2. Students will be able to understand how to identify forensic artifacts left by attacks.
3. Students will be able to understand how to acquire a forensically sound image.

Topics

To complete this KU, broad coverage of all the below topics and in-depth coverage, including hands-on-experience, of at least one of the below topics must be covered:

1. Operating system forensics
2. Device/Media forensics
3. Network forensics
4. Memory forensics

Optional- Systems Programming (SPG) (must include hands-on lab exercises)

This knowledge unit ensures that students will be proficient in programming systems software (i.e., software that interacts with the system hardware and/or other low-level system components that interact with the hardware). Systems programming usually uses a low-level programming language (e.g., C, assembly) that allows efficient use of core resources. Systems programming is sufficiently different from applications programming such that programmers tend to specialize in one or the other.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to build and integrate kernel modules, understand the system call mechanism and how malicious software subverts system calls. They should demonstrate sufficient knowledge of the networking stack to be able to construct network filter components. They will also be able to discuss strengths and weaknesses of alternative processors and demonstrate familiarity of tool sets for making use of alternative processors (e.g., GPUs).

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Kernel modules
2. Device drivers
3. Multi-threading
4. Use of alternate processors (e.g., graphics card processors)

Optional- Applied Cryptography

In cyber operations it is critical to understand the role of keys, cryptographic algorithms, and protocols as they relate to security (attacks and defenses) in complex real-life systems.

Outcomes

To complete this KU, students should be able to:

1. Students will be able to identify the appropriate uses of symmetric and asymmetric encryption. They will be able to assign some measure of strength to cryptographic algorithms and the associated keys.
2. Students will understand the common pitfalls or shortcomings associated with the implementation of cryptography, and will understand the challenges and limitations of current key management systems.
3. Given an enterprise architecture scenario consisting of different components (e.g. servers, clients, databases) with information that has various temporal and distribution constraints, networks, multiple sites, and trusted and untrusted clients, students will describe the appropriate cryptographic tools/algorithms/protocols that can be applied at various locations throughout that architecture in order to achieve a variety of goals, and the management challenges/tradeoffs associated with their choices.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Cryptographic primitives (e.g. randomization)
2. Symmetric and asymmetric cryptography, hash functions and data integrity, public-key encryption and digital signatures, key establishment and key management
3. The appropriate application of different types of cryptography to Internet security, computer security and communications security

Optional- Industrial Control System (ICS)

ICSs are crucial to the operations of U.S. critical infrastructures that are often widely deployed, interconnected and mutually dependent systems. ICSs can include Supervisory Control and Data Acquisition (SCADA) systems and Distributed Control Systems (DCS), and other control system configurations. Several infrastructures that use ICSs have critical national security impact including electric, water and wastewater, oil and natural gas, transportation, chemical, and aerospace. Cyber operators should have knowledge of the attack and defense of ICSs.

Outcomes

To complete this KU, students should be able to:

1. Students will have an overall comprehension of key U.S. infrastructures controlled by ICS including the associated vulnerabilities associated with each infrastructure.
2. Students will be able to describe how embedded systems are employed in industrial infrastructures and control systems. They will be able to identify means for capturing instrument telemetry and identifying feedback controls. They should be able to describe methods for managing distributed nodes and identify potential security vulnerabilities associated with the use of such systems and means for mitigating these vulnerabilities.
3. Students will be able to demonstrate the ability to discover and understand an ICS environment and identify the attack surface.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. SCADA
2. DCS
3. Vulnerabilities, countermeasures and attacks of ICS ecosystems

Optional- User Experience (UX)/Human Computer Interface (HCI) Security

HCI is the practice and study of human interaction with machines. This includes usability, machine interaction design, and psychological reactions to the interface. UX deals with the entirety of the user experience relative to a product (not just the user interface). UX includes HCI but also encompasses the emotional, physical, and behavioral perception of a product or service. Cyber security professionals must acknowledge that while they need to give utmost precedence to system security, they cannot overlook user experience, and vice versa.

Outcomes

To complete this KU, students should be able to:

1. Students will understand user interface issues that will affect the implementation of and perception of security mechanisms and the behavioral impacts of various security "policies."
2. Students will understand the tension between user security and convenience which results in user behavior that undermines system security. Students will learn how to develop approaches which have the right balance.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Authentication interfaces and passwords
2. Implicit and explicit policies in systems
3. Policies that users control and hidden policies controlled by the system
4. The role of social engineering and how it continues to be the primary attack vector
5. How implementing security affects the user experience.

Optional- Offensive Cyber Operations

Offensive cyber operations is everything related to reconnaissance and exploitation in the cyber space offensive mission. This knowledge unit provides a high-level overview of the different phases of cyber operations including target identification, reconnaissance, fingerprinting, development of operational plans, decision authorities/authorization, execution, and assessment.

Outcomes

To complete this KU, students should be able to:

1. Students will understand the phases of a cyber operation, what each phase entails, who has authorities to conduct each phase, and how operations are assessed after completion.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Cyber attacks are restricted to military members of DoD, as restricted by international law. Authorities are derived from U.S. Code Title 10.
2. Cyber kill chain
3. Mission planning and execution process
4. Define mission objectives and desired effects from the overall mission standpoint
5. The different phases of cyber operations

Optional- Hardware Reverse Engineering (HRE) (must include hands-on lab exercises)

Hardware Reverse Engineering is the study of hardware hacking and reverse engineering approaches that are routinely used against electronic devices and embedded systems. This knowledge unit provides students with an introduction to the basic procedures necessary to perform reverse engineering of hardware components to determine their functionality, inputs, outputs, and stored data.

Outcomes

To complete this KU, students should be able to:

1. Students will understand basic fundamental procedures such as probing, measuring, and data collection to identify functionality and to affect modifications to the hardware functionality.
2. Students will understand the proper use of evaluation tools and common hardware attack vectors.

Topics

To complete this KU, specific topics to be covered in this knowledge unit include, but are not limited to:

1. Hardware reverse engineering methodology
2. The use of tools and test measurement equipment
3. Circuit board analysis and modification
4. Embedded security
5. Common hardware attack vectors