# University of Idaho
## Bachelor of Science in Cybersecurity

<table>
<thead>
<tr>
<th>Freshman Fall</th>
<th>Freshman Spring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CYB 110</strong> Cybersecurity and Privacy <strong>CSP, CSF, PLE, PRI</strong></td>
<td><strong>CS 120</strong> Computer Science I <strong>BSP</strong></td>
</tr>
<tr>
<td><strong>CS 112</strong> Computational Thinking</td>
<td><strong>Math 176</strong> Discrete Math</td>
</tr>
<tr>
<td><strong>ISEM 101</strong> Integrated Seminar</td>
<td><strong>Comm 101</strong> Fundamentals of Public Speaking</td>
</tr>
<tr>
<td><strong>ENGL 102</strong> College Writing &amp; Rhetoric</td>
<td><strong>Phil 103</strong> Ethics</td>
</tr>
<tr>
<td><strong>ELECTIVE</strong> Hum/Social Science</td>
<td><strong>ELECTIVE</strong> Science Elective w/Lab</td>
</tr>
<tr>
<td><strong>Total Credits</strong> 15</td>
<td><strong>Total Credits</strong> 16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sophomore Fall</th>
<th>Sophomore Spring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CS 121</strong> Computer Science II</td>
<td><strong>CS 270</strong> System Software</td>
</tr>
<tr>
<td><strong>CS 150</strong> Computer Organization &amp; Arch.</td>
<td><strong>CS 240</strong> Operating Systems <strong>OSC, OTH</strong></td>
</tr>
<tr>
<td><strong>CYB 210</strong> Cybersecurity Management <strong>CPM, SPM, ISC</strong></td>
<td><strong>CYB 220</strong> Secure Coding and Analysis <strong>SPP, SSA, QAT</strong></td>
</tr>
<tr>
<td><strong>ELECTIVE</strong> Hum/Social Science</td>
<td><strong>ELECTIVE</strong> Science Elective w/Lab</td>
</tr>
<tr>
<td><strong>MATH 160 or 170</strong> Survey of Calculus or Calc I</td>
<td><strong>STAT 251 or 301</strong> Statistical Methods</td>
</tr>
<tr>
<td><strong>Total Credits</strong> 16</td>
<td><strong>Total Credits</strong> 16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Junior Fall</th>
<th>Junior Spring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CYB 310</strong> Intermediate Cybersecurity (was <strong>CS 336</strong>) <strong>CTH, BCY, IAA</strong></td>
<td><strong>CS 383</strong> Software Engineering</td>
</tr>
<tr>
<td><strong>ISEM 301</strong> Great Issues Seminar</td>
<td><strong>CYB 340</strong> Network Defense (was <strong>CS 438</strong>) <strong>NDF, IDS</strong></td>
</tr>
<tr>
<td><strong>CYB 330</strong> Networking Fundamentals <strong>BNW, NTP</strong></td>
<td><strong>CYB 350</strong> Operating System Defense <strong>OSH, OSA, BCO</strong></td>
</tr>
<tr>
<td><strong>CYB 380</strong> Cybersecurity Lab I</td>
<td><strong>CYB 381</strong> Cybersecurity Lab II (was <strong>CS 439</strong>)</td>
</tr>
<tr>
<td><strong>ELECTIVE</strong> Free Electives</td>
<td><strong>ELECTIVE</strong> Free Electives</td>
</tr>
<tr>
<td><strong>ENGL 317</strong> Technical Writing</td>
<td><strong>ELECTIVE</strong> Hum/Social Science</td>
</tr>
<tr>
<td><strong>Total Credits</strong> 16</td>
<td><strong>Total Credits</strong> 15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Senior Fall</th>
<th>Senior Spring</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CYB 401</strong> Cybersecurity Professional Development (can be CS 400)</td>
<td><strong>CYB 440</strong> Software Vulnerability Analysis <strong>SAS, VLA</strong></td>
</tr>
<tr>
<td><strong>CYB 420</strong> Computer and Network Forensics (was <strong>CS 447</strong>) <strong>DFS, HOF, NWF</strong></td>
<td><strong>CYB 481</strong> Senior Capstone Design II</td>
</tr>
<tr>
<td><strong>CYB 480</strong> Senior Capstone Design I</td>
<td><strong>ELECTIVE</strong> Hum/Social Science</td>
</tr>
<tr>
<td><strong>ELECTIVE</strong> Free Electives</td>
<td><strong>ELECTIVE</strong> Free Electives</td>
</tr>
<tr>
<td><strong>ELECTIVE</strong> Hum/Social Science</td>
<td><strong>ELECTIVE</strong> Hum/Social Science</td>
</tr>
<tr>
<td><strong>Total Credits</strong> 13</td>
<td><strong>Total Credits</strong> 13</td>
</tr>
</tbody>
</table>

Courses in **RED** are new Cybersecurity Courses
Courses in **BLUE** are modified existing CS courses
Foundational KU are in **BOLD Underline GREEN**
Core Technical KU are in **Underlined RED**
Core Non-technical KU are **Underline Brown**
Other Optional KUs are in **Purple**

Outcomes:

- Describe the fundamental concepts of the cybersecurity discipline and use to provide system security. (CAE KU: CSF)
- Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks. (CAE KU: CSF)
- Describe appropriate measures to be taken should a system compromise occur. (CAE KU: CSF)
- Properly use the Vocabulary associated with cyber security. (CAE KU: CSF)
- List the applicable laws and policies related to cyber defense and describe the major components of each pertaining to the storage and transmission of data. (CAE KU: PLE)
- Describe their responsibilities related to the handling of data as it pertains to legal, ethical and/or agency auditing issues. (CAE KU: PLE)
- Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it. (CAE KU: PLE)
- Examine concepts of privacy. (CAE KU: PRI)
- Explore the effects the Internet has on privacy (CAE KU: PRI)
- Describe approaches individuals, organizations, and governments have taken to protect privacy. (CAE KU: PRI)
- Compare and contrast privacy policies and laws of different jurisdictions (CAE KU: PRI)

CAE KUs:

- Cybersecurity Foundations (CSF)
- Policy, Legal, Ethics, and Compliance (PLE),
- Privacy (PRI)
- Cyber Security Principles (CSP)

Vocabulary

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

NICE Framework Categories

- Securely Provision (SP)
- Operate and Maintain (OM)
- Oversee and Govern (OV)
- Protect and Defend (PR)
- Analyze (AN)
- Collect and Operate (CO)
- Investigate (IN)
Topics
To complete this KU, all Topics and sub-Topics must be completed

**CSF (24 HOURS)**
1. Threats and Adversaries (threat actors, malware, natural phenomena)
2. Vulnerabilities and Risk management (include backups and recovery)
3. Common Attacks
4. Basic Risk Assessment
5. Security Life-Cycle
6. Applications of Cryptography and PKI
7. Data Security (in transmission, at rest, in processing)
8. Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
9. Access Control Models (MAC, DAC, RBAC, Lattice)
10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
11. Session Management
12. Exception Management
13. Security Mechanisms (e.g., Identification/Authentication, Audit)
14. Malicious activity detection / forms of attack
15. Appropriate Countermeasures
16. Legal issues
17. Ethics (Ethics associated with cybersecurity profession)

**PRI (8 HOURS)**
18. Personally Identifiable Information
19. 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
20. Privacy Impact Assessments
21. Anonymity and Pseudonymity
22. Privacy Policies, Laws and Regulations
23. Risks to Privacy
24. Tracking and Surveillance
25. Privacy tools
   a. Encryption
   b. VPNs
   c. Scramblers
26. Privacy Laws and legal basis

**PLE (8 HOURS)**
27. Federal Laws and Authorities
   a. Computer Security Act
   b. Sarbanes – Oxley
   c. Gramm – Leach – Bliley
   d. Privacy (COPPA) HIPAA / FERPA
   e. USA Patriot Act
f. Americans with Disabilities Act, Section 508

g. Other Federal laws and regulations

28. State, US and international standards / jurisdictions

29. Payment Card Industry Data Security Standard (PCI DSS)

30. BYOD issues

1. Principles
   a. Separation (of domains/duties)
   b. Isolation
   c. Encapsulation
   d. Modularity
   e. Simplicity of design (Economy of Mechanism)
   f. Minimization of implementation (Least Common Mechanism)
   g. Open Design
   h. Complete Mediation
   i. Layering (Defense in depth)
   j. Least Privilege
   k. Fail Safe Defaults / Fail Secure
   l. Least Astonishment (Psychological Acceptability)
   m. Minimize Trust Surface (Reluctance to trust)
   n. Usability
   o. Trust relationships
CYB 210 : 3 cr. Cybersecurity Management. Introduces the components in an information technology system and their roles in system operation. Teaches students how to use these components to develop plans and processes for a holistic approach to cybersecurity for an organization. Prereq: CYB 110

Outcomes

- Describe the hardware components of modern computing environments and their individual functions. (CAE KU: ISC)
- Describe the basic security implications of modern computing environments. (CAE KU: ISC)
- Understand the Federal, State and Local Cyber Defense partners/structures. (CAE KU: ISC)
- Properly use the Vocabulary associated with cyber security. (CAE KU: ISC)
- Examine the placement of security functions in a system and describe the strengths and weaknesses. (CAE KU: CPM)
- Develop contingency plans for various size organizations to include: business continuity, disaster recovery and incident response. . (CAE KU: CPM)
- Develop system specific plans for: . (CAE KU: CPM)
  - The protection of intellectual property
  - The implementation of access controls
  - Patch and change management
- Outline and explain the roles of personnel in planning and managing security, including: . (CAE KU: CPM)
  - Board of Directors
  - Senior Management
  - Chief Information Security Officer (CISO)
  - IT Management (CIO, IT Director, etc)
  - Functional Area Management
  - Information Security personnel
  - End users
- Apply knowledge to develop a security program, identifying goals, objectives and metrics. . (CAE KU: SPM)
- Apply knowledge to effectively manage a security program. (CAE KU: SPM)
- Assess the effectiveness of a security program. (CAE KU: SPM)

CAE KUs:

- IT Systems Components (ISC)
- Cybersecurity Planning and Management (CPM)
- Security Program Management (SPM)

Vocabulary

BYOD, IaaS, PaaS, SaaS, SAN, USB, CISO, CIO, IT

NICE Framework Categories

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

Topics

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

**ISC (15 HOURS)**

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

**CPM (15 HOURS)**
17. Broad coverage of the cybersecurity Common Body of Knowledge (CBK) and how it affects planning and management.
18. Differentiate and provided examples of Operational, Tactical, and Strategic Planning and Management
19. Examine C-Level Functions which impact cybersecurity.
20. Making cybersecurity a strategic essential (part of core organizational strategy)
21. Identify requirements and create plans for Business Continuity / Disaster Recovery
22. Develop processes and procedures for incident response
23. Planning for protection of intellectual property
24. Managing the implementation of access controls
25. Managing patch and change control

**SPM (12 HOURS)**
26. Goals and objectives of a security program.
27. Measuring the effectiveness of a security program (metrics).
28. Roles and Responsibilities of the Security Organization
30. Compliance with Applicable Laws and Regulations
32. Security Baselining
33. Program Monitoring and Control
34. Security Awareness, Training and Education
35. Security program addresses:
    b. Physical Security
    c. Personnel Security
    d. System and Data Identification
    e. System security plans.
    f. Configuration and Patch management
    g. System Documentation
    h. Incident Response Program
    i. Disaster Recovery Program.
    j. Certification and Accreditation
**CYB 220 : 2 cr. Secure Coding and Analysis.** Describes the characteristics of secure programs and the ability to implement programs that are free from vulnerabilities. Practice evaluating software, including adding security mechanisms into software and testing software for vulnerabilities. 2 hr lecture and 2 hour lab. Prereq: CYB 110, CS 121

### Outcomes

- Produce software components that satisfy their functional requirements without introducing vulnerabilities. (CAE KU: SPP)
- Describe the characteristics of secure programming. (CAE KU: SPP)
- Understand the vulnerabilities inherent in different programming languages. (CAE KU: SPP)
- Examine vulnerabilities introduced through the use of libraries and how to mitigate those vulnerabilities. (CAE KU: SPP)
- Describe software security analysis tools and techniques. (CAE KU: SSA)
- Apply knowledge to perform software security analysis, using common tools, against previously unknown software components. (CAE KU: SSA)
- Develop effective tests in a structured, organized manner. (CAE KU: QAT)
- Perform security functional testing to demonstrate that security policies and mechanisms are completely and correctly implemented. (CAE KU: QAT)

### CAE KUs:

- Secure Programming Practices (SPP)
- Software Security Analysis (SSA)
- QA/Functional Testing (QAT)

### NICE Framework Categories

### Topics

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

**SPP (15 HOURS)**

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

**SSA (15 HOURS)**
10. Testing Methodologies
11. Source and Binary Code Analysis
12. Static and Dynamic Analysis Techniques
13. Sandboxing
14. Common analysis tools and methods

**QAT (12 HOURS)**
15. Testing methodologies (white, grey, black box testing)
16. Test coverage analysis
17. Automatic and manual generation of test inputs
18. Test execution
19. Validation of results
CYB 310: 3 cr. Cybersecurity Technical Foundations. Provide students with basic information about the threats that may be present in the cyber realm and introduce architectural mitigation strategies including cryptography. Prereq CYB 110, CS 240

Outcomes

1. Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk. (CAE KU: CTH)
2. Describe different types of attacks and their characteristics. (CAE KU: CTH)
3. Examine a specific architecture and identify potential vulnerabilities. (CAE KU: IAA)
4. Design a secure architecture for a given application. (CAE KU: IAA)
5. Students will be able to identify the elements of a cryptographic system. (CAE KU: BCY)
6. Students will be able to describe the differences between symmetric and asymmetric algorithms. (CAE KU: BCY)
7. Students will be able to describe which cryptographic protocols, tools and techniques are appropriate for a given situation. (CAE KU: BCY)
8. Students will be able to describe how crypto can be used, strengths and weaknesses, modes, and issues that have to be addressed in an implementation (e.g., key management), etc. (CAE KU: BCY)

CAE KUs:
- Cyber Threats (CTH)
- Basic Cryptography (BCY)
- IA Architectures (IAA)

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

**CTH (15 HOURS)**
1. Motivations and Techniques
2. The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)
3. Types of Attacks (and vulnerabilities that enable them)
   a. Password guessing / cracking
   b. Backdoors / trojans / viruses / wireless attacks
   c. Sniffing / spoofing / session hijacking
   d. Denial of service / distributed
   e. DOS / BOTs
   f. MAC spoofing / web app attacks / 0-day exploits
   g. Advanced Persistent Threat (APT)
4. Events that indicate an attack is/has happened
5. Attack Timing (within x minutes of being attached to the net)
6. Attack surfaces / vectors, and trees
7. Covert Channels
8. Social Engineering
9. Insider problem
10. Threat Information Sources (e.g., CERT)
11. Legal Issues associated with cyber threats

**IAA (12 HOURS)**
12. Defense in Depth
13. DMZs
14. Proxy Servers
15. Composition and Security
16. Cascading
17. Emergent Properties
18. Dependencies
19. TCB Subsets
20. Enterprise Architectures / Security Architectures
21. Secure network design

**BCY (15 HOURS)**

22. Common cryptographic uses
23. Security Functions (data protection, data integrity, authentication, non-repudiation)
24. Block vs. stream data
25. Digital Signatures (Authentication)
26. Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)
   a. Integrity checking
   b. For protecting authentication data
   c. Collision resistance
27. Symmetric Cryptography (DES, Twofish)
28. Public Key Cryptography (Diffie-Hellman, RSA, ECC, ElGamal, DSA)
   a. Public Key Infrastructure
   b. Certificates
   c. Key Management (creation, exchange/distribution)
29. Cryptography in practice
   a. Common Cryptographic Protocols
   b. DES -> AES (evolution from DES to AES)
   c. Cryptographic Modes (and their strengths and weaknesses)
   d. Cryptographic standards (FIPS 140 series)
30. Cryptographic failures
   a. Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)
   b. Implementation failures
CYB 330. 2 cr. Networking and Control Systems. Covers common network protocols, how network components interact, and how networks evolve over time. Use of tools to monitor and analyze a network. Students expand their familiarity with network vulnerabilities. Prereq CS 240

Outcomes

- Describe the fundamental concepts, technologies, components and issues related to communications and data networks. (CAE KU: BNW)
- Design a basic network architecture given a specific need and set of hosts/clients. (CAE KU: BNW)
- Describe common network vulnerabilities. (CAE KU: BNW)
- Demonstrate an understanding of layer 2 networking (Ethernet) (CAE KU: NTP)
- Demonstrate an understanding of the structure and use of key networking protocols (IPv4 and IPv6). (CAE KU: NTP)
- Identify and describe a variety of common network vulnerabilities. (CAE KU: NTP)
- Explain the weaknesses of WEP and which weaknesses have been addressed and how. (CAE KU: NTP)

Following satisfied by Cybersecurity Lab I

- Track and identify the packets involved in a simple TCP connection (or a trace of such a connection). (CAE KU: BNW)
- Use a network monitoring tools to observe the flow of packets (e.g., WireShark). (CAE KU: BNW)
- Perform network mapping (enumeration and identification of network components) (e.g., Nmap). (CAE KU: BNW)
- Identify and mitigate security concerns at layer 2 and layer 3 of a network. (CAE KU: NTP)
- Demonstrate the use of multiple tools to analyze and troubleshoot a network. (CAE KU: NTP)

CAE KUs:
- Basic Networking (BNW)
- Network Technology and Protocols (NTP)

NICE Framework Categories

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

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

BNW (18 HOURS)
1. Networking models (OSI and IP).
2. Network media (wired, optical, and wireless)
3. Network Architectures and topologies (PAN, LAN/WAN, DMZ, Enclaves, VLAN, NAT, subnetting, supernetting)
4. Common Network Devices and their role in the network. (Routers, Switches, Hosts, VPNs, Firewalls)
5. Network Protocols introduction (IP, TCP, UDP, ICMP)
6. Network Services and protocols introduction (DNS, NTP, VLAN, etc.).
7. Network Applications and protocols introduction (SMTP, HTTP, VoIP, SSH, etc.).
8. Use of basic network administration tools.
9. Overview of Network Security Issues

NTP (18 hours)
10. Network Switching (Ethernet)
a. ARP and RARP
b. Layer 2 security issues
11. IPv4 suite
   a. IPv4 Addressing
12. IPv6 suite
   a. IPv6 Addressing
   a. Routing tables and metrics
   b. Layer 3 security issues
   c. IPsec
14. Network naming
   a. DNS
   b. NetBIOS
15. Network Analysis/Troubleshooting
   a. Netflow
CYB 340. 3 cr. Network Defense. Covers 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. Provide students with knowledge and skills related to detecting and analyzing vulnerabilities and threats and taking steps to mitigate associated risks. Prereq CYB 310, 330

Outcomes

- Describe the key concepts in network defense (defense in depth, minimizing exposure, etc.). (CAE KU: NDF)
- Explain how network defense tools (firewalls, IDS, etc.) are used to defend against attacks and mitigate vulnerabilities. (CAE KU: NDF)
- Analyze how security policies are implemented on systems to protect a network. (CAE KU: NDF)
- Evaluate how network operational procedures relate to network security. (CAE KU: NDF)
- Detect, identify, resolve and document host or network intrusions. (CAE KU: IDS)
- Use tools and algorithms to detect various types of malware (keyloggers, rootkits) and unauthorized devices (rogue wireless access points) on a live network. (CAE KU: IDS)
- Configure IDS/IPS systems to reduce false positives and false negatives. (CAE KU: IDS)
- Deploy reactive measures to respond to detected intrusion profiles. (CAE KU: IDS)

CAE KUs:
- Network Defense (NDF)
- Intrusion Detection and Prevention Systems (IDS)

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

NDF (21 HOURS)

1. Outline concepts of network defense, such as:
   a. Defense in Depth
   b. Network attacks
   c. Network Hardening
   d. Minimizing Exposure (Attack Surface and Vectors)
2. Network defense/monitoring tools:
   a. Implementing Firewalls
   b. DMZs / Proxy Servers
   c. VPNs
   d. Honeypots and Honeynets
   e. Implementing IDS/IPS
3. Network Operations
   a. Network Security Monitoring
   b. Network Traffic Analysis
4. Network security policies as they relate to network defense/security:
   a. Network Access Control (internal and external)
   b. Network Policy Development and Enforcement
IDS (21 HOURS)

1. Deep Packet Inspection
2. Log File Analysis
3. Log Aggregation
4. Cross Log Comparison and Analysis
5. Anomaly Detection
   a. Establishing profiles
   b. Anomaly algorithms, such as:
      i. Statistical Techniques
      ii. Correlation Techniques
      iii. Fuzzy Logic Approaches
      iv. Artificial Intelligence
      v. Filtering Algorithms
      vi. Neural Networks
6. Misuse Detection (Signature Detection)
7. Specification-based Detection
8. Host-based Intrusion Detection and Prevention
9. Network-based Intrusion Detection and Prevention
   a. Stealth mode
10. Distributed Intrusion Detection
11. Hierarchical IDS's
12. Honeynets/Honeypots
13. Intrusion response
   a. Device Reconfiguration
   b. Notifications
      i. Logging
      ii. SNMP Trap
      iii. Email
      iv. Visual/Audio Alert
   c. Trace Recording
   d. Opening Application
   e. Session Interruption
   f. Reach back
**CYB 350. 3 cr. Operating System Defense.** This course provides fundamentals of secure operating system administration and hardening. Provide students with an understanding of the authorities, roles and steps associated with cyber operations. Prereq CS 240, CYB 310

**Outcomes**

- Describe, for a given OS, the steps necessary for hardening the OS with respect to various applications. (CAE KU: OSH)
- Describe the laws that provide US entities the authority to perform cyber operations. (CAE KU: BCO)
- List the phases of a well-organized cyber operation and describe the goals and objectives of each phase. (CAE KU: BCO)
- Identify specific phases of a cyber operation in network traffic. (CAE KU: BCO)
- Describe potential motivations that might prompt an entity to perform a cyber operation. (CAE KU: BCO)

Following satisfied by Computer Security Lab II and lectures

- 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. (CAE KU: OSH)
- Set up user accounts. (CAE KU: OSA)
- Configure appropriate authentication policies. (CAE KU: OSA)
- Configure audit capabilities. (CAE KU: OSA)
- Performing back-ups and restoring the system from a backup. (CAE KU: OSA)
- Install patches and updates. (CAE KU: OSA)
- Review security logs. (CAE KU: OSA)

**CAE KUs:**

- Basic Cyber Operations (BCO)
- Operating System Administration (OSA)
- Operating System Hardening (OSH)

**Topics**

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

**BCO (18 HOURS)**

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

**OSA (12 HOURS)**
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

OSH (12 HOURS)
14. Secure Installation
15. Removing unnecessary components
16. File system maintenance (isolation of sensitive data)
17. User restrictions (access and authorizations)
18. User/Group/File Management
19. Password Standards and Requirements
20. Shutting Down Unnecessary/Unneeded Services
21. Closing Unnecessary/Unneeded Ports
22. Patch Management/Software Updates
23. Virtualization
24. Vulnerability Scanning
**CYB 380: 3 cr. Cybersecurity Lab I.** This hands-on laboratory class allows students to get practical experience related to the cybersecurity threats, mitigations and scenarios that they have been introduced to in other courses. This includes classic buffer overflow and SQL injection style vulnerabilities as well as network security monitoring. Lab course. Co-req CYB 310, 330

**Outcomes**

- Track and identify the packets involved in a simple TCP connection (or a trace of such a connection). (CAE KU: BNW)
- Use a network monitoring tools to observe the flow of packets (e.g., WireShark). (CAE KU: BNW)
- Perform network mapping (enumeration and identification of network components) (e.g., Nmap). (CAE KU: BNW)
- Identify and mitigate security concerns at layer 2 and layer 3 of a network. (CAE KU: NTP)
- Demonstrate the use of multiple tools to analyze and troubleshoot a network. (CAE KU: NTP)

**CYB 381: 3 cr. Cybersecurity Lab II.** This hands-on laboratory class allows students to get practical experience related to operating system administration and security, including Windows and Linux security configurations. Co-req CYB 340, 350

**Outcomes**

- 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. (CAE KU: OSH)
- Set up user accounts. (CAE KU: OSA)
- Configure appropriate authentication policies. (CAE KU: OSA)
- Configure audit capabilities. (CAE KU: OSA)
- Performing back-ups and restoring the system from a backup. (CAE KU: OSA)
- Install patches and updates. (CAE KU: OSA)
- Review security logs. (CAE KU: OSA)

**CYB 401: 1cr.** Ethical, legal, social, and intellectual property issues; current research topics; and other issues of importance to the cybersecurity professional. (Cross listed CS 401)
**CYB 420: 3 cr. Computer Forensics.** Provide students with the skills to apply forensics techniques throughout an investigation life cycle with a focus on complying with legal requirements. Provide students with the ability apply forensics techniques to investigate and analyze network traffic. Prereq CYB 310

**Outcomes**
- Discuss the rules, laws, policies, and procedures that affect digital forensics (CAE KU: DFS)
- Use one or more common DF tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit. (CAE KU: DFS)
- Describe what can/cannot be retrieved from various Operating Systems, (CAE KU: HOF)
- Describe the methodologies used in host forensics. (CAE KU: HOF)
- Describe the methodologies used in network forensics. (CAE KU: NWF)
- Analyze and decipher network traffic, identify anomalous or malicious activity, and provide a summary of the effects on the system. (CAE KU: NWF)

**CAE KUs:**
- Digital Forensics (DFS)
- Host Forensics (HOF)
- Network Forensics (NWF)

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

**DFS (6 HOURS)**
1. Legal Compliance
   a. Applicable Laws
   b. Affidavits
   c. How to Testify
   d. Case Law
   e. Chain of custody
2. Digital Investigations
   a. E-Discovery
   b. Authentication of Evidence
   c. Chain of Custody Procedures
   d. Metadata
   e. Root Cause Analysis
   f. Using Virtual Machines for Analysis

**HOF (20 HOURS) (More than one operating system should be demonstrated.)**
3. File Systems and File System Forensics
4. Hypervisor Analysis
5. Cryptanalysis
6. Rainbow Tables
7. Known File Filters (KFF)
8. Steganography
9. File Carving
10. Live System Investigations
11. Timeline Analysis
12. Include samples of hands-on activities

*Examples of acceptable operating system specific Topics may include:*
13. Registry Analysis, NTFS (Microsoft Windows)
14. Preference List Analysis, HFS+/AFS (Apple MacOS)
15. System configuration Analysis, EXT2/3/4 (Linux, e.g. /etc)

**NWF (24 HOURS)**

1. Packet Capture and Analysis (Wifi, LAN)
2. Intrusion Detection and Prevention
3. Interlacing of device and network forensics
4. Log-file Analysis
5. Forensic Imaging and Analysis
CYB 440: 3 cr. Software Vulnerability Analysis. Provide students with a thorough understanding of system vulnerabilities, to include what they are, how they can be found/identified, the different types of vulnerabilities, how to determine the root cause of a vulnerability, and how to mitigate their effect on an operational system. 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. Prereq CYB 220, 310

Outcomes

- Apply tools and techniques for identifying vulnerabilities. (CAE KU: VLA)
- Create and apply a vulnerability map of a system. (CAE KU: VLA)
- Apply techniques to trace a vulnerability to its root cause. (CAE KU: VLA)
- Propose and analyze countermeasures to mitigate vulnerabilities. (CAE KU: VLA)
- Explain the circumstances under which a vulnerability must be disclosed. (CAE KU: VLA)
- Apply security design principles. (CAE KU: SAS)
- Describe how system design and architecture affects security. (CAE KU: SAS)
- Create a system design optimized to meet appropriate security requirements. (CAE KU: SAS)
- Apply modeling and vulnerability assessment to create a secure design. (CAE KU: SAS)
- Explain the importance of Design Reviews in creating secure systems. (CAE KU: SAS)

CAE KUs:

- Software Vulnerability Analysis (VLA)
- Software Assurance (SAS)

Topics

To complete this KU, all Topics and sub-Topics must be completed: (must include hands-on exercises)

**VLA (24 HOURS)**

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

**SAS (24 HOURS)**

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

---

**CYB 480. 3 cr. Cybersecurity Senior Capstone Design I**

Capstone design sequence for cybersecurity science majors. Formal development techniques applied to definition, design, coding, testing, and documentation of a comprehensive cybersecurity. Projects are customer-specified, includes real-world design constraints, and usually encompasses two semesters. Students work in teams. Significant lab work required. Prereq Engl 317, CS 383, CYB 310

**CYB 481. 3 cr. Cybersecurity Senior Capstone Design II**

Continuation of CYB 480. Application of formal design techniques to development of a large cybersecurity science project performed by students working in teams. Significant lab work required. Prereq CYB 481