CS A255: CYBERSECURITY FOUNDATIONS AND PRINCIPLES

Item	Value
Curriculum Committee Approval Date	12/08/2021
Top Code	070600 - Computer Science (Transfer)
Units	3 Total Units
Hours	90 Total Hours (Lecture Hours 36; Lab Hours 54)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

Cybersecurity is the science of protecting users and systems against hackers, malware, and other threats permeating modern day cyberspace. This course covers the theoretical foundations of cybersecurity, such as the concepts of confidentiality, integrity, and availability, and access control models, as well as the principles and practices of system, information, and network security. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Students will be able to analyze cybersecurity attacks and identify proper defense countermeasures.
2. Students will be able to employ the principles of cybersecurity to analyze security designs and security policies and failures.

Course Objectives

- 1. Define confidentiality, integrity, and availability
- 2. Describe the role of cybersecurity in modern computing
- 3. Identify the role of cybersecurity within organizations and the broader society
- 4. Identify the proper access controls in diverse organizational environments
- 5. Analyze cybersecurity attacks and identify proper defense countermeasures
- 6. Utilize appropriate cybersecurity vocabulary in cybersecurity discussions
- 7. Discuss the importance of each principle of cybersecurity
- 8. Employ principles of cybersecurity to analyze security designs and security policies and failures
- 9. Identify the critical design principles necessary for ensuring security in specific scenarios
- 10. Describe the Federal, State, and Local Cyber Defense partners/ structures.

Lecture Content

The course is designed to cover the three fundamental Knowledge Units (KUs) outlined in the criteria for National Centers of Academic Excellence in Cyber Defense (CAE-CD) published by the National Security Agency (NSA) and the Department of Homeland Security (DHS). The three KUs are Cybersecurity Foundations (CSF), Cybersecurity Principals (CSP), and Information Systems Components (ISC). Each topic in the weekly course schedule at the end of this document includes the KU topic it corresponds to. For example, CSPa next to a topic means that the topic corresponds to the CSP KU topic a. Overview of Cybersecurity CSF1 Threats and Adversaries (threat actors, malware, natural phenomena) CSF2 Vulnerabilities and Risk management (includes backups and recovery) CSF3 Common attacks CSPa Separation (of domains/ duties) CSPb Isolation CSPc Encapsulation CSPd Modularity CSPi Layering (Defense in depth) CSPj Least Privilege CSPk Fail Safe Defaults / Fail Secure CSPl Least Astonishment (Psychological Acceptability) CSPe Simplicity of design (Economy of Mechanism) CSPf Minimization of implementation (Least common mechanism) CSPg Open design CSPh Complete Mediation CSPm Minimize Trust Surface (Reluctance to trust) CSPn Usability CSPo Trust relationships Access Controls and IT Security Management CSF4 Basic Risk Assessme nt CSF5 Security Life-Cycle CSF12 Exception Management (https://resources.infosecinstitute.com/topic/exception-management/) Cryptographic Tools and Message Confidentiality CSF6 Applications of Cryptography and PKI CSF7 Data Security (in transmissions, at rest, in processing) Linux and Windows Security CSF8 Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security) CSF9 Access Control Models (MAC, DAC, RBAC, Lattice) CSF10 Confidentiality, Integrity, Availability, Access, Authenticity, Authorization, Non-Repudiation, Privacy Intrusion Detection CSF13 Security Mechanisms (e.g. Identification/Authentication, Audit) CSF14 Malicious activity detection / forms of attack CSF 15 Appropriate Countermeasures Denial of Service, Firewalls and Internet Security Protocols ISC5 Networks (Internet, LANs, wireless) ISC6 Network Mapping (enumeration and identification of network components) ISC7 Network Security Components (Data Loss Prevention, VPNS / Firewalls) ISC8 Intrusion Detection and Prevention Systems, Incident Response ISC13 Vulnerability Scanning (e.g., Windows 0-day vulnerabilities) Operating System, Cloud and IoT Security Controls ISC1 Endpoint protection (Workstations, servers, appliances, mobile devices, peripheral devices Printers, scanners, external storage) ISC2 Storage Devices ISC3 System Architectures Virtualization / Containers Cloud ISC4 Alternative E nvironments (SCADA, real time systems, critical infrastructures) ISC15 Physical and environmental security concerns ISC16 Internet of Things (IoT) Buffer Overflow and Software Security ISC9 Managed Services ISC10 Software Security (secure coding principles, software issues by type) ISC11 Configuration Management ISC12 Patching (OS and Application Updates) Human Resources, Legal, and Ethical Aspects of Security ISC14 People and Security (social engineering) ISC17 Cyber Defense Partnerships (Federal, State, local, Industry) CSF 16 Legal issues CSF 17 Ethics (Ethics associated with cybersecurity profession)

Lab Content

Lab materials availabe at https://seedsecuritylabs.org/labs.html User Authentication Pluggable Authentication Module: explore a flexible authentication technique. (1 week) Access Control Web Access Control: explore the Same-Origin Access Control Policy in web browsers (1 week) Linux Capability-Based Access Control: explore the capability-based access control in Linux (1 week) Database Security SQL Injection Attack: experience the SQL-Injection attacks (1 week) Malicious Software

Clickjacking Attack: experience the ClickJacking attacks (1 week) Denial of Service Attacks TCP/IP Attacks: exploit the vulnerabilities of the TCP/IP protocols (2 weeks) SYN Cookie: explore the SYN Cookies mechanism in Linux. (1 week) Firewalls Linux Firewall Exploration: Students will explore various firewall-related technologies, such as netfilter, web proxy, URL rewriting, and using SSH tunnels to evade egress filtering (1 week) Buffer Overflow Buffer Overflow Vulnerability: exploit the buffer overflow vulnerability using the shell-code approach (1 week) Return-to-libc Attack: exploit the buffer-overflow vulnerabilities using the return-to-libc attack (1 week) Software Security Format String Vulnerability: exploiting the format string vulnerability (1 week) Race Condition Vulnerability: exploiting the race condition vulnerability (1 week) Set-UID Program Vulnerability: exploiting the vulnerabilities of the privileged Set-UID programs (1 week) Cross-Site Request Forgery Attack: exploiting cross-site request forgery vulnerabilities (1 week) Cross-Site Scripting Attack: exploiting cross-site scripting vulnerabilities (1 week) OS Security Chroot Sandbox Vulnerability: explore how the chroot sandbox can be broken (1 week) Symetric Encryption and Message Confidentiality Secret Key Encryption: explore secret-key encryption and its applications using OpenSSL (1 week) Public-key Cryptography and Message Authentication One-Way Hash Function: explore one-way hash function and its applications using OpenSSL (1 week) Public-Key Infrastructure: explore public-key cryptography, digital signature, certificate, and PKI using OpenSSL (1 week) Internet Security Protocols and Standards Packet Sniffing Spoofing: explore how sniffing and spoofing tools are implemented (1 week)

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

Lecture Demonstration Guided Lab Exercises Peer instruction (clickers) Textbook

Reading Assignments

Students should expect to spend 2 hours a week reading the textbook.

Writing Assignments

None.

Out-of-class Assignments

Students should expect to spend about 3 hours a week completing hands-on , out-of-class security lab and exercises. Students will create virtual machines and then spend time configuring them and exploring different kinds of security flaws and prevention.

Demonstration of Critical Thinking

Students will identify the critical design principles necessary for ensuring security in specific scenarios.

Required Writing, Problem Solving, Skills Demonstration

Students will employ principles of cybersecurity to analyze security designs and security policies and failures.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelors degree and two years of professional experience, or any associate degree and six years of professional experience. Computer science: Masters degree in computer science or computer engineering OR bachelors degree in either of the above AND masters degree in mathematics, cybernetics, business administration, accounting or engineering OR bachelors degree in engineering AND masters degree in cybernetics, engineering mathematics, or business administration OR bachelors degree in mathematics AND masters degree in cybernetics, engineering mathematics, or business administration OR bachelors degree in any of the above AND a masters degree in information science, computer information systems, or information systems OR the equivalent. Note: Courses in the use of computer programs for application to a particular discipline may be classified, for the minimum qualification purposes, under the discipline of the application. Masters degree required.

Textbooks Resources

1. Required Stallings, W., Brown, L.. Computer Security: Principles and Practice, 4th ed. New York City: Pearson (US), 2017

Other Resources

1. SEED Hands-on Labs for Security Education https://seedsecuritylabs.org/index.html