

CS 82.55 Course Outline as of Fall 2014**CATALOG INFORMATION**

Dept and Nbr: CS 82.55 Title: COMPUTER SECURITY PRNCPL

Full Title: Principles of Computer Security

Last Reviewed: 10/14/2013

Units		Course Hours per Week		Nbr of Weeks	Course Hours Total	
Maximum	4.00	Lecture Scheduled	4.00	17.5	Lecture Scheduled	70.00
Minimum	4.00	Lab Scheduled	0	8	Lab Scheduled	0
		Contact DHR	0		Contact DHR	0
		Contact Total	4.00		Contact Total	70.00
		Non-contact DHR	0		Non-contact DHR	0

Total Out of Class Hours: 140.00

Total Student Learning Hours: 210.00

Title 5 Category: AA Degree Applicable

Grading: Grade or P/NP

Repeatability: 00 - Two Repeats if Grade was D, F, NC, or NP

Also Listed As:

Formerly: CIS 56.21

Catalog Description:

Students will begin learning the essentials of computer security. They will be aware of security objectives and the role of policy deployment while practicing to defend against network attacks. After a review of security trends, concepts, roles and network fundamentals students will learn: cryptography, public key infrastructure, standards and protocols, impact of physical security on computer security, infrastructure security, remote access, wireless and instant messaging, intrusion detection and system baselines. Internet-based curriculum describing a start-up company in which the coverage of CompTIA's Security+ certification exam and the International Information Systems Security Certification Consortium (ISC)2 Systems Security Certified Practitioner (SSCP) certification, focuses on best practices, roles, and responsibilities of security experts, is integral to the course.

Prerequisites/Corequisites:**Recommended Preparation:**

Completion of CS 80.13 and CS 82.21A AND Eligibility for ENGL 100 OR ESL 100

Limits on Enrollment:

Schedule of Classes Information:

Description: Students will begin learning the essentials of computer security. They will be aware of security objectives and the role of policy deployment while practicing to defend against network attacks. After a review of security trends, concepts, roles and network fundamentals students will learn: cryptography, public key infrastructure, standards and protocols, impact of physical security on computer security, infrastructure security, remote access, wireless and instant messaging, intrusion detection and system baselines. Internet-based curriculum describing a start-up company in which the coverage of CompTIA's Security+ certification exam and the International Information Systems Security Certification Consortium (ISC)2 Systems Security Certified Practitioner (SSCP) certification, focuses on best practices, roles, and responsibilities of security experts, is integral to the course. (Grade or P/NP)

Prerequisites/Corequisites:

Recommended: Completion of CS 80.13 and CS 82.21A AND Eligibility for ENGL 100 OR ESL 100

Limits on Enrollment:

Transfer Credit: CSU;

Repeatability: Two Repeats if Grade was D, F, NC, or NP

ARTICULATION, MAJOR, and CERTIFICATION INFORMATION:

AS Degree:	Area			Effective:	Inactive:
CSU GE:	Transfer Area			Effective:	Inactive:
IGETC:	Transfer Area			Effective:	Inactive:
CSU Transfer:	Transferable	Effective:	Spring 2006	Inactive:	Fall 2020
UC Transfer:		Effective:		Inactive:	

CID:

Certificate/Major Applicable:

Certificate Applicable Course

COURSE CONTENT

Student Learning Outcomes:

At the conclusion of this course, the student should be able to:

1. Define and explain cryptography, public key infrastructure, standards and protocols, impact of physical security on computer security, infrastructure security, remote access, wireless and instant messaging, intrusion detection and system baselines.
2. Solve problems involving security vulnerabilities, wireless technologies, and network security breaches.
3. Pass a mock certification exam for CompTIA Security+ certification.

Objectives:

Upon completion of this course, students will be able to:

1. Examine current computer security vulnerabilities
2. Describe general computer security concepts
3. Identify operational and organizational elements central to ensuring a secure computer system environment

4. Delineate the role of people in security
5. Evaluate the use of cryptography as a security resource
6. Analyze public key infrastructure
7. Evaluate the various standards and protocols used to secure data transmission
8. Relate a secure physical environment to computer security
9. Critique system infrastructure security components
10. Solve problems involving remote access security vulnerabilities
11. Examine wireless and instant messaging technologies for the vulnerabilities
12. Inspect network security breaches using intrusion detection systems
13. Assess security baselines for network policy implementation

Topics and Scope:

I. Computer security vulnerabilities

A. Identifying security problems

1. Security incidents
2. Threats to security
3. Security trends

B. Identify various avenues of attack

II. General concepts

A. Basic security terminology

1. Security basics
2. Access control
3. Authentication

B. Security models

1. Confidentiality models
2. Integrity models

III. Operational and organizational elements

A. Security operations in an organization

1. Policies, procedures, standards, and guidelines
2. The security perimeter

B. Physical security

1. Access controls
2. Physical barriers

C. Social engineering

D. Environment

E. Wireless

F. Electromagnetic eavesdropping

G. Location

IV. The role of people in security

A. People as a security problem

B. People as a security tool

V. Cryptography

A. Define algorithms

B. Hash

C. Symmetric encryption

D. Asymmetric encryption

E. Usage

1. Confidentiality
2. Integrity
3. Nonrepudiation
4. Authentication

- 5. Digital signatures
- 6. Key escrow
- VI. Public key infrastructure
 - A. The basics of public key infrastructures
 - B. Certificate authorities
 - C. Registration authorities
 - D. Certificate repositories
 - E. Trust and certificate verification
 - F. Digital certificates
 - G. Centralized or decentralized infrastructures
 - H. Private key protection
 - I. Public certificate authorities
 - J. In-house certificate authorities
 - K. Outsourced certificate authorities
 - L. Certificate usage
- VII. Standards and protocols used to secure network data transmission
- VIII. The impact of physical security on network security
 - A. The problem
 - B. Physical security safeguards
- IX. Network fundamentals
 - A. Network architectures
 - B. Network topology
 - C. Network protocols
 - D. Packet delivery
- X. Infrastructure security
 - A. Devices
 - B. Media
 - C. Security concerns for transmission media
 - D. Removable media
 - E. Security topologies
 - 1. Security zones
 - 2. Virtual local area networks (VLANs)
 - 3. Network address translation (NAT)
 - 4. Tunneling
- XI. Remote access
 - A. The remote access process
 - 1. Identification
 - 2. Authentication
 - 3. Authorization
 - B. Telnet
 - C. Secure shell (SSH)
 - D. Layer 2 tunneling protocol (L2TP)
 - E. Point to point tunneling protocol (PPTP)
 - F. Institute of electric and electronics engineers (IEEE) 802.11
 - G. Virtual private network (VPN)
 - H. Internet protocol security (IPSec)
 - I. IEEE 802.1x
 - J. Remote authentication dial-in user (RADIUS)
 - K. Terminal access controller access control system (TACACS+)
 - L. Vulnerabilities
- XII. Wireless and instant messaging
- XIII. Intrusion detection systems

- A. History of intrusion detection systems
- B. Intrusion detection system (IDS) overview
- C. Host-based intrusion detection systems
- D. Network-based intrusion detection systems
- E. Signatures
- F. False positives and negatives
- G. IDS models
- XIV. Security baselines
 - A. Overview baselines
 - B. Password selection
 - 1. Password policy guidelines
 - 2. Selecting a password
 - 3. Components of a good password
 - 4. Password aging
 - C. Operating System and network operating system hardening
 - D. Network Hardening
 - E. Application Hardening

Assignment:

1. Online research of current security appliances and best practices
2. Read topical weekly online newsletters and security reports
3. Prepare written security policies and procedures
4. Write 4-6 one-page reports on security problems and their solutions
5. 4-6 quizzes
6. Computer security skills examinations

Methods of Evaluation/Basis of Grade:

Writing: Assessment tools that demonstrate writing skills and/or require students to select, organize and explain ideas in writing.

Reports

Writing
10 - 30%

Problem Solving: Assessment tools, other than exams, that demonstrate competence in computational or non-computational problem solving skills.

Written security policies and procedures

Problem solving
10 - 30%

Skill Demonstrations: All skill-based and physical demonstrations used for assessment purposes including skill performance exams.

Computer security skills exams

Skill Demonstrations
20 - 30%

Exams: All forms of formal testing, other than skill performance exams.

4-6 quizzes

Exams
20 - 30%

Other: Includes any assessment tools that do not logically fit into the above categories.

Class participation

Other Category 0 - 20%

Representative Textbooks and Materials:

Principles of Computer Security: CompTia Security+ and Beyond (2nd). Nestler, Vincent, et al.
McGraw-Hill: 2011