Course number and name:	**CS 06417: Principles of Network Security**
Credits and contact hours:	3 credits / 3 contact hours
Instructor's or course coordinator's name:	Vahid Heydari
Text book, title, author, and year:	Network Security, Firewalls and VPNs, Second Edition, by Michael Stewart, 2018

Specific course information

Catalog description: This course examines the fundamentals of network security. The material covered in this course includes such topics as cryptographic systems necessary for network security, public key infrastructure, principles of data integrity, authentication, and key management, Internet architecture and TCP/ICP protocol suite, application layer security, secure sockets layer and transport layer security protocols, IPSec, distributed and cloud security, wireless and mobile security, network security techniques and components, network-based vulnerability detection and penetration testing, defense in depth, and others. Students will prepare and deliver technical presentations on state-of-the-art research topics in the network security.

Prerequisites: (CS 01210 Introduction To Computer Networks And Data Communications ***or*** CS 06410 Data Communications and Networking) ***and***

CS 07351 Cyber Security: Fundamentals, Principles and Applications

Type of Course: ☐ Required ☐ Elective ☒ Selected Elective

Specific goals for the course:

1. Describe a basic network architecture and common network vulnerabilities.
2. Describe the key concepts in network defense.
3. Explain how network defense tools (firewalls, IDS, IPsec, etc.) are used to defend against attacks and mitigate vulnerabilities.
4. Use network monitoring, mapping, and analyze and decipher network traffic.
5. Describe the methodologies used in network forensics.
6. Describe the differences between symmetric and asymmetric algorithms and how they can be used.
7. Analyze how security policies are implemented on systems to protect a network.
8. Evaluate how network operational procedures related to network security.
9. Securely install a given OS and describe the steps necessary for hardening the OS with respect to various applications.

Required list of topics to be covered:

1. Network Security Components (Data Loss Prevention, VPNs / Firewalls)
2. Intrusion Detection and Prevention Systems, Incident Response
3. Use of basic network administration tools
4. Layer 2 and 3 security issues
5. Network Analysis, Monitoring, and Troubleshooting
6. Outline concepts of network defense
7. Network defense/monitoring tools
8. Network security policies
9. Network Forensics
10. Operating Systems Hardening
11. Public Key Cryptography and Hash Functions