Course number and name:	**CS 10200: Fundamentals of Network Security**
Credits and contact hours:	3 credits / 3 contact hours
Instructor's or course coordinator's name:	Fred Stinchcombe
Text book, title, author, and year:	Kizza, Joseph Migga. *Guide to Computer Network Security*. Springer; 5th ed. 2020. .

Specific course information

Catalog description: This course is a study of key security issues and procedures in computer and mobile communication networks. Among the issues to be discussed are: the security of LANs, WANs, databases, and network operating systems; threats to computer networks through exploitation of network infrastructure design weaknesses; security flaws in the network infrastructure protocols; security of content in computer network services; risk assessment and security policies; and security in mobile communication networks. Procedures will include: networks intrusion detection and forensics technologies, cryptographic and authentication systems, capability and access control mechanisms, and new developments in Internet routing and transport protocols, secure mail, directory, and multimedia multicast services. Current trends and research in security policies and technologies will also be discussed.

Prerequisites:

Type of Course: ☐ Required ☒ Elective ☐ Selected Elective

Specific goals for the course:

1. To make students aware of the security perils and vulnerabilities in computing in general and in both fixed computer and mobile networks in particular
2. To familiarize students with the important issues pertaining to protecting computer systems against unauthorized penetration and access and denial of service to computing systems
3. To introduce to students current and effective procedures to deal with network security threats, including use of "best practices" software tools.
4. To cultivate students' interests in the search for network security solutions with the hope that some of them, in later years, may become lead scientists in this search for durable solutions
5. To create and nurture an ideal atmosphere for academic dialogue, debate, and question-answer sessions among students intended to deepen the understanding of security of their computerized and networked environments

Required List of Topics to Be Covered:

1. Basic Security Concepts–(Security: General, Information, Computer, and Network).
2. The Status of Computer Network Security: Security Threats; How pervasive are security attacks
3. Vulnerability of Computer Networks
4. Cyber Crimes and Hackers & Hostile Scripts
5. Security Assessment, Analysis and Assurance
6. Dealing with Network Security Challenges
7. Access Control and Authorization
8. Authentication -
9. Cryptography (Conventional and public-key encryption and hash
10. Functions)
11. Cryptography (Encryption algorithms, confidentiality, key distribution, message authentication, digital signatures)
12. Firewalls & Network Security Practice (Authentication protocols: Kerberos,
13. X.509 Directory Authentication Service)
14. Intrusion Detection
15. Network Security Practice(IP Sec, S/Mime, PGP)
16. Security Evaluations of Computer Products
17. Mobile network infrastructure and protocols (Security protocols and operations