



Introduction to Cybersecurity

21:198:351 (3 credits)

COURSE DESCRIPTION

This course covers the fundamentals of Cybersecurity. It introduces many different areas of security such as cryptography, malicious code, authentication and access control, trusted computer systems, operating systems, and network security. A combination of interactive lectures and integrated technology is used to provide a more effective, productive, and enhanced learning experience for students.

PREREQUISITE

21:198:356 Introduction to Computer Networks OR 28:544:120 Introduction to Network Technology

TEXT BOOK

Security in Computing, Charles P. and Shari Lawrence Pfleeger, Prentice Hall, Fourth edition, 2007, ISBN 0-13-239077-9

Recommended

Security+ Guide to Networking Security Fundamentals, Ciampa, Mark. 3rd edition, Course Technology, 2008.

DEPARTMENT WEB SITE: www.ncas.rutgers.edu/math

THIS COURSE COVERS THE FOLLOWING

1. Introduction: What is computer security?
 - The vulnerability, threat and control paradigm
2. Authentication, and access control strategies
 - Identification Vs Authentication, access policies
3. Cryptography
 - Symmetric key cryptography, asymmetric key cryptography
 - Pretty Good Privacy (PGP) and digital signatures
4. Programs and programming
 - Unintentional programming oversights
5. Operating systems
 - Security in operating systems
6. Networks and network security
 - Network security attacks.
7. Strategic Defenses
 - Security countermeasures, cryptography in network security
8. Database security
 - Security countermeasures, reliability and integrity
9. Legal issues and ethics
 - Protecting programs and data, copyrights, patents, information and the law
10. Emerging Topics
 - The Internet of Things (IOT), cyber warfare