CTS1120 - Fundamentals of Cybersecurity

Three Credits, Four and a half hours, Engineering Topic.

Instructor: Dr. Himanshu Upadhyay

Textbook: Fundamentals of Information Security(recommended) Kim David and Michael G. Soloman Jones and Bartlette, Third Edition,2018 ISBN-10: 1284116458

Specific Course Information:

This is undergraduate-level course which covers the basics of cybersecurity. The course presents an insider's perspective on malicious attacks, threats and vulnerabilities with wireless, web and social engineering. information system security, access control, cyber risk and response, basic introduction to network / cryptography and associated threats, threats with loT devices. cyber education, standards and compliance laws. Since the course is intended to serve students with all backgrounds.no programming or information technology skills are expected. Students should have knowledge of internet and familiar with computer, mobile devices, tablets etc.

This course will consist of 15 modules followed by 15 quizzes. Module availability is open and can be completed at the student's individual pace on weekly basis followed by quizzes for the module. Quizzes will be due after one week from the module completion. Quizzes will be evaluated within two days of the Quiz completion date. There will be mid-term and final exam in addition to the quizzes. Communication will take place primarily via email and professor announcements. At the end of the course, you would have leaned various malicious threats, attacks, vulnerabilities and associated tools how to protect from cyber-attacks, basic knowledge of web wireless and social media threats, how to secure personal data, US and international laws to protects individual and organization, career opportunities in cyber security field including various certifications. This is the basic course which will provide foundational learning opportunities in various areas of cybersecurity.

Specific Goals for the Course

a. Specific outcomes of instruction

Upon successful completion of this course, the student will:

1.Describe how unauthorized access can lead to data breach and identify layered security approach throughout the seven domains. Student will be able to develop an IT security policy framework to help reduce risk from common threats and vulnerabilities

2.Identify malicious software and implement countermeasures, recognize social engineering and reduce associated risk, Identify threats and types of attacks on web and wireless network

3.Describe risk management and distinguish BIA, BCP and DRP from each other. Identify risks associated with mobile workers and use of personally owned devices. Describe the impact of risk, threats and vulnerabilities on IT infrastructure.

4.Describe access control concepts and technologies, formal models of access control, identity management and system access control.

5.Create and support security policies and classify data, develop and maintain security programs understand professional ethics describe security infrastructure.

6.Describe the practices and principles of security audit, review logs, system monitoring with intrusion detection system and intrusion prevention system, explain metrics for system performance and security compliance.
7. Identify the principles of risk management and analyze incidents, prevent and recover from disruptions using business continuity plan.
8. Define basic concepts of cryptography, symmetric, asymmetric, and hashing algorithms, examine various use of cryptography and associated challenges, define certificate management.
9.Describe open systems interconnection (OSI) reference model, understand basics of network types of protocols and security risks and identify basic tools to defend against network security risks10.Define Trojan, virus, worm, spyware, adware, ransomware and spam, understand malicious software risks and threats to individual and organization, understand phases of malicious software attack, define social engineering, understand incident detection and attack prevention tools/technique.
11.Identify information security organizations, summarize what ISO 17799 contains, explain ISO/IEC27002 pertains to information security and describe PCI DSS requirements, identify security education programs and professional certifications
12.Explain information security compliance, describe main features of FISMA, HIPA, Sarbanes Oxley, PCI-DSS and CIPA.
13.Describe lo T evolution and its impact on human and business life, explain lo T strategy and how IP mobility is driving both personal and business environment, list new challenges created by lo T.
14.Identify and compare education programs in cybersecurity.
<u>b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.</u>
In this course the student will have to show
(a) an ability to apply knowledge of mathematics, science, and engineering (N/A)
(b) an ability to design and conduct experiments (simulations), as well as to analyze, interpret data (N/A)
(c) an ability to design a system, component, or process to meet desired needs (N/A)
(d) an ability to function in multi-disciplinary teams (N/A)
(e) an ability to identify, formulate, and solve engineering problems (homework) (N/A)
(f) an understanding of professional and ethical responsibility (N/A)
(g) an ability to communicate effectively (through project reports) (N/A)
(h) the broad education necessary to understand the impact of engineering solutions in a global and societal context (N/A)
(i) a recognition of the need, and an ability to engage in life-long learning (N/A)
(j) a knowledge of contemporary issues (N/A)
(k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice (N/A)
(l) a knowledge of probability and statistics (N/A)

Brief list of the topics to be covered

This course examines the principles, mechanisms and implementation of network security and data protection. The topics presented will help students gain the fundamentals of network security and explain what happens behind the scenes and from the point of view of a computer. Topics include definition and use of password crackers, operating system exploits, what is a Hacker, IP Spoofing, Session Hijacking, Denial of Service attacks (DOS), Buffer Overloads, general concepts of password security, how to create a company-wide security policy, how to perform security audits and how to recover from such attacks.

GRADING:

Course Requirements	Weight
Chapter Quizzes	15%
Midterm Exam	15%
Final Exam	10%
Overall Grade	100%

Conversion of Numerical Grade to Letter Grade

95<=A<=100	83<=B<86	70<=C<76
90<=A-<94	80<=B-<82	60<=D<69
87<=B+<89	77<=C+<79	F: Below 60