CS 3320 : INTRODUCTION TO COMPUTER SECURITY

Semester Hours: 3.0

Coordinator: Ruinian Li


Author(s): STALLINGS, W AND BROWN, L

Year: 2015

SPECIFIC COURSE INFORMATION

Catalog Description:

Computer security principles: confidentiality, integrity and availability. Basic security mechanisms such as access control, authentication, cryptography and software security. Overview of data logs audit and analysis. Introduction to spyware and malware. Prerequisites: Grade of C or better in CS 2020 and CS 2170 or CS 2190.

Course type: ELECTIVE

SPECIFIC COURSE GOALS

- I can explain how security protocols such as https works.
- I can understand cryptography basic concepts such as cipher, symmetric, public/private key.
- I can explain the context of encryption and decryption, signature algorithm, and message digest.
- I can use certain tools or techniques to detect and remove spyware and malware.
- I can understand data logs and do basic analysis.
- I can explain certain operating system security specific features or issues, for example, malware, audit.

LIST OF TOPICS COVERED

- Course Overview (~7%)
  - Basic concepts such as confidentiality, integrity, availability
  - General principles of computer security
- Access Control and Authentication (~7%)
• Basic Cryptography (~34%)
  o Cipher, symmetric, public/private key, message digest, signature algorithm
  o Encryption and decryption
  o Classic cryptography
• Software Security (~14%)
  o Vulnerability
  o Database
• Network Security (~10%)
  o Https
  o Web application vulnerability
• Spyware and malware (~14%)
  o Detection
  o Tools and techniques to help remove
• Data log (~7%)
  o Audit tool
  o Data log analysis
• Platform specific issues (~7%)
  o Windows
  o iOS and Android
  o Unix