CIS-5372 Fundamentals of Computer Security

Catalog Description
Information assurance algorithms and techniques. Security vulnerabilities. Symmetric and public key encryption. Authentication and Kerberos. Key infrastructure and certificate. Mathematical foundations. (3 credits)

Prerequisites
SCIS Graduate Standing

Type
Required for MSIT

Course Objectives
This course provides an in-depth understanding into the fundamental concepts of computer security. It covers basic cryptography, including symmetric and public key cryptosystems as well as key management and distribution and user authentication. It provides an introduction to digital signatures, hash functions, message authentication codes and their application to message and user authentication. The course further focuses on software vulnerabilities and the malware exploiting them. It introduces the basic concepts of access control as well as network security and privacy.

Topics
Basic computer security concepts, threat models, common security goals
Key management and distribution, certificates, x509
Authentication protocols including Needham-Schroeder, Kerberos, Denning-Sacco, Woo-Lam
Cryptography and cryptographic protocols
Symmetric cryptography
Public key cryptography
Digital signatures
Hash functions
Message authentication codes
Vulnerabilities, including buffer overflows and incomplete mediation.
Malware, including viruses, worms, trapdoors, rootkits, trojan horses and covert channels
Access control
Network security
Concepts of privacy and anonymity

Textbook
William Stallings. *Cryptography and Network Security, 5th Edition* (Prentice Hall)

Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in Computing, 4th Edition* (Prentice Hall)

Last Update
Bogdan Carbunar, 8/30/2012