CIS 5370 Principles of Cybersecurity

Catalog Description
Cybersecurity algorithms and techniques. Mathematical foundations. Symmetric and public key encryption. Authentication, key infrastructure and certificates. Covert channels. Access control. Vulnerabilities. (3 credits)

Prerequisites
Graduate Standing

Type
Required for MS-Cybersecurity

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. The course also covers basic access control mechanisms and policies, as well as covert channels. The course further focuses on software vulnerabilities, the malware exploiting them, and network security.

Topics
1. Classic Cryptography + Symmetric Key Cryptography, DES
2. Public Key Crypto (RSA, Diffie Hellman), Hash functions/HMAC, Signatures
3. Network Security, IPSec/SSL/PEM
4. Key management and distribution, certificates, x509
5. Authentication
6. Access Control
7. Covert Channel
8. Malware
9. Vulnerabilities
10. Intrusion Detection Systems

Textbooks

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

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

Bruce Schneier. *Applied Cryptography, 2nd Edition* (Wiley)

Last Update
Bogdan Carbunar, 1/24/2014