CIS-5374 Information Security and Privacy

Catalog Description
Information Security Planning, Planning for Contingencies, Policy, Security Program, Security Management Models, Database Security, Privacy, Information Security Analysis, Protection Mechanism. (3 credits)

Prerequisites
CIS-5372

Type
Can be an elective for MSCS, MSIT, and Ph.D. students.

Course Objectives
This course provides an in-depth understanding of the concepts of privacy and security in distributed environments. It introduces the fundamental building blocks, including secret sharing, bit commitment, fair coin flips and zero knowledge protocols as well as the basic concepts of symmetric and public key cryptography. It the applies these building blocks to explore more complex privacy and security constructs, including oblivious transfer and private information retrieval, digital payment technologies, anonymizers, network and web security and privacy.

Topics
Secret sharing
Time stamping
Bit commitment
Fair coin flips
One-way accumulators
Zero knowledge proofs
Cryptography and cryptographic protocols
Symmetric cryptography
Public key cryptography, including RSA, ElGamal.
Oblivious transfer
Oblivious signatures
Private information retrieval.
Blind signatures
Digital payments.
Anonymizers, mixnets. Case studies: Tor, Crowds, etc.
Network security and privacy
Web security and privacy

Textbook
Bruce Schneier. *Applied Cryptography 2nd Edition* (John Wiley and Sons)
Charles P. Pfleeger and Shari Lawrence Pfleeger. *Security in Computing, 4th Edition* (Prentice Hall)

Last Update
Bogdan Carbunar, 8/30/2012