DEPARTMENT OF COMPUTER SCIENCE COURSE SYLLABUS

CS 45203/55203 COMPUTER NETWORK SECURITY 3 credit hours

Instructor’s Name: Kambiz Ghazinour

Online Material

Course Content:
(Cross-listed with CS 55203) Overview of network security including attacks and vulnerabilities and defense measures, secure network design, network and transport layers security, intrusion detection techniques, defense against denial of service attacks, network hardware, software, and applications attacks and their defense, security policies, legal and ethical issues in cyber and computer crimes.

Prerequisites or co-requisites: CS 35201
Required, elective, or selected elective

Topics to be Covered (45 Hours):
1. An Introduction to Network Security (1 hours)
2. A Review of Network Protocols (4 hours)
3. Physical Layer Security (4 hours)
4. LAN Security (4 hours)
5. Resilient Network Topologies (4 hours)
6. IP Security Issues (4 hours)
7. Network Layer Defense (4 hours)
8. A Taxonomy of Attacks and Vulnerabilities (4 hours)
9. Attacks Classification (4 hours)
10. Distributed Denial of Service (DDoS) Attacks (4 hours)
11. DoS and DDoS Attack Defenses (4 hours)
12. Statistical Detection Techniques (4 hours)

Learning Outcomes:
1. Describe the different categories of network threats and attacks.
2. Describe the architecture for public and private key cryptography and how PKI supports network security.
3. Describe virtues and limitations of security technologies at each layer of the network stack.
4. Identify the appropriate defense mechanism(s) and its limitations given a network threat.
5. Discuss security properties and limitations of other non-wired networks.
6. Identify the additional threats faced by non-wired networks.
7. Describe threats that can and cannot be protected against using secure communication channels.
8. Summarize defenses against network censorship.

Assessment of Learning Outcomes:
1. Midterm Exam
2. Final Exam
3. Assignments
4. Class discussion