CSxxx/ECExxx: Network Security

Course Description:

This course provides a comprehensive introduction to the field of network security. The course focuses on the fundamentals of network security concepts and principle. Critical network security aspects are identified and examined from the standpoints of both the user and the attacker. The practice of network security, practical applications and security standards that have been implemented and are in use to provide network security are surveyed. Network security architectures and protocol design principles are examined and their impact on computer and network security are evaluated.

Prerequisites:

Students are expected to have a good knowledge of cryptography (e.g., from the new security course) and TCP/IP networking.

Textbook:

Potential textbooks:

- Network Security: Private Communication in a Public World, by Charlie Kaufman, Radia Perlman, Mike Speciner
- Cryptography and Network Security: Principles and Practice, by William Stallings

Topics to be covered:

- Fundamental concepts
  - Review of network security architecture, basic security concepts, basic cryptographic techniques, and basic networking concepts and attacks
  - Overview of Authentication Systems, authentication of people
  - Security handshake pitfalls, real-time communication security
- Security standards
  - Network Authentication Protocol - Kerberos
  - Public Key Infrastructure
  - Network Security Protocol - IPSec
  - Network Security Protocol - SSL/TLS
  - Email Security
- Other network security topics
  - Firewalls, Intrusion detection, System security topics
  - Infrastructure security: BGP and DNS
  - Wireless security: WEP, WPA2, GSM,3GPP