CSC411 COMPUTER NETWORK SECURITY

Learning Outcomes

- Describe the enhancements made to IPv4 by IPSec
- Identify protocols used to enhance Internet communication, and choose the appropriate protocol for a particular case.
- Understand Intrusions and intrusion detection
- Understand how public-key cryptography works and Distinguish between the use of private- and public-key algorithms.
- Summarize common authentication protocols.
- Summarize the capabilities and limitations of the means of cryptography that are conveniently available to the general public.
- Summarize the strengths and weaknesses associated with different approaches to security.

Content

Types of threats to information security, secret-key crypto, hashes & message digests, public key algorithms, number theory, operating system vulnerabilities, intrusion detection, authentication systems, Kerberos, email security (PGP, S/MIME), firewalls, IP security (IPsec), SSL, TLS, WWW security, Ensuring Security for Electronic Commerce, Financial Networks, Intranets and Extranets, Business Continuity and Disaster Recovery Planning.

Pre-requisites

CSC225 Computer Networks

Delivery

Lectures and Tutorials