

ELEN689/CPSC689 will be team taught by Reddy, Bettati and Klappenecker. The course will cover three facets of security: encryption, protection of resources through QOS/accounting style techniques, privacy and confidentiality. The tentative list of topics include (in no particular order):

(1) Types and nature of security attacks – basic introduction – spoofing, floods, smurf attacks, portscans, SYN attacks, buffer overflow attacks, DDOS attacks (1 or 2 classes)

(2) Fall & Floyd paper – impact of nonresponsive flows on network, TCP –controlling DOS floods (1 class)

(3) Resource accounting as a means of security – Larry Peterson’s work, Partial state based work (LRU-RED, LRU-FQ, RED-PD, Andreas), Varghese & Estan’s work, Cisco’s netflow (2 classes)

(4) Identifying source of attacks – traceback, ingress filtering (1 class)

(5) Statistical techniques to detect traffic anomalies – Anu’s work, Paul Barford’s work, SeongSoo’s work, USC’s work, HT Kung’s work – wavelets (1 class)

(6) Protecting end servers from floods – Aman’s work (resources versus sources), HP’s web QOS mechanisms, Google’s SYN cookies etc. (1 class)

(7) Firewalls and packeteer style edge devices to control traffic consumption, TCP ack pacing (1 class)

(8) Worms, worm propagation, speed of propagation, controlling worms by limiting packets from individual machines (HP work) (1 class)

(9) Intrusions: Modeling and modeling of responses. (1 hour)

- Anonymity (1 hour)
- Definitions, Applications (anonym. comm. systems, e-cash)

(10) Traffic Analysis and Anonymous Communication Systems (2 hours)

- Metrics
- Examples (Chaum Mixes, Crowds, Onion Routing, Anonymous File Sharing)
- Traffic Analysis Attacks

(11) Traffic Analysis and Covert Channels (2 hours)

- Metrics
- Unintentional Covert Channels
- Intentional Covert Channels

(12) Other Forms of Information Hiding (2 hours)

- Intro to Steganography
- Watermarking

(13) Symmetric Key Cryptography (AES, Serpent, Twofish; modes of operation, information leakage) [1-2 lectures]

(14) Hash Functions (MD5, SHA-1,256,384,512g RIPEMD-160) [1 lecture]

(15) Message Authentication Codes: CBC-MAC, HMAC [1 lecture]

(16) Public Key Cryptography (RSA, ElGamal, Diffe-Hellmann, Elliptic Curve Methods, and attacks) [1-2 lectures]

(17) Key management and Authentication (Kerberos, X.509, Public Key Infrastructures) [1 lecture]

(18) Virtual Private Networks (IP Security Architecture) [2 lectures]

(19) Prospects and limitations of quantum cryptography (key exchange, bit commitment, discrete logarithms) [1 lecture]