ENPM693 Syllabus

Course: ENPM 693 - Network Security (formerly ENPM 808N)

Semester: Fall 2016

Instructor: Dr. S. Farshad Bahari, Ph.D.

Day; Time: Th, 7:00 PM - 9:40 PM

Location: JMP 2216

Email: fbahari at umd dot edu

Office Hour: Thursdays, 6:45 PM - 7:00 PM at JMP 2216, by appointment

Required Textbook

Kaufman, Perlman, and Speciner. "Network Security: Private Communication in a Public World, Second Edition," Prentice Hall PTR, 2002, ISBN: 0130460192

Recommended Textbook

Ross Anderson. "Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition," Wiley, 2008, ISBN: 9780470068526 (available for free: https://www.cl.cam.ac.uk/~rja14/book.html)

Course Objective

This course addresses network security mechanisms as a means of mitigating security threats on networked devices. Ubiquitous usage of networked enabled devices in day-to-day life and critical infrastructure introduces significant dependency and as a result raises potential risk of service disruption due to malicious unauthorized accesses and other vulnerabilities. To combat against such threats, traditional security mechanisms including physical security would not be sufficient and need to be improved. In this course a broad range of network security measures and protocols countering such threats will be covered resulting in a foundational knowledge and in-depth review of security techniques and standards, available tools, and core concepts.

Specific topics that will be covered include an overview of cryptography with emphasis on stream ciphers and public key cryptography, PKI and key distribution, keyed hash functions and MACs, access control, authentication mechanisms, privacy, DNS, IPSec and IKE, web security SSL/TLS, HTTPS, wireless infrastructure security, secure routing, secure email, and VoIP security. As other topics of interest, various attack models will be addressed such as man-in-the-middle attack and denial-of-service (DoS and DDoS) attacks. Also viruses and worms, firewall, intrusion detection and prevention systems IDS/IPS will be

considered albeit briefly as the detailed discussion of these topics are designed for follow up courses. Finally, Wireshark and BackTrack will be introduced as security tools for implementing various security protocols and applications.

Grading System

The grade for the course will be mainly based on a midterm exam and a final project/term paper as well as a few homework sets/reading assignments, which their respective contributions to the overall grade are given below. All examinations will be conducted in open book format.

Homework/Reading	20%	
Midterm Exam	40%	Exam date (TBD)
Final Project	40%	To be presented on two sessions dated on the last day of class (TBD) and the final exam day (TBD)

It is the student's responsibility to inform the instructor of any intended absences for religious observations in advance. Notice should be provided as soon as possible but no later than the end of the adjustment period.

Course Syllabus

- Introduction to network vulnerabilities
    - Threat model and malicious behaviors by intruders
    - Worms, viruses, … (various network level adversary models)
    - Denial of service (DoS and DDoS)
    - Introduction to Firewall as a defense mechanism
- Cryptography

- Cryptosystems and cipher algorithms
- Secret key cryptography
  - Stream cipher
  - Block cipher
  - Modes of operation
- Cryptographic hash functions
- Public key cryptography
  - Digital signatures

· Key distribution management

- Key distribution centers (KDCs)
- Certification authorities (CAs)
- Trust management
- PKI standard

· Authentication and secure protocols

- Network authentication
- Multi-factor authentication
- Strong password protocol

· Real-time communication security

- Session key establishment
- Perfect forward secrecy
- SSL/TLS
- IPsec

    - Web security

- Network applications
    - Email security and phishing
    - Voice over IP (VoIP) security

Code of Academic Integrity

The University of Maryland, College Park has a nationally recognized Code of Academic Integrity, administered by the Student Honor Council. This Code sets standards for academic integrity at Maryland for all undergraduate and graduate students. As a student you are responsible for upholding these standards for this course. It is very important for you to be aware of the consequences of cheating, fabrication, facilitation, and plagiarism. For more information on the Code of Academic Integrity of the Student Honor Council, please visit http://shc.umd.edu/SHC/HonorPledgeInformation.aspx.