Course Name: Fundamental Technologies of Cyber Security

Offered: Summer 2019; Sunday-Thursday, July 2-18, 9:00-12:00pm

Lecturer: Prof. Amit Kleinmann

Course Evaluation Requirements:
Final Exam: 70%
Assignments: 30%

Attendance and Participation:
Attendance to class is mandatory. Students who will miss more than one class without a valid excuse will not be allowed to take the exam.

Professor Contact Information
a.b.kleinmann@gmail.com

Syllabus:

Review of course topics, our digital world and its future, BYOD, IoT, cyber warfare, the threats, the types of enemies. APT, malware types, zero-day attacks, current statistics and impact

Chapter 2 – Overview of Cyber Security

Domains of cyber security, security objectives, identity authentication principles, passwords challenge-response, zero knowledge identification protocols, authentication using physical devices, biometrics, access control, confidentiality, (data) Integrity, availability/serviceability, non-repudiation, tampering, standards.

Chapter 3 – Steganography

Definition, steganography history, network steganography, modern steganography

Chapter 4 –Cryptography

- Part 1 – Fundamental cryptography concepts:
  What is Cryptography? History - the classical era, substitution & transposition ciphers, monoalphabetic & polyalphabetic ciphers, frequency analysis, encoding versus encryption, unicity distance, Shannon's theory of secrecy, Kirchhoff principle, cryptoanalysis
- Part 2 - Hash function:
  Function, hash function, cryptographic hash functions, MD5, SHA, rainbow tables
- Part 3 - Basic crypto-techniques:
  Communication channel and participants, the building blocks of a crypto system, symmetric encryption, Feistel cipher, DES, 3DES, RC4, AES, key management, Kerberos, Diffie-Hellman, Rijndael block cipher, stream ciphers vs. block ciphers, cipher block modes of operation, integrity, MAC, HMAC
- Part 4 - Public-Key cryptography:

Modular arithmetic (prime numbers, co-prime numbers and the Totient function), Euclid algorithm for finding GCD, extended Euclid algorithm, RSA, Elliptic curves, digital signatures, DSA

Chapter 5 – Networks Security

ARP poisoning, ICMP Scanning, Smurf attack, Syn flood DoS, Shrew attack, port scanning, DNS spoofing, downgrade attacks, from IRC to botnets, WiFi Security, IPSec, VPNs, RADIUS

Chapter 6 – Protecting the vulnerability of the World Wide Web

Cookies, PKI, SSL, SOP, CORS, CSP, XSS, CSRF, SQL injection, file inclusion, spider trap, black SEO techniques and mitigation, the deep-web, the dark-net, dorks.

Chapter 7 – Common Attacks and Defense – Concepts & Tools

Monetization of finding and exploiting vulnerabilities, common attacks (DoS/DDoS, SPAM, MITB, Phishing, Smishing, and Vishing, social engineering , buffer overflow, watering hole, supply chain attacks, air gap, tempest Attacks), attack vector, taxonomy of attacks, how can we achieve security, perimeter protection, filtering, zoning, tools (e.g.: Firewall, NIDS, anti-virus, honeypot), securing applications, Email security, instant messaging security, VoIP security

Chapter 8 – Distributed Ledger Technology

Virtual money, cryptocurrency, blockchain, timestamping, mining, wallet, bitcoin, hyperledger

Chapter 9 – Security Challenges of Cyber-Physical Systems

Unique risks in Cyberphysical system (CPS), Industrial Control Systems (ICS), Internet Of Things (IOT).