FUNDAMENTAL TECHNOLOGIES OF CYBER SYSTEMS

(3 CREDITS)

Mr. Amit Kleinman/ Faculty of Engineering

Course Number: 2120-1004-05 (First Session, June 17 - July 16, 2015)

Abstract: The course provides an overview of the following topics: Cyber security objectives, Computer structure limitations and vulnerabilities, Communication networks, The evolvement of the internet and its operational model, Protocols and their vulnerabilities, The web network and its inherent dangers, Cloud computing and associated security challenges, Fundamental cryptography and tools, Common attacks, Attack infrastructures, Defense (protocols and tools).

Lecturer: Amit Kleinman

Syllabus:

Chapter 1 – Introduction

Review of course topics, cyber and its future, what is cyber warfare? Risks, types of enemies, security objectives, and taxonomy of authentication techniques

Chapter 2 – Computer structure and the role of the Operating System

Computer architecture, computer components (processors, memory hierarchy, interfaces), number representation, programming languages, operating system, compiler and interpreter, the concept of algorithm, time and space limitations.

Chapter 3 – Communication network

Circuit switching versus packet switching, layering, The 7 Layers of the OSI Model, wire and wireless networks, WAN, MAN and LAN, network architecture, client-server model versus peer-to-peer model, addresses, the concept of protocol, unicast, multicast and broadcast communication.

Chapter 4 – Fundamentals of the Internet network

Internet history, Internet architecture IP protocol, IP address, ARP, ICMP, Routing, NAT, DNS, Standardization

Chapter 5 – Internet – transport layer and application layer

Connection oriented, communication port, UDP, TCP (incl. detailed description of its 3-way handshake, Syn flood, flow control, congestion control, shrew attacks), application protocols (Telnet, SSH, FTP, SMTP, IRC), risks

Chapter 6 – Vulnerability of the World Wide Web

History, from SGML to HTML and XML, Browsers, Standardization, Threats, Risks and Exploits (e.g. XSS)

Chapter 7 – Risks in cloud computing

Virtual machine and Hyperjacking, what is cloud computing? Types of cloud computing (taxonomy), regulations in creation, Risks

Chapter 8 – Cryptography

History (e.g., Scytale, Caesar cipher, Alberti cipher, Tabula recta, Vigenère cipher, Gilbert Vernam one-time pad, Jefferson disk, and the Enigma vulnerability),
The concepts of: encoding vs. encryption, confusion vs. diffusion,
Basic techniques:

- Unkeyed (e.g., cryptographic hash functions, passwords, rainbow tables),
- Shared Key (e.g., symmetric key encryption, Feistel Cipher/Network, block cipher versus stream cipher),
- Public Key (e.g., public key encryption and signatures, Euclid's (and extended) algorithm, RSA),

Homomorphic Encryption, Message integrity, MAC, KEK, AONT,
Regulations, export policy and law, Chaffing and winnowing, Back Doors

Chapter 9 – PKI

Key management, key exchange, key generation techniques such as Diffie-Hellman, Trust, PGP, Certificate Authority hierarchy, SSL/TLS, Tunneling, VPN, IPSEC

Chapter 10 – Common attacks

Types of Malware, Attack vector, Taxonomy of Attacks, Attack Classification, Man in the Middle (MiM), Denial of Service (DOS) + DDOS (Distributed DOS), Hijack, Vishing, Smishing and Phishing, Botnets, Supply Chain Attacks

Chapter 11 – Defense: Tools, standardization, certification

Firewall, NIDS, Anti-Virus, Honeypot, standardization

Chapter 12 – Attack techniques

Forensic, covering techniques, Proxy ,Intermediaries, Steganography, Side channel attacks, Key loggers, Rootkits