TEL AVIV UNIVERSITY

Unlocking Information Security
Course Syllabus

Prof. Avishai Wool | Dan Gittik

Lesson 1 – Vulnerabilities, Exploits, and Why You Should Care

- Information security **basic terminology**: goals and threats, vulnerabilities and exploits
- The various kinds of **vulnerabilities**: design, implementation, operational and integration vulnerabilities
- What is an **exploit**? DoS, Information Disclosure, Remote Code Execution, Privilege Escalation
- **Hackers**: who they are and why do they hack
- A vulnerability case study – the **Meltdown** vulnerability

Quiz 1

Lesson 2 – Basic Cryptography

- A conceptual and historical **overview of cryptography**
- The mathematical foundation for **Symmetric Ciphers**
- **Cipher breaking**: Brute Force and Frequency Analysis
- The technical foundation for **digital ciphers:** One-Time Pad, Stream Ciphers, Block Ciphers
- **Kerchkoff's principle** of secure cryptosystems
- Famous modern ciphers: DES, AES, RC4

Quiz 2

Lesson 3 – Hash Functions

- **Hash functions** as a means for ensuring data integrity
- Hash Collisions
- The mathematical properties of **a good hash function**? the "one-way" property and the “collision-resistance” property
- Famous cryptographic hash functions: MD5, SHA1, SHA2, SHA3

Quiz 3

Lesson 4 – Authentication

- The challenge of user authentication and **the three main modes of authentication**
- **Password-based** authentication: weak points and defenses
- **Challenge-response** schemes and 2-factor authentication
- **Biometrics-based** authentication: advantages and pitfalls
- Useful **tips** on password usage

Quiz 4

Mid-Course Exam

Lesson 5 – Buffer Overflows

- **Buffer Overflow** basics
- Variations of Buffer Overflow: **Variable Overflow**, **Stack Overflow**
- **Return to Libc** attack
- Buffer Overflow **mitigations**: Canaries and DEP

Quiz 5

Lesson 6 – Network Vulnerabilities and Defenses

- An **overview of network communication**: the 7-layer OSI model and packet headers
- **LAN (**Layer 2) **vulnerabilities**: Promiscuous Mode and Arp Poisoning
- **IP** (Layer 3) **vulnerabilities**: IP Address Spoofing
- **TCP** (Layer 4) **vulnerabilities**: TCP Injection
- **DNS vulnerabilities**: DNS Poisoning
- **Network address translation** (NAT) and its security implications
- **Firewalls** and security policies

Quiz 6

Lesson 7 – Advanced Cryptography

- Internet-Scale Cryptographic Challenges
- The **Diffie Hellman Key Exchange**: setup, protocol and security
- **Public-Key Encryption** and the **RSA system**: setup, encryption/decryption and security
- **Digital Signatures**: the RSA construction and Hybrid Schemes

- Message Authentication Codes (**MAC**)

  Quiz 7

Lesson 8 – Web Vulnerabilities and Defenses

- **Introduction to the Web**: URLs, HTTP, HTML, CSS, JS
- **SQL Injections**: what they are and how they are mitigated
- **Cross-Site Request Forgery** (CSRF): what it is and how it is mitigated
- **Cross-Site Scripting** (XSS): what it is and how it is mitigated
- HTTPS

  Quiz 8

Lesson 9 – Computer Viruses and How to Beat Them

- A conceptual and historical **introduction to computer viruses**
- Types of malware: **Viruses**, **Worms** and **Trojan Horses**
- Anti-Viruses
- Static and Dynamic Signatures
- Reflections on Trusting Trust

  Quiz 9

Final Exam