Reading instructions for Stallings: “Computer Security” and other course material in the course EDA263 - rev7

Lecture number:

L01: Introduction; Threats, Vulnerabilities, Protection
Chapter 1 (except §1.4, pp.22-26)
Chapter 13 (overviewish) -- Physical security
DL1:Targeted Trojan Email Attacks

L02 - UNIX:
Chapter 23 -- Linux Security: all (23.7 for the interested)
Chapter 4 -- Access Control (UNIX): Only Section 4.4

L02 - Malware I (L02) + Malware II (L04):
Chapter 7 -- Malware: (for interested: Digital Immune System)
Chapter 11 -- Buffer Overflows: all (for now)
OP1 -- Covert channels, salami attacks

L03: Chapter 3 (except “Markov Model” p.85-88). (Overviewish: §§ 3.7-3.8, pp. 101-105)
Chapter 4 (except: § 4.4 - in L02; An access control model, Protection domains, pp.118-122; RBAC Reference Model, The NIST RBAC Model and Static Separation of Duty Relations, pp. 128-134) (Overviewish §4.6, pp. 135-136)
DL2: Testing biometric methods
DL3: Bank card skimming
DL4: Password trading
DL12: Password guessing

L04 Malware I (L02) + Malware II (L04):
Chapter 7 -- Malware: (for interested: Digital Immune System)
Chapter 11 -- Buffer Overflows
OP1 -- Covert channels, salami attacks

L05: Malware defences, Firewalls, Link encryption, Operating Systems Security:
DL7 (p. 1-7) -- Malware defences
§§ 9.1-9.5 -- Firewalls
§ 19.6 -- Link encryption
§ 10.3 -- Reference Monitor

L06: NW attacks, Denial-of-Service Attacks, Kerberos
Chapter 8 -- Denial-of-Service-attacks, spoofing
§ 22.1, OP4 – Kerberos NW authentication scheme

L07: Intrusion Detection Systems, Intrusion Tolerance
Chapter 6 -- Intrusion Detection
§ 9.6 -- Intrusion Prevention Systems
OP5 -- Intrusion tolerance (FRS system)

L08: An introduction to cryptology

Chapter 2	Cryptographic Tools
Chapter 19.1	Symmetric Encryption Principles (not: Feistel Cipher Structure)
Chapter 19.2	Data Encryption Standard
(Chapter 19.3	for interested students, read as an overview: AES)
Chapter 19.7	Key Distribution

Chapter 22.3	Public-Key Infrastructure
OP2-3	

L09: Security Policies and Models

Chapter 4.1	Access Control Principles
Chapter 4.2	Subjects, Objects, and Access Rights
Chapter 4.3	Discretionary Access Control
Chapter 10.1	The Bell-LaPadula Model Section “Abstract Operations” only as an overview. Section “Implementation Example – Multics” is not included.
Chapter 10.2	Other formal models for computer security the Certification and Enforcement rules on page 316 are only as an overview

L10: Security and Dependability modeling and Metrics

Lecture slides

DL8 -- A Framework for Security Metrics

L11: Security and Dependability metrics, Organisational issues, Human factors

§ 14.2-14.4 -- Organisational issues, Human factors, Security policy

§§ 14.1 overviewish -- Organisational issues, Human factors, Security policy

§ 16.4 -- Risk Analysis

§§ 16.1-3 overviewish -- Risk Analysis

§§ 17.3 - 17.5 -- Security plan

§§ 17.1 - 17.2 (overviewish) -- Security plan

DL9 -- The Risks of Key Recovery

L12: Defensive Programming and Database Security

§§ 5.1-5.5 (where 5.1-5.3 is database introduction. Should only be read to the extent necessary to understand the rest of the chapter)

Chapter 12

L13: Common Criteria, spam, etc

§10.6-7 (Fig. 10.5 overviewish)

DL 11: §1-2, §3 for reference, §6-9, A1-3, B1-3, C1-2, D1

L14: Hard Disk Data Recovery and Erasure

DL 5: Data Remanence

L15: Honeypots, Side-channel attacks, Ethics, Examination

§6.8, §18.4

DL 15: Introduction to Side-Channel Attacks