2015-02-25

Reading instructions for Stallings: “Computer Security” 3rd edition and other course material in the course EDA263 – rev150225-A

These notes are reading instructions for the third edition of the text book. It will be continuously updated during the course so please always download the last version.

Lecture number: (for all lectures, the lecture slides are part of the reading)

L01: Introduction; Threats, Vulnerabilities, Protection
Chapter 1 (except §1.5)
Chapter 16 -- Physical security (overviewish)

L02 – UNIX + Malware (see also L03):
Chapter 4 -- Access Control (UNIX): Only Section 4.4
Ch 25 (online, with book)
OP1: Stallings: Linux Security (equivalent to Ch 25 for those who do not have the book)

L03 – Malware (L02—L03):
Chapter 6 -- Malware: (for interested: Digital Immune System)
Chapter 10 -- Buffer Overflows: all
DL 1: Salami attack
OP2: Pfleeger: Covert Channels, Steganography,Easter eggs, trapdoors and Salami attacks

L04: Authentication, authorization and access control
Chapter 3 (overviewish pp.96-97, §3.7-3.8) (except Bloom Filter pp.109, §3.5)
Chapter 4 (except: § 4.4 – covered in L02; RBAC Reference Model, pp. 150-153)
(overviewish: §4.6-4.9, pp. 153-170)
DL2: Password trading, DL3: Password guessing
DL 4: Smartphone malware, DL5: Testing biometric methods, DL6: Bank card skimming

L05: Introduction to cryptology, signatures, PKI, CA

Chapter 2	Cryptographic Tools
Chapter 20.1	Symmetric Encryption Principles (not: Feistel Cipher Structure)
Chapter 20.2	Data Encryption Standard
(Chapter 20.3	for interested students, read as an overview: AES)
Chapter 20.5	Cipher Block Modes
Chapter 20.7	Key Distribution
Chapter 23.3	Public-Key Infrastructure
OP4-5	

L06: Malware defences, Firewalls, Link encryption, Operating Systems Security
DL7: Malware defences principles (p. 1-7)
§§ 9.1-9.5 Firewalls
§ 20.6 Link encryption and end-to-end encryption
§ 13.3 Reference Monitors

L07: NW attacks, Denial-of-Service Attacks, Kerberos
Chapter 7 -- Denial-of-Service-attacks, spoofing
§ 23.1, OP6 – Kerberos NW authentication scheme

L08: Intrusion Detection Systems, Intrusion Tolerance
Chapter 8 -- Intrusion Detection
§ 9.6 -- Intrusion Prevention Systems
OP7 -- Intrusion tolerance (FRS system)

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 13.1	The Bell-LaPadula Model Section “Abstract Operations” only as an overview. Section “Implementation Example – Multics” is not included.
Chapter 13.2	Other formal models for computer security Certification and Enforcement rules on page 472 are only as overview

L10: Defensive Programming and Database Security

§§ 5.1-5.6, 5.8	(where 5.1-5.3 is database introduction. Should only be read to the extent necessary to understand the rest of the chapter)
Statistical databases	Will be provided on Ping Pong (part of edition 2, but not 3)
Chapter 11	

L11: Security and Dependability Modelling and Metrics

Lecture slides

DL8**:** Identifying Suitable Attributes for Security and Dependability Metrication

L12: Risk Analysis, Human and Organisational Factors

§ 14.4 -- Risk Analysis

§§ 14.1-3 overviewish -- Risk Analysis

§§ 17.2-17.3 – Human Resources Security

§§ 17.1 overviewish – Security Awareness, Training and Education

§§ 15.3 - 15.5 -- Security plan

§§ 15.1 - 15.2 (overviewish) -- Security plan

DL9: Why Cryptosystems fail

L13: Key Escrow Systems, Common Criteria, Spam Economics

Common criteria slides
§§ 13.6-7 – Common Criteria (Fig. 13.14 overviewish)
DL 10: Common Criteria – Introduction and General Model (§1-9, A1-A3, B1-B3, C1-C2, D1)
DL 11: Key Escrow Systems Taxonomy,
DL 12: The Risks of Key Recovery
DL 13: Spamalytics

L14: Side-channel attacks, Ethics (+catchup)

Chapter 19.4

DL14: Introduction to Side-channel attacks; DL15: Data remanence

OP3: Pfleeger, Ethics; DL16:The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research Companion (overviewish)