2014-02-11

Reading instructions for Stallings: “Computer Security” and other course material in the course EDA263 – rev140211-1

These notes are reading instructions for the second edition of the text book, which is the officially recommended book. It will be continuously updated during the course so please always download the last version.

Lecture number:

L01: Introduction; Threats, Vulnerabilities, Protection

Chapter 1 (except §1.4, pp.48-52)
Chapter 16 -- Physical security (overviewish)
DL1:Targeted Trojan Email Attacks

L02 – UNIX + Malware (see 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 4: Salami attack
OP2: Pfleeger: Covert Channels, Steganography,Easter eggs, trapdoors and Salami attacks

L04: Authentication, authorization and access control

Chapter 3 (except: pp. 105-106 and §3.5). (overviewish: §§ 3.7-3.8, pp. 119-123)
Chapter 4 (except: § 4.4 – covered in L02; RBAC Reference Model and The NIST RBAC Model, pp. 146-151)
(overviewish: §4.6, pp. 151-154)
DL2: Testing biometric methods
DL3: Bank card skimming
DL4: Password trading
DL12: Password guessing

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
DL8: Attacking Malicious Code

L07: NW attacks, Denial-of-Service Attacks, Kerberos

Chapter 7 -- Denial-of-Service-attacks, spoofing
§ 23.1, OP6 – Kerberos NW authentication scheme (note that pages in copy are in the reverse order)

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

L09: Security and Dependability modelling, Risk Analysis
Lecture slides
§ 14.4 -- Risk Analysis
§§ 14.1-3 overviewish -- Risk Analysis

L10: Security Metrics, Human and Organisational Factors
Lecture slides
§§ 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 -- Identifying Suitable Attributes for Security and Dependability Metrication
DL10 – Why Cryptosystems fail

L11: 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 455 are only as overview

L12: 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)
Chapter 11

L13: Guest Lecture from Microsoft
slides

L14: Key Escrow Systems, Common Criteria, Spam Economics, Computer Forensics
DL13 – Key Escrow Systems Taxonomy, DL9 – The Risks of Key Recovery
§§ 13.6-7 – Common Criteria (Fig. 13.15 overviewish)
DL9 -- The Risks of Key Recovery
DL 11: Common Criteria – Introduction and General Model (§1-9, A1-A3, B1-B3, C1-C2, D1)
DL14: Spamalytics

L15: Side-channel attacks, Ethics (+catchup)
Chapter 19.4
DL15: Introduction to Side-channel attacks; DL5: Data remanence
OP3: Pfleeger, Ethics;