Lectures and Slides

The lectures take place in HA4, Monday, Thursday, and some Fridays. See the full schedule at time edit. We will not use most Fridays (and for labs Mondays) so ignore these slots unless otherwise stated on this page.

The following is a draft for the course. It will be updated (and links to documents added) as the course goes on.

Lecture 0: (1) Course Memo, (2) Off Prints (OP)

Lecture 1: Introduction, Threats, Vulnerabilities, Protection
(Mon 2018-01-15, 13-15)
(1) Course Introduction, (2) Lab Intro, (3) Vulnerabilities, threats, and protection mechanisms.

Book: (1) Chapter 1, (2) Chapter 16 -- Physical security (overviewish)

Extra reading:

- Here is a description of an attack and the resulting problems for a private individual. Note the difference in assumptions between Amazon and Apple regarding the privacy of the numbers of the credit card.

Lecture 2: (0) single pdf for topics (1) UNIX Security, (2) Passwords, (3) Authentication, Authorization and Access Control

Book:

- 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)*
- Chapter 3 (except: pp. 105-106 and §3.5). (overviewish: §§ 3.7-3.8, pp. 119-123)
- Chapter 4 (except: RBAC Reference Model and The NIST RBAC Model, pp. 146-151)
- (overviewish: §4.6, pp. 151-154)

DL:

- Password trading

- Password guessing
- Testing biometric methods
- Bank card skimming
- Smartphone malware

Extra reading:

- A description of a large-scale analysis of passwords at a university (open in Chalmers): Measuring password guessability for an entire university, Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur.

Lecture 3: see material for Lecture 2.

Lecture 4: (1) Introduction to Malware, (2) Malware ex: Love Letter virus

DL:

- Salami attack
- Also look at the following material to prepare for buffer overflows.

Lecture 5: (1) Malware ex: The Morris Worm, (2) Mobile Malware, (3) Recent Malware: Stuxnet, Equation Group, and Rowhammer

DL:

- Smartphone malware
- Overview of the Equation Group
- Also look at the following material to prepare for buffer overflows.

Lecture 6: (1) Rowhammer (from L5), (2) Buffer Overflow part 1, (3) Buffer Overflow part 2, (4) Buffer Overflow & Defences, (4) Defensive Programming

ER:

- An article about how buffer overflows work in detail with code examples: Smashing the stack for fun and profit, Phrack Magazine vol. 7, issue 49

Lecture 7: (1) Buffer Overflow & Defences, (2) Defensive Programming

ER:

- Jailbreaking your Iphone - shows how complicated attacks can be. Note the discussion about Address Space Layout Randomization, ASLR.
- Description of vulnerability to take control of iPhone through some carefully crafted SMS.

Lecture 8: (1) Cryptography, (2) Key Escrow, (3) Information Hiding, (4) Side Channel Attacks

Extra Reading:

- GPU cluster guesses 350 billion passwords per second (in Swedish).
- Why cryptosystems fail
- How to explain zero-knowledge protocols to your children

Lecture 9: (1) Cryptography (cont), (2) Key Escrow, (3) Information Hiding, (4) Side Channel Attacks, (5) Operating System Defences

DL:

- Key Escrow systems taxonomy
- The Risks of Key Recovery
- Introduction to Side-channel attacks

Lecture 10: (1) Database Security, (2) Denial-of-Service Attacks

ER:

- Differential Privacy

Lecture 11: (1) Denial-of-Service Attacks (cont), (2) Network Security

ER:

- DoS attack against twitter (NY Times)

Lecture 12: (1) Overview of Kerberos (included in slides for lecture 11), (2) Vulnerability example of Kerberos (TOCTOU), (3) Intrusion Detection Systems, example the FRS file system (DL), honeypots, (4) Forensics, (5) Introduction to spam article in DL

DL:

- Spam Economics

ER:

- Ptacek and Newsham: Insertion, Evasion, and Denial of Service - Eluding Network Intrusion Detection
- Honey Pots and Honey Nets - Security through Deception (SANS Institute)

Lecture 13: (1a) Data Remanence, (1b) link versus end-to-end encryption, (2) Security Policies and Models, (3) Swedish Security Actors

ER:

- A security model for military message systems: Retrospective, Carl E. Landwehr, Constance L. Heitmeyer, John D. McLean
  (accessible from Chalmers network)

Lecture 14: (1) Common Criteria, (2) Risk Analysis, (3) Human and organisational factors

DL:

- Common Criteria - Introduction and General Model (see reading instructions)

ER:

- slides for "Human and organisational factors" have examples from the following: Why cryptosystems fail

---

Lecture 15: (1)Security Metrics, (2) Ethics

DL:

- CVSS tutorial (slides)
- The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research Companion (overviewish)

ER:

- The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research

---

Lecture 16: (1) Course recap

Lecture X (catchup): (1) Malicious Code Defences

DL:

- Attacking Malicious Code

Exam Feedback

Students asked about **question 160319-1**: *A basic system model of security, dependability and their attributes.*
The lecture was partly remade this year, and the answer is partly on slides L15, 29-32, but given that I presented the material in a new way I will not ask such a question on the exams this year.

Exam given 170321. The following is a guide to the solutions within the reading instructions, and esp. what we were looking for in the answers.