Computer Security DD2395

http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasak10/

Spring 2010
Sonja Buchegger
buc@kth.se

Lecture 1, Jan. 18, 2010

Goals

- Learn about security concepts
- Have tools and methods to reason about security
- Spot threats, vulnerabilities
- Know and propose counter-measures
- Present concepts to others

Outline

- About the course
- About computer security

Outline

- About the course
- About computer security

Syllabus: Times and Places

look at schema, course code DD2395

http://schema.sys.kth.se/4DACTION/WebShowSearch/2/1-0?wv_graphic=graphic&wv_obj1=17467000&wv_startWeek=1003&wv_stopWeek=1011&wv_ts=20100117T143135X%3C%3C%3C%3C

Syllabus: Content (preliminary) see course website for updates

- L1: intro, admin [ch1]
- L2: cryptography [2,20]
- L3: authentication [3]
- L4: buffer overflow [11]
- L5: access control [4]
- L6: firewalls [9]
- L7: intrusion detection [6]
- L8: sandboxes
- L9: malware
- L10: models
- L11: web attacks
- L12: programming
- L13: DoS
- L14: social engineering

Current Info

Check course website regularly for updates!
DD2395
http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasak10/

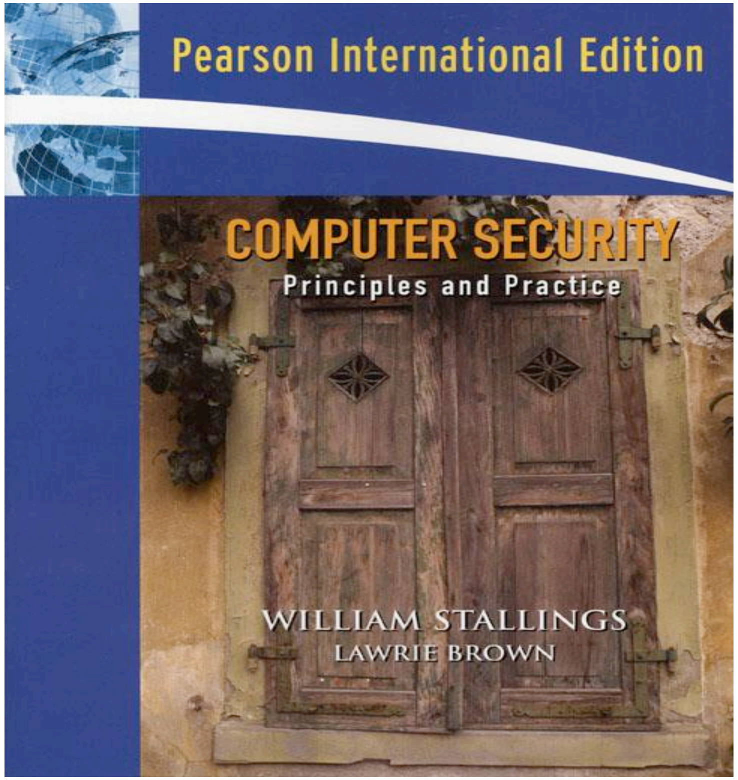
Extra Lectures

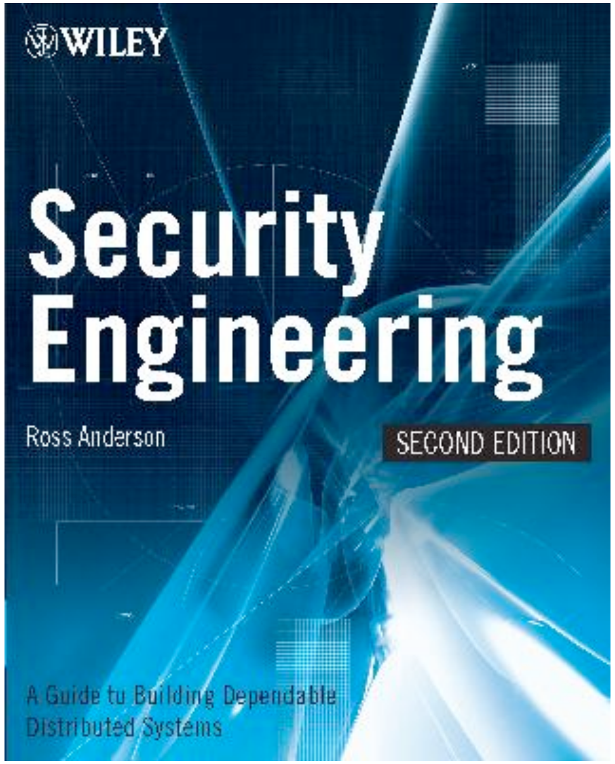
- Computer architectures: Wednesday, Jan 20, 13-15h, Stefan Nilsson, Room D31
- Operating systems: Thursday, Jan 21, 10-12h, Inge Frick, Room D41
- Computer networks: Wednesday, Jan 27, 13-15h, Olof Hagsand, Room D41

People

- Course leader: Sonja Buchegger, buc@csc
- Extra lectures given by Olof Hagsand, Stefan Nilsson, Inge Frick
- Lab assistants: Eric Druid, Pontus Walter
- Packet filtering lab: Olof Hagsand, Daniel, Dan

Books


Pearson International Edition
COMPUTER SECURITY
Principles and Practice
WILLIAM STALLINGS
LAWRIE BROWN


WILEY
Security Engineering
Ross Anderson
SECOND EDITION
A Guide to Building Dependable Distributed Systems

Exam

- March 15, 2010, 14h, Room D1
- Next exam in June

Grades

- Exam: two parts
  - part 1 needs to be passed
  - part 2 determines above-passing grade
- Labs:
  - pass/fail, no grades
  - bonus points for exam when handed in early, see lab descriptions, starting Jan 28

Lab Exercises

- See schema for times and rooms
- 4 different exercises
- 1st: starting January 28, on GnuPG, hand in
- 2nd: on February 12, on site
- Update: 3rd: presentation

Lab Exercise 4

- Presentation on computer security topic
- Pairs of students
- Next lecture: topic distribution
- Dry run
- Small group sessions, to be scheduled

Language

- Course given in English
- Some extra lectures in Swedish
- Questions in Swedish OK

Accounts

- Needed for lab exercises
- Who doesn't have an account and access card?
- Send me an e-mail buc@kth.se

RAPP

- Register for DD2395, details on Wednesday

Networking Security

- Course in the next term
- Building on this course

Questions for you:

- 1) prior knowledge/experience in security v. expectations
- 2) Have you had classes in
  - computer architecture?
  - operating systems?
  - networking?
- 3) Most important question
  - about the course
  - about computer security

Questions?

Outline

- About the course
- About computer security

Computer Security

Slides adapted from Lawrie Brown's set of slides
for the course book
“Computer Security: Principles and Practice”
by William Stallings and Lawrie Brown

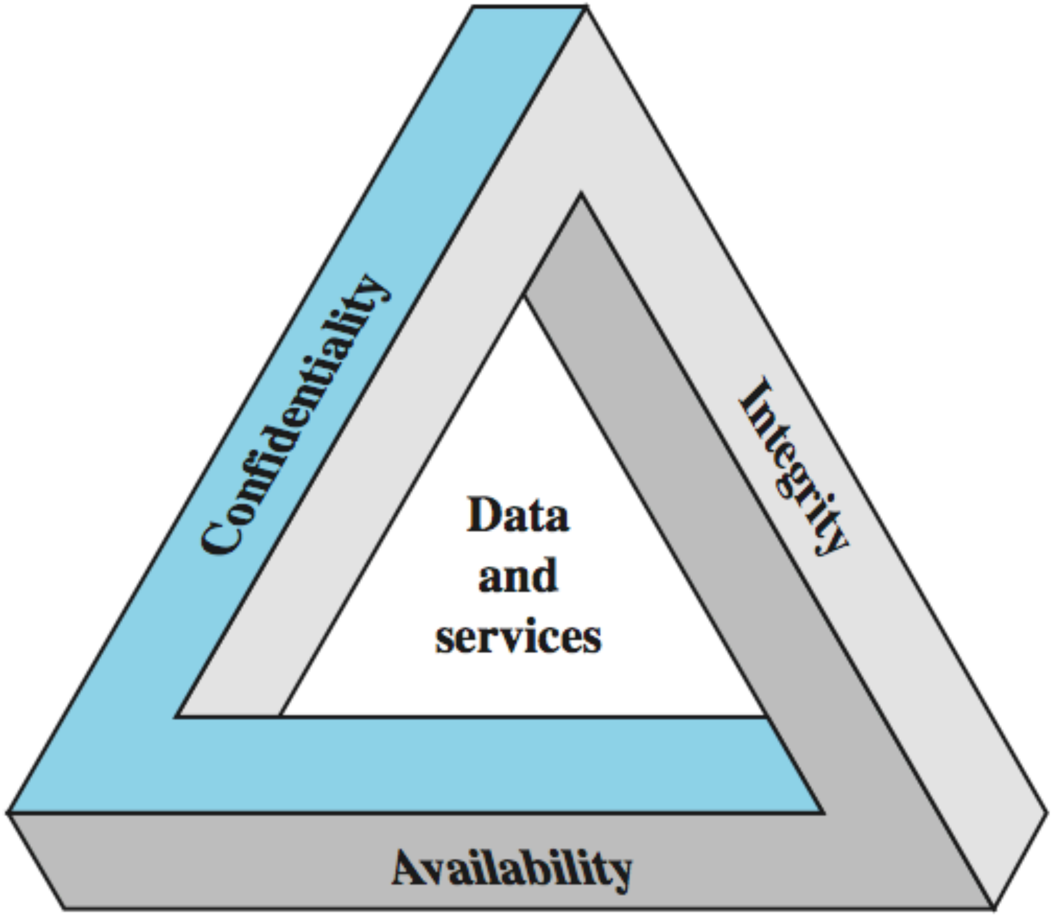
Computer Security

- privacy
- intrusions
- cryptography
- authentication
- correctness
- networking
- bad transactions

Overview

Computer Security: protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Key Security Concepts



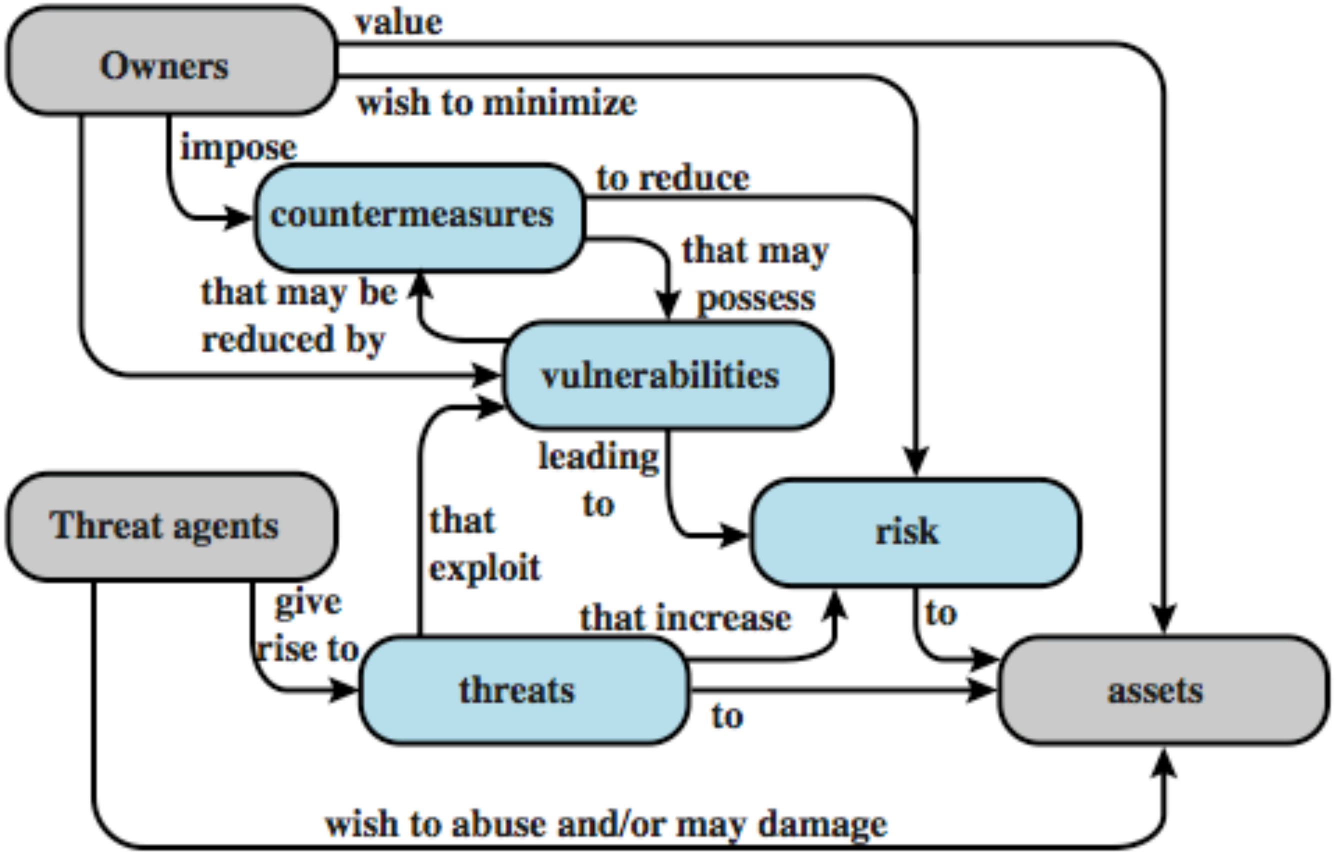
Challenges

- Why is security hard to achieve?
- Think about it for 2 min.
- Turn to your neighbor and discuss for 3 min.

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

Security Terminology



Vulnerabilities and Attacks

- system resource vulnerabilities may
  - be corrupted (loss of
  - become leaky (loss of
  - become unavailable (loss of
- attacks are threats carried out and may be
  - passive
  - active
  - insider
  - outsider

Countermeasures

- means used to deal with security attacks
  - prevent
  - detect
  - recover
- may result in new vulnerabilities
- will have residual vulnerability
- goal is to minimize risk given constraints

Threat Consequences

- unauthorized disclosure
  - exposure, interception, inference, intrusion
- deception
  - masquerade, falsification, repudiation
- disruption
  - incapacitation, corruption, obstruction
- usurpation
  - misappropriation, misuse