Säkerhet/Data security
EDA625

2017

Lärare: Paul Stankovski
Assistent: Adnan Mehmedagic
Kursansvarig: Ben Smeets

Introduction

- Don't forget to turn ON your cell phone, AFTER the lectures.....
- Course **organization** and **structure**.
- **Books** and further reading.
- Search for a **definition** of computer security.
- Propose: fundamental **design principles** for computer security.

Course Organization

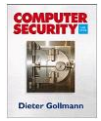
- Course WEB: **http://www.eit.lth.se/kurs/eda625**
- Lectures
  - 4 + 2 + 4 + 4 + 4 hours
- Instruction lessons
  - 2 hours
- Content:
  - Presentation of Course book
  - Feedback from projects, exercises
- 2 Projects and 3 Home Exercise problem sets
- Teachers:
  - Paul Stankovski, Adnan Mehmedagic (Project assistant)
- Course responsible (kursansvarig)
  - Ben Smeets

Prerequisites

- You need to be comfortable with Java programming.

Course material

- D. Gollmann: Computer Security, 3rd edition, Wiley & Sons, 2010, ISBN: 9780470741153



- Slide deck of lectures: via course web page
- Reading notes
- Assignments/home exercises: via course web page

A selection of books on Computer Security

- D. Gollmann: Computer Security, Wiley & Sons, 3rd ed, 2010
- C.P. Pfleeger: Security in Computing, Prentice-Hall, 4th ed, 2006
- W. Stallings, & L Brown, Computer Security: Principles and Practice, Prentice Hall, 3nd ed, 2015
- J.S. Park: AS/400 Security in a Client/Server Environment, Wiley & Sons, 1995
- L. Gong: Inside Java 2 Platform Security, Addison Wesley, 1999
- Ernst & Young: Logical Access Control, McGraw-Hill, 1993
- M. Gasser: Building a Secure Computer System. Van Nostrand Reinhold, 1988
- J. Viega, G. McGraw, Building Secure Software, Addison Wesley, 2002

Examination

- Exercises + Projects
  - See schedule on the course web
  - !!!!! Of exercises only first set has to be submitted
- Reports and code checked via **Urkund**
- Written exam
  - result determines your grade
    - Grade thresholds: 3: 30-39p, 4: 40-49 p, 5: 50-60 p
    - on exam 1p point can be given to reach next threshold if the written exam shows sufficient skills/knowledge for this course
- You need to pass the exam AND have all the reports and exercise approved before you are ready with this course

Exams

- **Thu 2017-03-16, 8 - 13, 3T:E210 and 3T:E421.**
- Wed 2017-04-19, 14 - 19, 3T:C525.
- Fri 2017-08-18, 8 - 13, 3T:C521.
- See more info on course home page

Projects and home exercises

- Groups of at most 2 persons.
- Hand in reports + code via email to
  - Paul.Stankovski.lu@analys.urkund.se **and**
  - paul.stankovski.@eit.lth.se
- Set subject to: EDA625:"here you put your text", see below

- Project assistance:
  - Adnan Mehmedagic will be available in Helsingborg
    Floor 6, EIT room C645 if available
    Details will be displayed on course web page
- All hand-ins must be ready 2016-03-15

E.g.
-----Original Message-----
From: Kalle Kallesson
Sent: den 15 mars 2017 23:59
To: Paul.Stankovski.lu@analys.urkund.se
Subject: EDA625: Vår lösning på …

Projects

There are 3 projects

- Project 1: On RSA and finding prime numbers
- Project 2: On setting up PKI for TLS and TLS
- Project 3: Controlling and security of remote light switch with Arduino system

  Project 3 runs as a laboratory lesson.
  Details will be displayed on course home page.
  At most 16 groups can do Project 3, first come first serve.

Project 1 is compulsory for all groups.

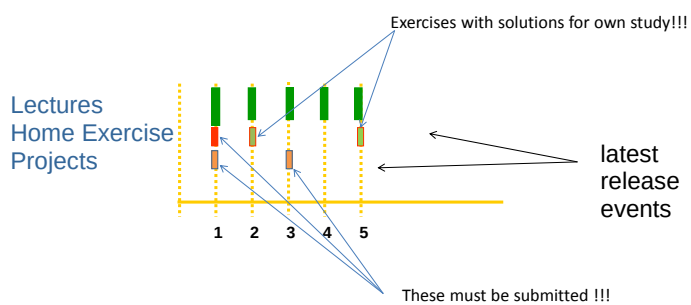
As long as place is available groups choose either
Project 2 or Project 3.

Home exercises

- Home exercise 1 must be submitted by all groups.

- Home exercises 2 and 3 are for self study and contain answers.

Time Line



Report format

- Report should be pdf file,
- **Names** on the first page,
- Image files repacked as document files are not accepted,
- Human-readable, concise and well-structured,
- Use 11pt - 12pt as font size,
- Exemplary reference handling,

(…more on course home page)

Course Objectives

General introduction to the very broad world of computer security

Insights into the fundamentals of:

- Cryptography
- Legal aspects
- Access control to systems
- Security Models and Operating System security
- Network- and web security
- Understanding the role of hardware for security
- Application and software security

End Terms

- Be familiar with the main concepts in computer security
- Have a basic understanding of security vulnerabilities
- Have a basic understanding of means and methods that provide increased security

Structure of the course

- Theoretical aspects
  - ✓Cryptography
  - ✓Authentication
  - ✓Access control structures
  - ✓Security models
  - ✓Security kernels
  - ✓Hardware security features
- Practical aspects
  - ✓Secure communication: TLS, IPSec, 4G, etc.
  - ✓Management aspects
  - ✓Legal aspects
  - ✓Operating system security: case studies
  - ✓Middleware security
  - ✓Web security
  - ✓Vulnerabilities: case studies, malicious software

Schedule 2017

Initial plan but likely it will be restructured a bit:
See course home page for updates

Föreläsning Övning	Datum	Ungefärligt innehåll	sidor i kursboken	PDF 2017	Från 2016
F1, F2	tis 17/1	Allmänt om datasäkerhet, kryptografi och nyckelförhandling.	1-48, 251-273, 275-292	TBA	Intro ,Lect1, Lect2
F3, Övning	ons 18/1	Forts. krypto, autentisering, lösenordskydd, lösenordsforcering, åtkomstkontroll och säkerhetsmodeller.	49-63 65-153, 205-233,	TBA	Lect3_A, B
F4, F5	ons 25/2	Säkerhets- och sårbarhetsanalyser, mjukvarusäkerhet.	235-249, 177-201	TBA	Lect4
F6, F7	ons 1/2	Operativsystem och webbsäkerhet.	385-400, 339-360,	TBA	Lect5 , Lect6
F8, F9	ons 8/2	Internet, nätverk, säkra exekveringsmiljöer, 3G-säkerhet och Android-säkerhet.	297-335, 364-370, 377-381	TBA	Lect7 , Lect9

More Security Courses at EIT

- Security / Computer Security (G2)
  - VT1, 7.5 credits
- Advanced Computer Security (A)
  - HT1, 7.5 credits
- Web Security (G2)
  - HT1, 4 credits
- Advanced Web Security (A)
  - HT2, 7.5 credits
- Cryptology (A)
  - HT2, 7.5 credits