Säkerhet/Data security EITF55 2021

Lärare: Ben Smeets
Christian Gehrmann
Kursansvarig: Ben Smeets

Introduction

- Goal of this course
- Course **organization** and **structure**.
- **Books** and further reading.

Goal for this course

- Be familiar with the main concepts in computer security
  - Definitions, models, evaluation, etc...
- Have a basic understanding of means and methods that provide increased security
  - Crypto, OS security, SSL, IPsec, key agreement protocols, etc...
- Have a basic understanding of security vulnerabilities
  - Attacks, implementation mistakes, etc…
- Get hands-on experience with RSA, digital certificates, secure connections, logon techniques, computer scanning, network sniffing, OpenSSL

Projects 1 & 2

Course Organization

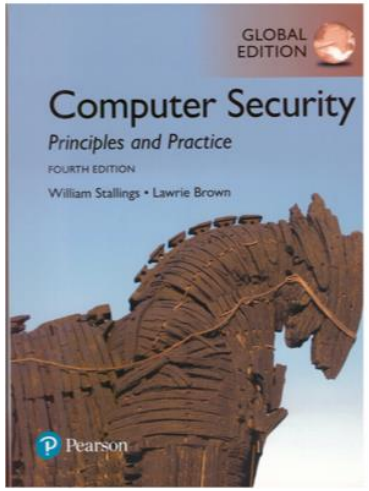
- Course WEB: **http://www.eit.lth.se/kurs/eitf55**
- Lectures
  - 4 + 2 + 4 + 4 + 4 hours
- Instruction lessons
  - 2 hours
- Content:
  - Presentation of Course book
  - Feedback from projects, exercises
- 2 Projects and 3 Home Exercise problem sets
- Teachers:
  - Ben Smeets, (Project assistant)
  - Christian Gehrmann
- Course responsible (kursansvarig)
  - Ben Smeets

Prerequisites

- You need to be comfortable with Java programming.

Course material

- W. Stallings, & L Brown, Computer Security: Principles and Practice, Global Edition, Prentice Hall, 4e,
- ISBN 9780134794181(ePub), 9781292220611(Paper)



- Slide deck of lectures: via course web page
  - Password to slides is given at first lecture.
- 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
- 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 the 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

- **Tenta**

Preliminärt planeras för ordinarie salstenta enligt TimeEdit men det kan komma ändras-

Tor 2021-03-18 14 - 19, 3T E210, 3T E230.

- **Omtentor**

Tor 2021-04-08 14 - 19, 3T E413.

Ons 2021-08-25 14 - 19, 3T C163.

- See more info on course home page

Projects and home exercises

- Groups of at most 2 persons.
- Hand in reports + code via email to
  - Ben.Smeets.lu@analys.urkund.se
- Set subject to: EITF55:”here you put your text”, see below

----Original Message-----
From: Kalle Kallesson
Sent: den 15 mars 2019 23:59
To: Ben.Smeetslu@analys.urkund.se
Subject: EITF55: Vår lösning på …

- Project assistance:
  - Book zoom session with Ben
    Details will be displayed on course web page
- Deadlines för
  - projekten är 2021-03-14 och för hemuppgiften **2021-02-09**,

Projects

There are 2 projects

- Project 1: On RSA and finding prime numbers
- Project 2: On setting up PKI for TLS and TLS

Project assistance

Once per week 4,5,6,7,8,9,10

For schedule see course web under “Inlämningsuppgifter”

https://www.eit.lth.se/index.php?ciuid=1368&coursepage=10035

Home exercises

- Home exercise 1 must be submitted by all groups.
- Home exercises 2 and 3 are for self study and contain answers. However, these are not yet updated to the 2019 course and still contain question that were covered only by the old course.

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, software, and IoT 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

Schedule 2021

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

Föreläsning Övning	Datum	Ungefärligt innehåll	sidor i kursboken
F1, F2	tis 19/1	Allmänt om datasäkerhet, kryptografi och nyckelförhandling. Några lagar rörande datasäkerthet.	Intro, 1_Overview
F3, Övning	tors 21/1	Forts. symmetrisk och asymmetrisk krypto, hash och mac algoritmer, Birthday paradox, digital signering, certificates, RSA, Diffie-Hellman, ECC.	2_Crypto1 3_Crypto2
F4, F5	ons 27/1	Lösenord, Användarautentisering och Access kontroll, access control policies, federation, Databas säkerhet,	4_Auth 5_Access
F6, F7	ons 3/2	Operativsystem och Virtualisering, Containers, Trusted computing	6_DB_OS 7_TComp
F8, F9	ons 10/2	DoS, DDoS, Brandväggar, DMZ, DNS, IPS, TLS, IPsec, Wireless kommunikation, LTE-säkerhet, WLAN Enterprise	8_Network 9_SecCom 10_WCom
F10, F11	ons 17/2	Mjukvara säkerhet, Common Criteria, och IoT-säkerhet. Övning på tenta,	11_SWsec 12_IoTsec

Password to lecture slides

- Will be given at first lecture:

More Security Courses at EIT/LTH

- 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