

Introduction

TDDE62 – Information Security:
Privacy, System and Network Security

Ulf Kargén

*Division for Database and Information Techniques (ADIT) at the
Department of Computer and Information Science (IDA)*

Agenda

- Topics
- Organization of the course
 - Exam
 - Labs
 - Prerequisites

Examiner

Ulf Kargén

Assistant professor @ IDA/LiU



Course web: <https://www.ida.liu.se/~TDDE62/>

Basic information

New course 2024

- This course together with TDDE63 replaces old course TDDD17
- Course consists of lectures and labs (project part of TDDD17 split out to TDDE63)
- Covers several distinct topics within the field of information security
 - Each topic is taught by different people with in-depth knowledge of the field

Examination

- Written exam (4 credits)
- 3 mandatory labs (2 credits)
- Labs are pass/fail
- Final grade depends on exam only

Course Topics

Network security

Three lectures, covering:

- **Secure network design**
 - Partitioning
 - Security devices (firewalls, IDS)
 - Trust relationships
- **Security of network protocols**
 - WiFi
 - ICMP, TCP, DNS, ...
- **Securing communications**
 - Network layer (IPSec)
 - Transport layer (TLS)

Andrei Gurtov

Professor @ IDA/LiU



Privacy

Two lectures, covering:

- **Basic concepts**
- **Privacy technologies**
 - Privacy-preserving communication, etc.
- **Privacy Preserving Data Publishing**
 - Differential privacy, k-anonymity, etc.

Jenni Reuben

PhD, Engineer @ Saab



System security

- **Introduction to system security**
 - Quick recap of basics
 - Hardware architecture
 - OS design
 - Security shortcomings in traditional OS and hardware architectures
 - Common attack techniques
- **Operating system security**
 - Security architecture
 - Security mechanisms
 - Hardware support

Ulf Kargén



Robert Malmgren

Independent consultant
Scada security expert



System security

- **Introduction to trusted computing**
 - Basic principles and concepts
 - TC technologies
 - Arm TrustZone, Intel SGX, etc.

- **Trusted computing + TC lab info**
 - Introduction to the TPM
 - Lab intro
 - TC wrap-up

Ben Smeets

Professor @ Lund

Engineer @ Ericsson

Expert in trusted computing
and mobile devices



Ulf Kargén



System security – malicious code

- **Introduction to malware defence**
 - Goal of malware writers
 - Infection methods
 - Antivirus and evasion techniques
- **Mobile malware and machine learning for malware defence**
 - Malware on mobile platforms
 - Machine learning for malware detection and analysis

Ulf Kargén



Organization

Examination

Written exam – 4 hp/ECTS

- Covers all topics of the course

Old TDDD17 exams available on course web site

- Should give a good idea about exam structure and scope also for this course
- **However**, note that
 - TDDD17 exam was 2 hp, this exam is 4 hp – more in-depth knowledge required to pass
 - Content on system security has been expanded in TDDE62

Labs

Three mandatory labs

- Two on network security
 - **FW** – Analyse network requirements and risks and configure a firewall
 - **Snort** – Configure a Network Intrusion Detection System (NIDS) to detect attacks
- and one on trusted computing
 - **TC** – Build a secure application using a (simulated) TPM
- Need to sign up in Webreg. Deadline **January 19**
 - **Unregistered students not allowed to register**, contact me if you have been admitted late to the course and are not registered by the deadline
- Hard hand-in deadline **March 15**
 - Hand in before this time to allow time for grading and possible re-submission!

Prerequisites

- Basic security course is required
 - We will assume that you know basic security concepts
- Network Security – Basic knowledge of TCP/IP networks is recommended
- System Security – Basic understanding of operating system design and computer hardware is recommended.

Other information

- Lecture slides will be made available on the course web site
 - Usually the day before, ***but no guarantees***
- Course literature on the course web site
 - Hand-outs
 - Collection of articles and book chapters