TDDD17

Information Security

Department of Computer and Information Science (IDA)

Division for Database and Information Techniques (ADIT)

LiU EXPANDING REALITY

Agenda

- Organization of the course
- Topics
- Prerequisites
- Examination

Examiner
Ulf Kargén

Postdoc @ IDA/LiU

Doing research in software and systems security

Course web page: https://www.ida.liu.se/~TDDD17/

Basic information

- Course runs over whole semester and consists of two parts
  - First period: Lectures + labs + exam + start of project
  - Second period: Independent project work
- Written exam (2 credits), labs (1 credit) and project (3 credits)
  - Final grade depends on exam
  - Labs and project are pass/fail only.
- Course covers several distinct topics within the field of information security
  - Set of topics updated over time
  - Each topic is taught by different people with in-depth knowledge of the field

TOPICS

Network security

- **Secure network design**
  - Partitioning
  - Security devices
  - Trust relationships
- **Network security protocols**
  - Network layer (IPSec)
  - Transport layer (TLS)

Andrei Gurtov

Professor @ IDA/LiU

Malware defence

- **Introduction to malware defense and traditional malware detection**
  - Goal of malware writers
  - Infection methods
  - Techniques used by antivirus products and evasion techniques used by malware writers

Ulf Kargén

Postdoc @ IDA/LiU

- **Mobile malware and machine learning for malware defence**
  - Malware on mobile platforms
  - Machine learning for malware detection and analysis

Alireza Mohammadinodooshan

PhD student @ IDA/LiU

Privacy

- **Two Lectures:**
  - Basic concepts
  - Privacy technologies
  - Privacy Preserving Data Publishing
    - Differential privacy, etc.

Jenni Reuben

PhD, researcher @ FOI

System security

- **Introduction to system security**
  - Quick recap of basics
    - Hardware architecture
    - OS design
  - Security shortcomings in traditional OS and hardware architectures

Ulf Kargén

Postdoc @ IDA/LiU

- **Operating system security**
  - Security mechanisms
  - Hardware support

Robert Malmgren

Independent consultant

Scada security expert

IDG top security expert

System security

- **Trusted computing**
  - Basic principles
  - Virtualization
  - Execution environments
  - Mobile devices

Ben Smeets

Professor @ Lund

Engineer @ Ericsson

Expert in trusted computing and mobile devices

ORGANIZATION

Labs

- Two mandatory labs
  - Firewall configuration
    - Analyse network requirements and risks and configure a firewall
  - NIDS
    - Configure a Network Intrusion Detection System (NIDS) to detect attacks

- Need to sign up in Webreg. Deadline **January 23**
  - Unregistered students not allowed to register, contact me if you have been admitted late to the course and are not registered by the deadline
- 4 scheduled lab sessions. Check course web page!
- Hard hand-in deadline **March 15**
  - Hand in before this time to allow time for grading and possible re-submission!

Project

- Work in groups of two (no exceptions)
- Choose from a list of topics (first-come-first-serve, sort of)
  - List of projects will be published **January 31 at 18:00**
  - See detailed instructions on web page
- Must meet intermediate milestones and deadlines
- Must produce written report and presentation

Prerequisites

- Basic security course is required
  - We will assume that you know some basic things

- Network Security – Basic knowledge of TCP/IP networks is recommended
- System Security – Basic understanding of operating system design and computer hardware is recommended.

Prerequisites

- Capable of independent study and research
  - Essential in the project phase…
  - …but also for when studying for the exam.
- Capable of producing a high-quality project report

Other information

- Hand-outs will be available on the course homepage before lectures (usually the day before, ***but no guarantees***)

- Course literature on the course homepage
  - Hand-outs
  - Collection of articles and book chapters

Previous year's course evaluation

- Overall score last year was 3.7 (of 5)
- Scores of all evaluation items available at: https://admin.evaliuate.liu.se/search?lang=en

Comments from students on things to improve:

- Supervisor didn't seem to have enough time for giving feedback etc.
  - **Action:** One supervisor who felt he didn't have enough time to provide good supervision has opted out from participation this year.
- Halftime-presentation placed on first day after the exam-period was stressful
  - **Action:** Tried to have some more margin between exam period and progress presentation.

Previous year's course evaluation (cont.)

- The lectures were too disjoint
  - **Comment:** The idea with the course is to give a broad view on different "hot topics" in information security.
- The quest lectures in privacy could be improved
  - **Action**: We have discussed improvements with Jenni.
- The project was good but took way too much time to only be worth 3 ECTs.
  - **Action**: This is a known issue with the course. Future plan is to split course up into a "lecture-labs-exam" course and a dedicated project course.

Linköpings universitet

expanding reality

www.liu.se