

Welcome to: EITN50 Advanced Computer Security (Avancerad Datorsäkerhet)

Start 15:15

I would give all my fame for a pot of ale, and safety
Henry V: Act 3, Scene 2

2021-08-09

EITN50 Dept. Electrical and Information Technology

1

Introduction

- Goal of this course and contents
 - Course organization and structure.
 - Course literature & books.
-
- As a rule all lectures will be on-line via Zoom

2021-08-09

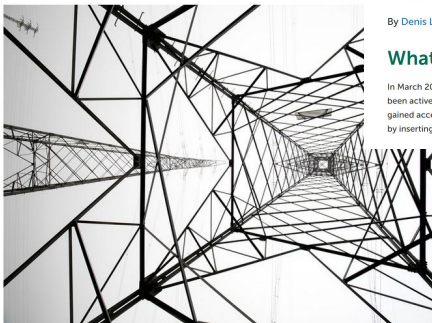
EITN50 Dept. Electrical and Information Technology

2

WE ARE INCREASINGLY DEPENDING ON SECURE IT SYSTEMS

KIM ZETTER SECURITY 03.03.16 07:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



SECURELIST

THREATS

CATEGORIES

TAGS

STATISTICS

ENCYCLOPEDIA

APT REPORTS

LuckyMouse hits national data center to organize country-level waterholing campaign

By Denis Legezo on June 13, 2018, 10:00 am

What happened?

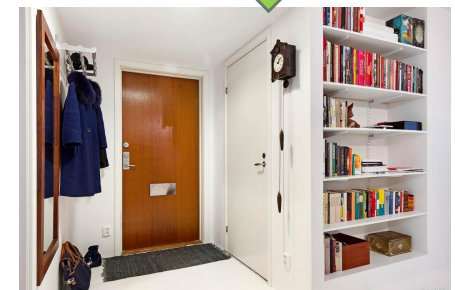
In March 2018 we detected an ongoing campaign targeting a national data center in the Central Asia that we believe has been active since autumn 2017. The choice of target made this campaign especially significant – it meant the attackers gained access to a wide range of government resources at one fell swoop. We believe this access was abused, for example, by inserting malicious scripts in the country's official websites in order to conduct watering hole attacks.

2021-08-09

EITN50 Dept. Electrical and Information Technology

3

Send to you?

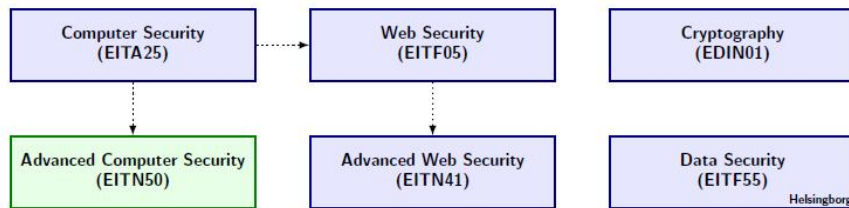


2021-08-09

EITN50 Dept. Electrical and Information Technology

4

Security Courses



Teachers EITN50

- Ben Smeets (kursansvarig)
ben.smeets at eit.lth.se
- xxxxx(support and handling projects)

Course Objectives

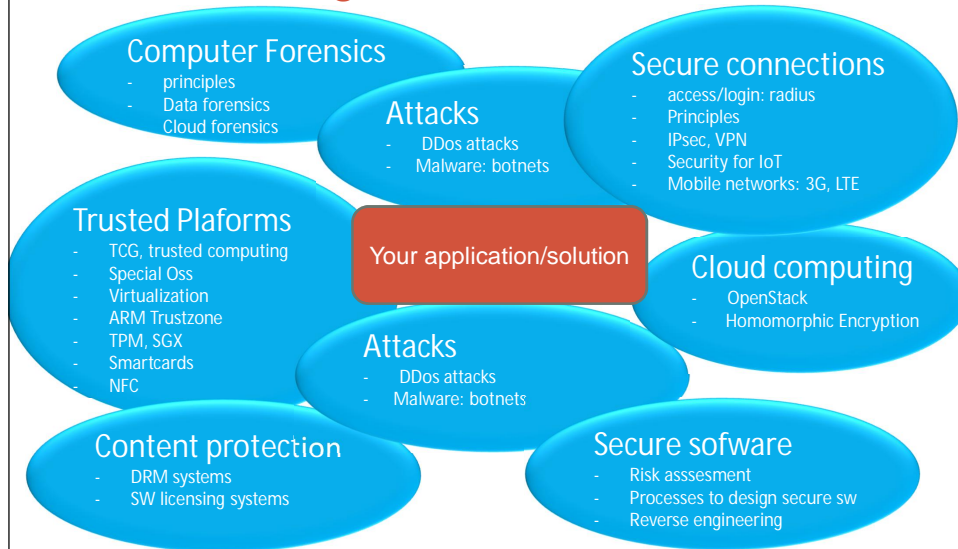
The goal of this course is to give the students an in-depth insight into the main problems and solutions within security for computers, embedded devices and networks.

As such it deepens acquired knowledge on computer security from earlier courses and gives an analytic understanding behind today's security solutions. This will allow the student to select by him/herself among existing solutions and/or to present solutions with good quality.

End Terms

- **Be familiar with the challenges of building a secure system** using trusted computing, secure networking and identity solutions
- Have a **basic understanding of means and methods** that provide increased security
- Have a **basic understanding of risks**
- How to act when something goes wrong
- Got some documented **hand-on experience in selected areas**

Course Organisation - content



2021-08-09

EITN50 Dept. Electrical and Information Technology

9

Course Organisation – work setup

- **Lectures**
 - 26 hours
- **5 projects and quizzes**
 - 170 hours
- **Teachers:**
 - Ben Smeets (kursansvarig)
 - Mustafa Albayati (support with projects)
- **This course requires students to seek much information on their own – with the provided material helping to narrow down your search for information.**
- **WEB** <http://www.eit.lth.se/kurs/eitn50>

2021-08-09

EITN50 Dept. Electrical and Information Technology

10

IMPORTANT

- The projects you do in groups of two people. Send me the names of the persons in your group and I will compile a list,

2021-08-09

EITN50 Dept. Electrical and Information Technology

11

Examination setup

- **Grading scale:** TH - (U,3,4,5) - (Fail, Three, Four, Five)
- **Assessment:** To pass this course all projects must be approved and all theme tests (5 quizzes) must be passed.
- **Quizzes:** Thresholds for passing is 70%.
- For grade 4 or higher you need to answer/do the B type assignments parts of at least 4 of the 5 projects.
- When you qualify for grade 4 you can obtain grade 5 through an oral exam. **Students should always sign-up for such or any other oral exam.**
- **signup for oral exam is required.**
Send email to Ben or Erik Göthe (kursexp@eit.lth.se)
- **Re-examination** in ordinary re-examination period: **Oral exam.**

2021-08-09

EITN50 Dept. Electrical and Information Technology

12

Final grading

- For grade 4 or higher you need to answer/do the B type assignments parts of at least 4 of the 5 projects.
- When you qualify for grade 4 you can obtain grade 5 through an oral exam
 - Note: you have to ask Ben or course admin (Erik Göthe) at EIT for this/any oral exam

5 Projects/Laboratory (with links)

Project Lab	Release Date (latest)	Planned Content	link to the assignment	First Deadline (at 23.59)
A	4/9	Forensic Analysis of disc and USB drive image	Forensics	17/10 quiz
B	4/9	Object security in communication	Objsec	26/9
C	17/9	TPM use	TPM	3/10
D	2/10	Anatomy of an Exploit	Exploit	20/10
E	2/10	Design secure camera	Camera	24/10



Project index

Quizzes close at 28/10
Last report update 20/10
Except project E: 24/10

Group/Project work

- Groups of 2 persons
- 5 Projects (previous slide)
 - 1 project is examined by a quiz
 - 4 written reports for the other projects. Projects have A and B type assignments. A type are mandatory and B type you need to do if you want a grade 4 or higher.
- Try to work at home but In the laboratory at 4th-floor E-building you have PC's that you can use to solve the problems.
- The times in TimeEdit shows the bookings made for this course but you can outside these hours use the laboratory as well. *However outside the reserved bookings you have to give room to bookings of other courses.*

Covid-19 implications for projects

- Conditions for projects are as follows. Like previous years most projects can be done at home. For some (parts) you need to run a Virtual Machine, in Virtual Box. Therefore we keep the possibility to do those parts in our labspace. For that reasons, we keep the labspace bookings (shown as "Projekt) in Time-Edit.
- Note that when you use our labspace you have to adhere to the university guidelines due the risk of Covid-19 virus spreading. **You are not allowed in the labspace to sit shoulder-to-shoulder and the amount of people is restricted to.** Daniel will keep office hours and you can book meetings with him. He has instructions and decides when to use protective masks when social distancing cannot not be kept.

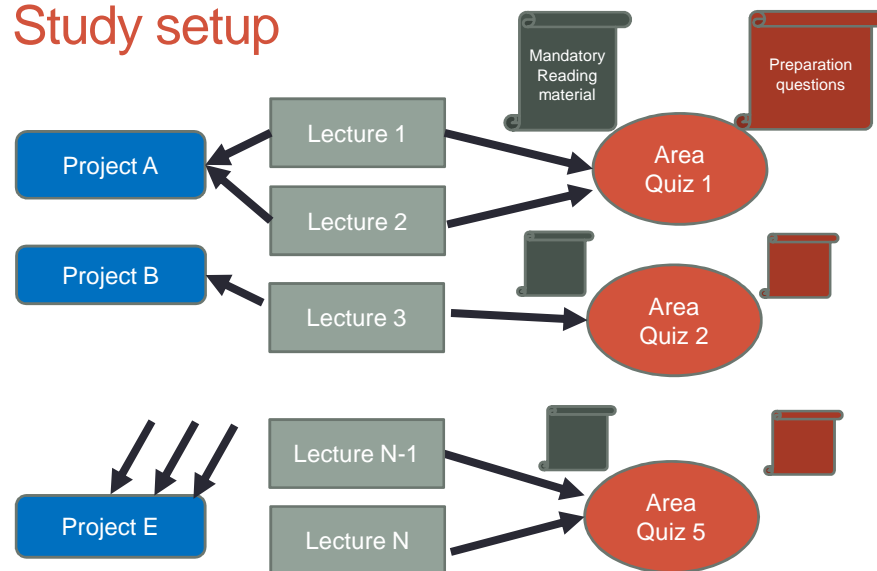
Reports - format

- **Reports must contain description/documentation of your project work so others understand what you have done/can repeat your experiments.**
- Each report must contain the following statement:
“*Rapporten är eget original arbete och källor av all icke egen material är angiven*”
 - **the names of the authors and their group number: adsecXY**
- Reports may be used during discussions or oral exam
- Reports should be submitted in pdf/txt form (not as scanned images in pdf file)
- Reports will be screened using “Ouriginal (Urkund)” for plagiarism
info: <https://www.lub.lu.se/sok/urkund>).

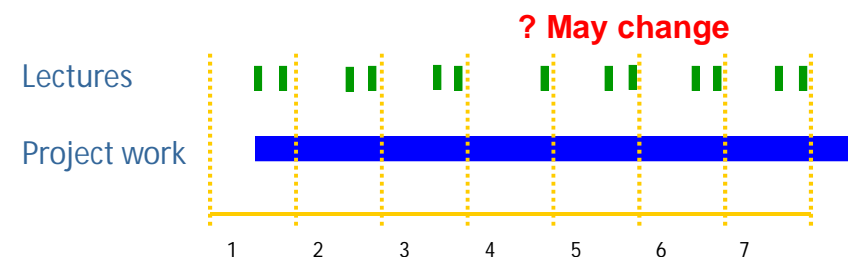
Quizzes

- There will be 6 mandatory short quizzes available via course Canvas
- The purpose of these quizzes is to test your overall understanding in 5 different areas and 1 quiz is to test you on one of the projects/labs in this course.
- Some questions are simple and some may require you to think a while. Of the possible answers **you have to choose the BEST alternative** (in case you think more than one make sense).
- **You have 2 regular attempts to pass the quizzes.** You can do a quiz whenever you want after it is made available. But you will have at most two hours from starting a quiz until you have to submit your answers. For passing 70% of your answers must be correct. Quizzes close on October 28. If you need to more than two attempts you need to contact Jonathan or Ben. If this happens too often we cap your maximum grade to 3

Study setup



Time Line



Final remark

- In this course it is expected that YOU look for additional information beyond what is in the slides and support material.
- In the quizzes often more than one answer may be possible. Think what is then the answer that fits best. Do not rush through the quiz. You have ample time to think and do go through the preparation material for the quizzes.