TEKNILLINEN KORKEAKOULU

T-110.4200/4206

Tietoturvallisuustekniikat (3 op)
Information Security Technology (3 ects)

Introduction for both courses

T-110.4200/4206 Information Security Technology

- Prerequisites: ”Good general knowledge of computer science”
  - Basic understanding of operating systems, programming, computer networks etc. assumed
  - Minimum requirement: T-110.2100, T-110.1100 or equivalent knowledge
- Goals:
  - Introduce basic concepts and provide a general view on the field of computer security, including networked computer security and network security
- Different codes for different languages, this year no big difference
  - T-110.4200 in Finnish, 4206 in English

TEKNILLINEN KORKEAKOULU

T-110.4200/4206 Practical Issues

- Please register in at OODI! (if you haven't yet)
  - Needed for the home exercises
- Monitor Noppa for information
  - https://noppa.tkk.fi/noppa/kurssi/t-110.4206/
- Newsgroup (otax): opinnot.tik.tietoturva
  - This is a good place to ask questions of general interest
- E-mail: titu@tml.hut.fi
  - This is the preferred way to ask questions about individual person's assignments etc.
- IRC #titu
- Assistants: Janne Kaavi and Nina Lehtinen

TEKNILLINEN KORKEAKOULU

T-110.4200/4206 Lectures

- Lecturer: Timo Kiravuo
- Lectures on Wednesdays at 14.15-16.00 and Thursdays at 16.15-18.00 in lecture room T1
  - Lecture language is English
- Lectures are organized according to the course book
- Slides will be published on the course web page

TEKNILLINEN KORKEAKOULU

T-110.4200/4206 Exercises

- Homework, online
- You need
  - Computing center and Niksula user account
- Pass/fail grading
- The exercises are relatively easy (we think) and are intended to illustrate key concepts and enhance the learning experience

TEKNILLINEN KORKEAKOULU

T-110.400/4206 Course Requirements

- Requirements for passing the course:
  - Exercises
  - Exam
    - Lectures
    - Lecture slides
    - Book
    - Exercises
    - Questions in Finnish and English
    - Answer in Finnish, Swedish or English
- Course book: Dieter Gollmann: Computer Security, 2nd edition

TEKNILLINEN KORKEAKOULU

Exam: Question Formats

- Concepts and acronyms
  - Q: Firewall (1p)
    - A: A device which limits traffic between two networks
    - A: An implementation of the security policy, controls information flows
  - Q: MAC (1p)
    - A: Mandatory Access Control, the system enforces access rules
    - A: Message Authentication Code, a cryptographic checksum (hash)
    - A: Message Authentication Code, ensures data integrity in communications
  - A short explanation of the concept or acronym is enough
- Justify the following statements either correct or false
  - Q: Bell - LaPadula is a model for information integrity (1p)
    - A: False, it is a model for information confidentiality
  - Q: All systems should have antivirus protection (1p)
    - A: Correct, Viruses may be transmitted over any media, like diskettes or e-mail
    - A: False, a dedicated system like an Unix database server is not likely to have viruses
  - Both the correct and false answer may be accepted for a particular question, the key is in being able to justify your position

Exam: Question Formats...

- Several short questions, like "How does a packet filtering firewall work? (3 p)"
  - A written reply, with a diagram if possible
  - Also questions which require applied knowledge, like "What would happen if message authentication codes (crypto checksums) were removed from a crypto protocol, like SSH, SSL or IPSec?".
- Essay (sometimes)
  - Requires you to show that you can discuss a subject in an intelligent manner. Bullet points or diagrams are not sufficient here, you should aim to write something that looks like an article, which could be published in a magazine.

Exam: What to answer

- Points will **not** be given for answers, which:
  - Discuss the subject without actually answering the question
  - Are correctly remembered from the course book, but do not actually answer the question
  - Contain the right terms, but do not form meaningful sentences in English, Finnish or Swedish
- We try to ask questions which require applied knowledge, which means that just blindly memorizing the slides and book should not get you through the exam
- Knowing the meaning of a technology or a concept is worth more points than getting the name exactly right