IMT6031 Intrusion Detection and Prevention - 2014-2015

Course code:
IMT6031

Course name:
Intrusion Detection and Prevention

Course level:
PhD (syklus 3)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First half of the autumn semester

Language of instruction:
English

On the basis of:
IMT4741 Intrusion Detection and Prevention, or equivalent

Expected learning outcomes:
Knowledge

- The candidate possesses knowledge at the most advanced frontier in the field of intrusion detection and prevention. The candidate has mastered academic theory and scientific methods in intrusion detection and prevention.
- The candidate is capable of considering suitability and use of different methods and processes in research in the field of intrusion detection and prevention.
- The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in the field of intrusion detection and prevention.

Skills

- The candidate is capable of formulating problems, planning and completing research projects in the field of intrusion detection and prevention.
- The candidate is capable of doing research and development at a high international level.
- The candidate is capable of handling complex academic tasks. The candidate can challenge established knowledge and practice in the field of intrusion detection and prevention.

General competence

- The candidate is capable of identifying relevant – and possibly new - ethical problems and exercising research in the field of intrusion detection and prevention with academic integrity.
- The candidate is capable of managing complex interdisciplinary tasks and projects.
- The candidate is capable of disseminating the results of research and development in the field of intrusion detection and prevention through approved national and international publication channels.
- The candidate is capable of taking part in debates in international forums within the field of intrusion detection and prevention.
- The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of intrusion detection and prevention.

Topic(s):

1. Introduction – definition and classification of IDS, basic elements of attacks against computer hosts/networks and their detection
2. Misuse-based IDS
3. Anomaly-based IDS
4. Testing IDS and measuring their performances
5. Automata theory and intrusion detection
6. Information theory and intrusion detection

Teaching Methods:
Lectures
Laboratory work
Exercises
Project work

Form(s) of Assessment:
Oral exam, individually
Evaluation of Project(s)

Form(s) of Assessment (additional text):

- Oral exam
- Project evaluation of one project
- Both parts must be passed.

Grading Scale:
Pass/Failure

External/internal examiner:
Project: one internal examiner. Every 4th year, an external examiner is used, next time in 2015.

Oral exam: two internal examiners. Every 4th year, an external examiner is used, next time in 2017.

Re-sit examination:
The whole course must be repeated

Tillatte hjelpemidler:

Examination support:
Calculator, dictionary

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Slobodan Petrovic

Teaching Materials:
Books:

1. Rebecca Gurley Bace, Intrusion Detection, Macmillan, 2000.

2. Jack Koziol, Intrusion Detection with SNORT, SAMS, 2003.

3. David J. Marchette, Computer Intrusion Detection and Network Monitoring - A Statistical Viewpoint, Springer Verlag, 2001.

4. Richard Bejtlich, Extrusion Detection - Security Monitoring for Internal Intrusions, Addison-Wesley, 2005.

5. Stephen Northcutt, Judy Novak, Network Intrusion Detection, 3rd edition, New Riders, 2003.

Various papers (available on-line)

Additional information:
There is room for 50 students for the course.

Publish:
Yes

Home page:
http://www.hig.no/imt/emnesider/imt4741