NTNU

Studieplan 2011/2012

PhD programme in Information Security

Studieprogramkode
PHD-IS

Innledning

Information security is a cross-cutting concern which is most closely related to Computer Science and Mathematics; in the context of the categorisation by the Norwegian Higher Education Institutions, this is most closely aligned with Mathematics and Natural Sciences, Information and Communication Science, and Security and Vulnerability. Although particularly at the research level it is inevitable that novel specializations arise whilst others decline in interest, the undergraduate curricula maintained by the joint IEEE/ACM Computing Curricula committee provide some indication of key areas; these cover both theoretical and mathematical foundations but also cryptography and abstract models of security-related properties as well as security-related aspects of application domains such as operating systems, networks, biometrics, or forensics. Moreover, ancillary domains such as policy, operational issues, and security management are also encompassed by these curricula and considered mainstream information security research, as is research on risk and threat analysis and vulnerabilities.

Similarly more applied sub-domains are also identified by the CISSP (Certified Information Systems Security Professional) certification1 and similar professional-level certification and training programmes.

As with any doctoral programme, however, one of the main objectives is to ensure that mathematical and scientific methods are acquired by students enrolled in the programme, providing the foundation to undertake largely independent research on completion of the programme whilst having undertaken specialized research within the domain of information security during the course of the programme.

Studiets varighet, omfang og nivå

The programme is considered part of the 3rd higher education cycle, namely the PhD level. The PhD programme is arranged such that it normally can be completed within a three year efficient research education period. Of this period, at least one semester (30 ECTS Credit Points) is reserved for organized teaching and learning in a form and manner appropriate to the study outcomes including but not limited to courses and seminars.

This taught component must be completed at the time of submission of the dissertation, but unless set out otherwise in case of a conditional admissions (see Course Structure), no further requirement on the time at which the taught credit points are to be accrued are made.

The PhD programme must be completed (as determined by the date at which the viva voce takes place) within eight years from the date of admission as specified in the letter of admission.

The above period may be prolonged in case of formal interruption of studies or where extenuating circumstances apply. Unless such extenuating circumstances are required to be considered by law, they are decided on a case by case basis by a committee consisting of the Director of Academic Affairs, the Director of the PhD programme in Information Security, and at least one of the academic supervisors of the candidate by unanimous consent. Where such consent is not reached, the application for prolonging the study period will be considered as denied.

A prolonged maximum study period may also be approved by the Admissions Board in consensus with the Director of Academic Affairs in cases where applicants wish to pursue the PhD programme on a part-time basis. In such cases the maximum period must not exceed ten years and will be noted in the letter of admission.

The PhD programme is a supervised programme. The PhD student will have regular contact with his or her supervisors and will typically participate in a research group.
For candidates pursuing their studies on a full-time basis, the targeted time to completion of studies is three years or four years in case the candidate holds relevant teaching duties.

Forventet læringsutbytte
The successful completion of a Ph.D. programme provides a number of specific learning outcomes listed in the sections below. Beyond these, it introduces candidates to the methods and principles of scientific inquiry. This is taught both explicitly in specific courses, and also attained by collaboration with researchers including the candidate's supervisors and research groups. This provides insights into the processes of research and project management beyond the immediate remit of a doctoral research project.

The specific learning outcomes expected to have been achieved upon completion of the study programme are grouped into three categories in accordance with the national qualification framework: Knowledge, Skills, and General Competence. These learning outcomes as listed below, relate to the generalised descriptions for Ph.D. level study released by Kunnskapsdepartementet (KD) {http://www.handboka.no/Sak/Rundskriv/Kd/kd5673.htm}}.

Knowledge

The Knowledge learning outcomes are primarily achieved through the development of the thesis and the guidance by the supervisor during the Ph.D. programme. The development of the thesis from the preparation of peer-reviewed publication during the programme ensures the student is at the forefront of research in their field. The taught component has amandatory course which teaches the foundation of ethical research and research methodology, and the optional courses provide an understanding of the current state in a specific research area.

1. Knowledge of the most advanced research in the candidate´s specialisation area of Information Security.
2. Strong understanding of academic theory and the preparation of high-quality research.
3. Ability to select appropriate research methods and sampling techniques for the candidate’s research field.
4. Understanding the current state-of-the-art and applying knowledge to the development of new knowledge, theories and presentation of research in Information Security.

Skills

The learning outcomes in the Skills domain relate to activity in the research community. Specifically, this refers to the participation and possible leadership of industrial or academic research projects. Although the latter is not achieved or typically achievable by candidates themselves as part of their studies, successful completion of the programme enables to translate the understanding of processes and dynamics from observations and taught elements into such abilities. As with the previously described Knowledge outcomes, the preparation of the thesis forms a significant part of the development of these learning outcomes. The experiences passed on from the supervisor and in the writing of peer-review publications contribute to the student's ability to interact with the international research community and to disseminate their research findings.

1. Ability to provide management and planning of research projects in Information Security in Academic and Industrial environments.
2. Ability to support and participate in Industrial and Academic research projects at a high international level.
3. Ability to comprehend complex academic issues and the related ethical considerations.
4. Ability to understand and challenge the existing knowledge and practise in Information Security.

General Competence

The development of the general competence required to participate actively and constructively in the international research community, and to interact with other collaborators from outside Information Security --- considering that the discipline is often called upon to serve as a bridge to other disciplines --- and the general public are covered by a more varied set of learning outcomes. The thesis preparation still has a major impact in teaching the student how to organise and explain their thoughts and research but these outcomes go beyond the formal written presentation of scientific research. The ability to speak with clarity about these advanced research topics needs to be developed and is provided by the student's attendance at conferences for the presentation and discussion of publications, in workshops and tutorials within IMT and culminating with the public oral defence of their research. Mandatory taught courses in research ethics and methodology are used to develop an understanding of the wider societal impact of their research, and the techniques to work with other disciplines and conduct projects to provide high-quality ethical research in diverse areas which may benefit advanced understanding of Information Security.

1. Ability to identify new problems arising from recent developments in Information Security and assess their impact on society.
2. Ability to conduct ethical, scientifically sound research in areas of Information Security at the boundaries of existing laws and accepted limits.
3. Ability to manage interdisciplinary projects with diverse groups of individuals to bring results in information security to fruition,
4. Ability to organize and participate in research and development through established national and international research frameworks.
5. Ability to argue the merits, limitations, and possibilities of new developments in information security in recognized international forums.
6. Capability of applying latest abstract research within information security to specific real-world problems in creative and innovative ways.

Målgruppe

The target group for the PhD study programme encompasses candidates holding a relevant Master degree whose degree classification matches the requirements set out in the section Admission Criterias. Such candidates may wish to pursue careers as academics, research scientists, or to hold advanced positions related to information security in industry and government.

Opptakskrav og rangering

In order to be admitted to a PhD programme, the applicant must normally hold a five-year Master degree or equivalent combination of undergraduate degree and Master level degree, which the university college has approved as basis for admission to the PhD programme.

Master degree programmes relevant for the purposes of the PhD in Information Security include but are not limited to Mathematics, Computer Science, and Electrical Engineering and combined degree programmes incorporating substantial elements of these. Further degree programmes in different or related subjects may be approved on an individual basis taking particularly the proposed area of doctoral research of a candidate into account.

For an application to be accepted, the above degrees must also satisfy minimum requirements for degree classification. Based on the common Norwegian degree classification scheme, these requirements are:

- Average grade for the Bachelor degree must be A, B or C
- Average grade for subjects/courses at Master level must be A or B
- The Master thesis must have grade A or B

These requirements may be waived or reduced in part by unanimous vote of the Admissions Board (see further information about the admission prosess here) in exceptional circumstances. These include cases where an equivalent degree classification cannot be established or mapped onto the above scale.

Moreover, waivers and reductions may also form part of a conditional admission. These may be granted if the Admissions Board is satisfied that extenuating circumstances are applicable for a given candidate. Failure on the part of the candidate to meet the requirements imposed by the Admission Board as part of the admission letter will result in the admission considered to be rejected effective with the date of the original decision regarding the application.

For further discussion of these requirements also refer to the website.

Studiets innhold, oppbygging og sammensetning
The taught component of an individual PhD study plan instance must comprise at least 30 ECTS credit points. These 30 credit points must be part of an approved study plan which may encompass more than 30 credit points together; the initial study plan is must form part of the application to the PhD programme but may be amended and altered subsequently. Any such changes must be submitted in writing and approved by the Director of the PhD programme.

If, as part of the elaboration of an individual study plan, it is determined that a candidate’s research or courses forming the core of the study plan have further prerequisites, a candidate can be required to take additional courses and seminars in excess of the 30 ECTS credit points.

No credit points are accrued for courses taken at the Bachelor level, but up to 10 credit points may be approved for courses at the Master level.

No courses forming part of the study plan may have been previously credited in the course of another degree programme. A review of individual study plans will ensure that overlap between courses credit to other degree programmes and the present study plans are minimized. From time to time courses may also be taken for credit from other accredited institutions provided that it can be established that the content and level of such courses is equivalent; the approval process for such external courses is as noted above. If a candidate has taken courses prior to commencing studies in the PhD programme, credit points which have not previously been credited to another degree programme may be credited provided that the examination awarding the marks and concomitant credit points has taken place less

than five years before the start of the studies under the PhD programme. If credit points are to be credited for courses which were not marked on a Pass/Failed basis, they must have been marked at either the A or B grade or equivalent.
Courses covering the area of Ethics and Legal Aspects of Scientific Research, IMT6001, and Introduction to Information Security, IMT6011, are mandatory and must be taken at the PhD level.

The list of approved courses and their availability in a given time period is updated from time to time and is considered at the time of submission of the individual study plan and when such study plans are considered for changes or amendments. The list of approved courses is hereby formally included by reference into this document.

See also Section 4.2 of §4 in the Regulation for the degree of Philosophiae Doctor (PhD) at Gjøvik University College (website).

Tekniske forutsetninger
No technical requirements are imposed at this point.

Sensorordning
In accordance with current recommendations from the Norwegian Association of Higher Education Institutions, all modules taken as part of coursework requirements will be graded as pass/fail. Where modules are approved from other study programmes such as the Master level or other institutions which do not follow the pass/fail schema, the equivalent of a good or very good (A/B) grade will be considered as sufficient to merit a pass for the nostrified module.

Individual courses may have further requirements and arrangements for examination; this is detailed in the course descriptions which may also change for each offering of a given module and hence are to be considered binding only for the cycle in which the module is offered.

Internasjonalisering
Establishing links to academics outside the college and particularly internationally is highly desirable, as is an exposure to working conditions and academic approaches at other, international institutions.

An individual study plan should therefore identify one or two opportunities for gaining experience at overseas institutions over the course of the doctoral studies. Whilst overseas visits and stays are not mandatory and need not be arranged at the time of drawing up an individual study programme, the need for making appropriate arrangements with hosting institutions makes taking such steps early on advisable.

The duration of the overseas stays should be several weeks to ensure sufficient exposure to the research environment at the hosting institution.

Klar for publisering
Ja
Godkjenning
The study plan for the PhD programme in Information Security is approved by the GUC Programme Committee in June 2010.

Utdanningsnivå

Doktorgrad

Courses

Emnekode	Emnets navn	O/V *)	Studiepoeng pr. semester	
			S1(H)	S2(V)
IMT6011	**Introduction to Information Security**	O	5	5
IMT6001	**Ethics and Legal Aspects of Scientific Research**	O	5	5
IMT6041	**Selected Topics in Cryptology**	V	5	
IMT6031	**Intrusion Detection and Prevention**	V	5	
IMT6021	**Foundations of Information Security**	V	5	
IMT6051	**Wireless Communication Security**	V	5	
IMT6061	**Risk Management II**	V	5	
IMT6081	**Modern Cryptology**	V	5	
IMT6091	**Computational Forensics**	V	5	5
IMT6111	**Risk Management I**	V	5	
IMT6121	**Authentication**	V	5	5
IMT6071	**Biometrics**	V		5
IMT6101	**Computational Intelligence**	V		5
		Sum:	0	0

*) O - Obligatorisk emne, V - Valgbare emne

Emneoversikt

IMT6011 Introduction to Information Security - 2011-2012

Emnekode:
IMT6011

Emnenavn:
Introduction to Information Security

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst
Vår

Språk:
Engelsk

Forventet læringsutbytte:
Having completed the course, the student should have

- developed an advanced understanding of core issues from different sub-areas of information security research including security models, cryptography, network and operating system security, security management, and security engineering
- achieved in-depth knowledge on one of the core areas through independent study
- developed analytical skills enabling them to critically assess research publications and presentations

Emnets temaer:

- Key results in the theory and modelling of information security
- Network security
- Operating system security
- Human factors in security
- Security engineering and assurance
- Cryptography and cryptanalysis
- Database security
- Security management
- Anonymity and privacy

Pedagogiske metoder:
Annet

Pedagogiske metoder (fritekst):

- Lectures
- Seminar discussions

Vurderingsformer:
Annet

Vurderingsformer:
Students must provide two papers. One is a term paper on a topic chosen by the student in coordination with the lecturer (see below), the other is a final report which at least two other areas beyond those covered by the student in the term paper must be described concisely.

- Term paper: 67%
- Final report: 33%.
- Both parts must be passed.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by external and internal examiner.

Utsatt eksamen (tidl. kontinuasjon):
The whole subject must be repeated.

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Dictionaries.

Obligatoriske arbeidskrav:
Students are required to prepare a term paper on one of the subject areas covered in the course in coordination with and approved by the lecturer and must provide a presentation of results and findings in a seminar. The delivery date for the term paper is arranged individually to match the seminar schedule.

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Stephen D. Wolthusen

Læremidler:
Textbooks, monographs, and research articles including but not limited to:

- M. Bishop: Computer Security: Art and Science.Addison-Wesley, 2003.
- M. A. Harrison, W. L. Ruzzo, J. D. Ullman: Protection in Operating Systems. Communications of the ACM 19(8):461-471 (1976)
- C. E. Landwehr: Formal Models for Computer Security. ACM Computing Surveys 13(3):247-278 (1981)
- D. Dolev and A. C. Yao: On the security of public key protocols. IEEE Transactions on Information Theory, IT-29(2):198–208, 1983
- J. Goubault-Larrecq: Towards Producing Formally Checkable Security Proofs, Automatically Proceedings of the 21st IEEE Computer Security Foundations Symposium (CSFW 2008), IEEE, Pittsburgh, PA, USA, June 2008, pp. 224-238.
- L. F. Cranor and S. Garfinkel: Security and Usability: Designing Secure Systems that People Can Use O'Reilly, 2005
- J. C. Brustoloni and R.Villamarin-Salomon: Improving Security Decisions with Polymorphic and Audited Dialogs. Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS'2007), ACM, Pittsburgh, PA, USA, July 2007, pp. 76-87.
- W. Diffie and M. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory 22(6):644-654 (1976)
- R. L. Rivest, A. Shamir,, and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21(2):120-126 (1978)
- E. Bertino and R. Sandhu: Database Security - Concepts, Approaches, and Challenges. IEEE Transactions on Dependable and Secure Computing 2(1):2-19 (2005)
- J. Vaidya and C. Clifton: Privacy-Preserving Decision Trees over Vertically Partitioned Data. ACM Transactions on Knowledge Discovery from Data 2(3):14 (2008)
- K. Thompson: Reflections on Trusting Trust Communications of the ACM 27(8):761-763 (1984)
- J. Feigenbaum, A. Johnson, and P. Syverson: A Model of Onion Routing with Provable Anonymity" Proceedings of the 11th International Conference Financial Cryptography and Data Security (FC 2007), Vol. 4886 of Lecture Notes in Computer Science. Trinidad/Tobago, Feb. 2007, Springer-Verlag.
- E. Peeters, F.-X. Standaert, and J.-J. Quisquater: Power and Electromagnetic Analysis: Improved Model, Consequences, and Comparisons Integration: The VLSI Journal 40(1):52-60 (2007)
- D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi: The EM Side-Channel(s) Proceedings of Cryptographic Hardware and Embedded Systems (CHES 2002), Vol. 2523 of Lecture Notes in Computer Science, Lausanne, Switzerland, Sep. 2002, Springer-Verlag.

Supplerende opplysninger:
The course will be limited to 12 students except by arrangement with the lecturer.

Klar for publisering:
Ja

IMT6001 Ethics and Legal Aspects of Scientific Research - 2011-2012

Emnekode:
IMT6001

Emnenavn:
Ethics and Legal Aspects of Scientific Research

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst
Vår

Språk:
Engelsk

Forventet læringsutbytte:
See English version

Emnets temaer:
See English version

Pedagogiske metoder:
Annet

Pedagogiske metoder (fritekst):
See English version

Vurderingsformer:
Annet

Vurderingsformer:
See English version

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
See English version

Utsatt eksamen (tidl. kontinuasjon):
See English version

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
See English version

Obligatoriske arbeidskrav:
See English version

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Stephen D. Wolthusen

Læremidler:
See English version

Klar for publisering:
Ja

IMT6041 Selected Topics in Cryptology - 2011-2012

Emnekode:
IMT6041

Emnenavn:
Selected Topics in Cryptology

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst

Varighet (fritekst):
Second half of the autumn semester

Språk:
Engelsk

Anbefalt forkunnskap:

- IMT4532 Cryptology 1, IMT4552 Cryptology 2, or equivalent

Forventet læringsutbytte:
Knowledge

The candidate possesses knowledge at the most advanced frontier in the field of cryptology. The candidate has mastered academic theory and scientific methods in cryptology.

The candidate is capable of considering suitability and use of different methods and processes in research in the field of cryptology.

The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in cryptology.

Skills

The candidate is capable of formulating problems, planning and completing research projects in cryptology.

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 cryptology.

General competence

The candidate is capable of identifying relevant – and possibly new - ethical problems and exercising research in cryptology 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 cryptology through approved national and international publication channels.

The candidate is capable of taking part in debates in international forums within the field of cryptology.

The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of cryptology.

Emnets temaer:
1. Introduction – elements of information theory, symmetric and asymmetric cipher theory

2. Elements of modern symmetric cipher theory

3. Modern public key systems

Pedagogiske metoder:
Forelesninger
Oppgaveløsning
Prosjektarbeid

Pedagogiske metoder (fritekst):
Lectures

Numerical exercises

Project work

Vurderingsformer:
Skriftlig eksamen, 3 timer
Vurdering av prosjekt(er)

Vurderingsformer:
Written exam, 3 hours (alternatively oral exam) (counts 51% of the final mark)

Project evaluation (counts 49% of the final mark)

Both parts must be passed.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by the lecturer

Utsatt eksamen (tidl. kontinuasjon):
The whole subject must be repeated

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Calculator

Dictionary

Obligatoriske arbeidskrav:
None.

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Slobodan Petrovic

Læremidler:
Books:

1. Introduction to Cryptography and Coding Theory, 2. edition, Trappe W., Washington L., Prentice Hall, 2006, ISBN: 0131981994.

2. Handbook of Applied Cryptography, Menezes A., http://www.cacr.math.uwaterloo.ca/hac

Various papers (available on-line)

Supplerende opplysninger:
There is room for 50 students for the course.

Klar for publisering:
Ja

Emneside (URL):
http://www.hig.no/imt/emnesider/imt4552

IMT6031 Intrusion Detection and Prevention - 2011-2012

Emnekode:
IMT6031

Emnenavn:
Intrusion Detection and Prevention

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst

Varighet (fritekst):
First half of the autumn semester

Språk:
Engelsk

Anbefalt forkunnskap:
IMT4741 Intrusion Detection and Prevention, or equivalent

Forventet læringsutbytte:
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.

Emnets temaer:

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

Pedagogiske metoder:
Forelesninger
Lab.øvelser
Oppgaveløsning
Prosjektarbeid

Pedagogiske metoder (fritekst):
Lectures

Laboratory exercises

Numerical exercises

Project work

Vurderingsformer:
Skriftlig eksamen, 3 timer
Vurdering av prosjekt(er)

Vurderingsformer:
Written exam, 3 hours (alternatively oral exam) (counts 51% of the final mark)

Project evaluation (counts 49% of the final mark)

Both parts must be passed.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by the lecturer

Utsatt eksamen (tidl. kontinuasjon):
The whole subject must be repeated

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Calculator, dictionary

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Slobodan Petrovic

Læremidler:
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)

Supplerende opplysninger:
There is room for 50 students for the course.

Klar for publisering:
Ja

Emneside (URL):
http://www.hig.no/imt/emnesider/imt4741

IMT6021 Foundations of Information Security - 2011-2012

Emnekode:
IMT6021

Emnenavn:
Foundations of Information Security

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst

Språk:
Engelsk

Forventet læringsutbytte:
Having completed the course, the student should have

- the ability to derive and apply modelling techniques used for secure computer systems and reasoning about them
- in-depth knowledge of selected access control mechanisms and their mathematical foundations as well as an in-depth understanding of identification and authentication mechanisms
- obtained a solid understanding of security analysis and developmental assurance techniques and issues

Emnets temaer:

- Identification and authentication mechanisms including biometrics
- Access control models and formalisms
- Decidability results and limitations of access control and security models
- Security models including the Bell-LaPadula, RBAC, and Chinese Wall models
- Information-theoretic models of information flow and covert channels
- Developmental assurance and evaluation criteria

Pedagogiske metoder:
Annet

Pedagogiske metoder (fritekst):

- Lectures
- Term paper

Vurderingsformer:
Annet

Vurderingsformer:
Term paper. Ph.D. students must pass the written examination with at least an A or B grade, but will be evaluated mainly on the term paper, which is assessed to different, more stringent criteria than the M.Sc. version.

- Written exam (alternatively oral exam): 33%
- Term paper: 67%
- Ph.D. students must pass both parts and pass with A or B on the written exam.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by external and internal examiner.

Utsatt eksamen (tidl. kontinuasjon):
A new term paper must be provided and the examination must be re-sat next autumn.

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Dictionary, simple calculator

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Stephen Wolthusen

Læremidler:
The following textbooks are the primary references; further recommended reading is provided in the course syllabus.

- M. Bishop: Computer Security: Art and Science. Addison-Wesley, 2003.
- D. Gollmann: Computer Security, 2nd edition Wiley, 2006

Supplerende opplysninger:
Capacity of the course is limited to 50 students unless explicitly arranged by lecturer.

Klar for publisering:
Ja

IMT6051 Wireless Communication Security - 2011-2012

Emnekode:
IMT6051

Emnenavn:
Wireless Communication Security

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst

Varighet (fritekst):
Second part of the autumn semester

Språk:
Engelsk

Anbefalt forkunnskap:
IMT4751 Wireless Communication Security, or equivalent

Forventet læringsutbytte:
Knowledge

The candidate possesses knowledge at the most advanced frontier in the field of wireless communication security. The candidate has mastered academic theory and scientific methods in wireless communication security.

The candidate is capable of considering suitability and use of different methods and processes in research in the field of wireless communication security.

The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in the field of wireless communication security.

Skills

The candidate is capable of formulating problems, planning and completing research projects in the field of wireless communication security.

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 wireless communication security.

General competence

The candidate is capable of identifying relevant – and possibly new - ethical problems and exercising research in the field of wireless communication security 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 wireless communication security through approved national and international publication channels.

The candidate is capable of taking part in debates in international forums within the field of wireless communication security.

The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of wireless communication security.

Emnets temaer:

1. Introduction – elements of radio frequency theory, elements of information security with applications in the wireless environment
2. Elements of RFID systems security analysis with case studies: the electronic passport
3. Elements of WLAN security analysis
4. Bluetooth system security
5. Security in mobile telephony systems with case studies: the 2G, the 3G and beyond.

Pedagogiske metoder:
Forelesninger
Prosjektarbeid

Pedagogiske metoder (fritekst):
Lectures

Project work

Vurderingsformer:
Skriftlig eksamen, 3 timer
Vurdering av prosjekt(er)

Vurderingsformer:
Written exam, 3 hours (alternatively oral exam) (counts 51% of the final mark)

Project evaluation (counts 49% of the final mark)

Both parts must be passed.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by the lecturer

Utsatt eksamen (tidl. kontinuasjon):
The whole subject must be repeated

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Calculator, dictionary

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Slobodan Petrovic

Læremidler:
Books:

1. Gunter Schafer, Security in Fixed and Wireless Networks: An Introduction to Securing Data Communications, John Wiley & Son Inc. 2003

2. V. Niemi, K. Nyberg, UMTS Security, John Wiley & Sons, 2005

Various papers (available on-line)

Supplerende opplysninger:
There is room for 50 students for the course

Klar for publisering:
Ja

Emneside (URL):
http://www.hig.no/imt/emnesider/imt4751

IMT6061 Risk Management II - 2011-2012

Emnekode:
IMT6061

Emnenavn:
Risk Management II

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst

Språk:
Engelsk

Forventet læringsutbytte:
The course contributes towards the following learning outcomes:

- Is able to consider suitability and use of different methods and processes in research and in academic and/or artistic development projects
- Is able to handle complex academic issues and to challenge established knowledge and practise in the subject area.

Having completed the course, the students should have:

- advanced level of understanding of assumptions and models on which risk analysis methods are based
- deep understanding of how different assumptions/models influence outcomes of different risk analysis methods
- understand the key elements of Risk Analysis methods such as to be able to make assessments with respect to the suitability of particular risk analysis methods for a given application.

Emnets temaer:

- Classifications of Risk Management methods
- Examples of Risk Management Methods.
- Decission theory
- Risk, Threat and vulnerability discovery
- Uncertainty
- Game theory

Pedagogiske metoder:
Forelesninger
Oppgaveløsning

Vurderingsformer:
Muntlig, individuelt
Vurdering av prosjekt(er)

Vurderingsformer:

- Project(s)
- Oral exam (individual)
- Both parts must be passed

The students are free to choose if they want to complete the project individually or in groups. Every group must have no more than 3 members, and all members of the group must be registered on the same course code. To ensure fairness, course deliverable grading will depend on deliverable quantity, quality and the number of contributing students.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by external and internal examiner.

Utsatt eksamen (tidl. kontinuasjon):
The whole course must be repeated.

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Approved calculator

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Einar Snekkenes

Læremidler:
Books, articles and WEB resources such as

RA method classification

Douglas J. Landoll. The security risk assessment handbook, p. 8-15. CRC. 2005.

Bornman, G, and Labuschagne, L, 2004, A comparative framework for evaluating information security risk management methods, In proceedings of the Information Security South Africa Conference. 2004, www.infosecsa.co.za

Vorster, A. and Labuschagne, L. 2005. A framework for comparing different information security risk analysis methodologies. In Proceedings of the 2005 Annual Research Conference of the South African institute of Computer Scientists and information Technologists on IT Research in Developing Countries (White River, South Africa, September 20 - 22, 2005). ACM International Conference Proceeding Series, vol. 150. South African Institute for Computer Scientists and Information Technologists, 95-103.

ENISA. Inventory of risk assessment and risk management methods. Deliverable 1, Final version Version 1.0, 0/03/2006

Campbell and Stamp. A classification scheme for Risk Assessment Methods. Sandia Report. SAND2004-4233.

RA method examples

IDART (http://www.idart.sandia.gov/method.html)

NIST SP 800-42, p3.1 - 3.21, 4.1- 4.3, C.1-C.9

NIST SP 800-30. p8-27

OECD, “OECD Guidelines for the Security of Information Systems and Networks -- Towards a Culture of Security.” Paris: OECD. July 2002. www.oecd.org. P 10-12

ISO/IEC 27005:2008(E) Information technology - Security techniqueues - Information security risk management

Decision theory

Sven Ove Hansson. Decision Theory - A brief introduction. 2005

http://en.wikipedia.org/wiki/Newcomb%27s_paradox

http://en.wikipedia.org/wiki/St_Petersburg_Paradox

Sven Ove Hansson. Fallacies of Risk

Risk Threat and Vulnerability discovery

ISO 27005, Annex C,D

Ed Yourdon. Just enough Structured Analysis. Chapter 9, Dataflow diagrams. + 'How to'.

The vulnerability assessment and mitigation methodology. Chapter 1-4, p. 1-36. MITRE technical report..

Uncertainty

Lindley, Dennis V. (2006-09-11). Understanding Uncertainty. Wiley-Interscience. ISBN 978-0470043837

H. Campbell. Risk assessment: subjective or objective? Engineering science and education journal, 7:57 -63, 1998.

F. Redmill. Risk analysis-a subjective process? Engineering Management Journal. Apr 2002. Volume: 12, Issue: 2. p. 91-96

Game theory

Stanford Encyclopedia of Philosophy . Game theory. Available from http://plato.stanford.edu/entries/game-theory/

Fudenberg, Drew & Tirole, Jean (1991), Game theory, MIT Press, ISBN 978-0-262-06141-4 , Chapters 1,3,6,8

Supplerende opplysninger:
There is room for 50 students for the course.

Klar for publisering:
Ja

IMT6081 Modern Cryptology - 2011-2012

Emnekode:
IMT6081

Emnenavn:
Modern Cryptology

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst

Varighet (fritekst):
First half of the autumn semester

Språk:
Engelsk

Anbefalt forkunnskap:
IMT4532 Cryptology 1, IMT4552 Cryptology 2, or equivalent

Forventet læringsutbytte:
Knowledge

The candidate possesses knowledge at the most advanced frontier in the field of cryptology. The candidate has mastered academic theory and scientific methods in cryptology.

The candidate is capable of considering suitability and use of different methods and processes in research in the field of cryptology.

The candidate is capable of contributing to development of new knowledge, theories, methods, interpretations and forms of documentation in cryptology.

Skills

The candidate is capable of formulating problems, planning and completing research projects in cryptology.

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 cryptology.

General competence

The candidate is capable of identifying relevant – and possibly new - ethical problems and exercising research in cryptology 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 cryptology through approved national and international publication channels.

The candidate is capable of taking part in debates in international forums within the field of cryptology.

The candidate is capable of considering the need for, taking initiative to and engaging in innovation in the field of cryptology.

Emnets temaer:

- Introduction – elements of information theory, general cipher system theory
- Contemporary theory of randomness – randomness and indistinguishability
- Elements of modern symmetric ciphers theory – Galois fields, primitive polynomials, Boolean functions theory, block ciphers theory, hash functions theory
- Public key cryptography – RSA theory, digital signatures

Pedagogiske metoder:
Forelesninger
Oppgaveløsning
Prosjektarbeid

Pedagogiske metoder (fritekst):
Lectures

Numerical exercises

Project work

Vurderingsformer:
Skriftlig eksamen, 3 timer
Vurdering av prosjekt(er)

Vurderingsformer:
Written exam, 3 hours (alternatively oral exam) (counts 51% of the final mark)

Project evaluation (counts 49% of the final mark)

Both parts must be passed.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by the lecturer

Utsatt eksamen (tidl. kontinuasjon):
The whole subject must be repeated.

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Calculator, dictionary

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Slobodan Petrovic

Læremidler:
Books:
1. Introduction to Cryptography and Coding Theory, 2. edition, Trappe W., Washington L., Prentice Hall, 2006, ISBN: 0131981994.
2. Handbook of Applied Cryptography, Menezes A., http://www.cacr.math.uwaterloo.ca/hac

3. Introduction to modern cryptography, Katz J., Lindell Y., Chapman&Hall/CRC, 2008, ISBN: 1-58488-551-3

Various papers (available on-line)

Supplerende opplysninger:
There is room for 50 students for the course.

Klar for publisering:
Ja

Emneside (URL):
http://www.hig.no/imt/emnesider/imt4532

IMT6091 Computational Forensics - 2011-2012

Emnekode:
IMT6091

Emnenavn:
Computational Forensics

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst
Vår

Språk:
Engelsk

Forventet læringsutbytte:
The course offers students a deeper understanding of cutting-edge problems in computational and forensic sciences as well as their applications. Students will strengthen their ability to work with the original scientific literature.On completion of this course the students will be able to:- Collect, analyze and discuss previously published research results in the field- Identify, plan, prepare and conduct independent research in computational forensics- Formulate specific requirements for a given problem and propose an appropriate solution- Predict and judge the performance of proposed method.

Emnets temaer:

- Forensic Imaging
- Signal and Video Processing
- Computer Visualization
- Forensic Statistics
- Information Retrieval
- Data Mining
- Pattern Recognition and Machine Learning
- Applications: Digital and Media Forensics, Crime Scene Investigation, Psychological and Behavioral Analysis, Questioned Document Examination, Forensic Linguistic, Speaker Identification, Tool Mark, Trace or Blood-strain Pattern Investigation.

Pedagogiske metoder:
Forelesninger
Prosjektarbeid

Pedagogiske metoder (fritekst):
Face-to-face Meetings

Vurderingsformer:
Vurdering av prosjekt(er)

Vurderingsformer:
1 Project

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by the lecturer(s)

Utsatt eksamen (tidl. kontinuasjon):
The whole subject must be repeated.

Tillatte hjelpemidler:

Obligatoriske arbeidskrav:
None

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Dr. Katrin Franke, Associate Professor

Læremidler:
Scientific Articles related to the field of Specialization.

Supplerende opplysninger:
In case there will be less than 5 students that will apply for the course, it will be at the discretion of Studieprogramansvarlig whether the course will be offered or not an if yes, in which form.

Klar for publisering:
Ja

IMT6111 Risk Management I - 2011-2012

Emnekode:
IMT6111

Emnenavn:
Risk Management I

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst

Varighet (fritekst):
First part of the semester

Språk:
Engelsk

Forventet læringsutbytte:
When the course is completed, the student should have

- Advanced level of understanding of challenges facing the IS Risk Analyst
- Deep understanding of one method for Risk Management
- Deep understanding of how to plan and organize a Risk Management project.
- Understand the limitations of the Risk Management methods covered by the course from a pragmatical perspective such as to be able to formulate suitable research questions to adress the limitations identified.

Emnets temaer:

- Risk Management in the context of an Information Security Management system
- Study of a method for risk management

Pedagogiske metoder:
Forelesninger
Gruppearbeid
Nettstøttet læring
Prosjektarbeid
Samling(er)/seminar(er)
Veiledning

Pedagogiske metoder (fritekst):
The course will include an introductory lecture providing an overview of the course content. The primary teaching method for the course is project work. The students are required to carry out and document a Risk Management activity by means of a case study.

Students are expected to present their work-in-progress at the seminars for discussions. Guidance, supervision and feedback will be provided during seminars only and given on material presented at the seminars only..

Students that cannot be present during the seminars are expected to be present by means of the Fronter Teleconference tool.

Vurderingsformer:
Muntlig, individuelt
Vurdering av prosjekt(er)

Vurderingsformer:

- Project(s)
- Oral exam (individual)
- Both parts must be passed

The students are free to choose if they want to complete the project individually or in groups. Every group must have no more than 3 members, and all members of the group must be registered on the same course code. To ensure fairness, course deliverable grading will depend on deliverable quantity, quality and the number of contributing students.

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by external and internal examiner.

Utsatt eksamen (tidl. kontinuasjon):
Not allowed.

Tillatte hjelpemidler:

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Tone Hoddø Bakås

Læremidler:
The course litterature will be the documents listed below or similar.

All litterature listed below are available from ISACA (www.isaca.org).

ISACA. The Risk IT Framework. 2009. ISBN 978-1-60420-111-6

ISACA. THE RISK IT PRACTITIONER GUIDE. 2009. ISBN 978-1-60420-116-1

Additional recommended reading

IT Governance Institute. COBIT 4.1. 2007.. ISBN 1-933284-72-2

Klar for publisering:
Ja

IMT6121 Authentication - 2011-2012

Emnekode:
IMT6121

Emnenavn:
Authentication

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Høst
Vår

Språk:
Engelsk

Forventet læringsutbytte:
See English version

Emnets temaer:
See English version

Pedagogiske metoder:
Forelesninger
Prosjektarbeid
Veiledning

Pedagogiske metoder (fritekst):
See English version

Vurderingsformer:
Mappevurdering (utfyllende opplysning i tekstfelt)

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
See English version

Utsatt eksamen (tidl. kontinuasjon):
See English version

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
See English version

Obligatoriske arbeidskrav:
See English version

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Ass.Prof. Patrick Bours

Læremidler:
See English version

Supplerende opplysninger:
See English version

Klar for publisering:
Ja

IMT6071 Biometrics - 2011-2012

Emnekode:
IMT6071

Emnenavn:
Biometrics

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Annet

Språk:
Engelsk

Anbefalt forkunnskap:
The course content will be complementary to the course "Authentication".

Forventet læringsutbytte:
After the course, the students should have the capabilities to

- demonstrate a systematic understanding of biometric systems and react on disadvantages with appropriate technical and organizational measurers

- apply the skills of modality specific feature extraction techniques

- apply statistical tools for biometric and conduct performance evaluation

- apply multimodal analysis and solve the score normalization challenge in fusion systems

- analyze threats for biometric reference data, categorize them and implement protection techniques accordingly

- assess the appropriate position of a biometric component in a security system

Furthermore the students should have the competence to

- demonstrate the ability to design a biometric system suitable for a give scenario

- judge the relevance of ethical and privacy issues

- investigate for a given scenario technical solutions and evaluate them in a critical analysis. Synthesize new ideas during evaluation phase.

- can communicate with peers in the biometric community in terms of reviewing research topics

- manage team work

Emnets temaer:

- Fingerprint recognition
- Vein recognition
- Face recognition specifically focused on three dimensional data
- Iris recognition
- Multimodal biometrics
- Score Normalization
- Attack mechanisms
- Privacy Enhancing Technologies
- Revocable biometric references

Pedagogiske metoder:
Forelesninger
Oppgaveløsning

Vurderingsformer:
Skriftlig eksamen, 3 timer

Vurderingsformer:
Written examination in English

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
Evaluated by the lecturer.

Utsatt eksamen (tidl. kontinuasjon):
The whole course must be repeated.

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
Dictionaries allowed

Obligatoriske arbeidskrav:
Students must provide a research report (term paper) on a topic that is chosen by the student in coordination with the lecturer

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Professor Christoph Busch

Læremidler:
[1] LI , S . Z. , AND JAIN, A. K. , Eds. Handbook of Face Recognition. Springer-Verlag,

Heidelberg, Germany, 2005.

[2] MALTONI , D. , MAIO, D. , JAIN, A. K. , AND PRABHAKAR , S . Handbook of Fingerprint Recognition. Springer-Verlag, Heidelberg, Germany, 2005.

[3] WAYMAN, J . , JAIN, A. , MALTONI , D. , AND MAI O, D. , Biometric Systems.

Springer-Verlag, Heidelberg, Germany, 2004.

[4] JAIN, L.C. , HALICI, U. , HAYASHI, I. ; LEE, S.B., TSUTSUI, S. Intelligent Biometric Techniques in Fingerprint and Face Recognition. CRC PressVerlag, 1999.

[5] TUYLS, P., SKROIC, B., KEVENAAR, T. Security with Noisy Data. Springer-Verlag, 2007

Klar for publisering:
Ja

IMT6101 Computational Intelligence - 2011-2012

Emnekode:
IMT6101

Emnenavn:
Computational Intelligence

Faglig nivå:
PhD (syklus 3)

Studiepoeng:
5

Varighet:
Annet

Språk:
Engelsk

Forutsetter bestått:
IMT4612 Machine Learning and Pattern Recognition I

IMT4632 Machine Learning and Pattern Recognition II,

eller tilsvarende

Forventet læringsutbytte:
See English version

Emnets temaer:
See English version

Pedagogiske metoder:
Annet

Pedagogiske metoder (fritekst):
See English version

Vurderingsformer:
Annet

Vurderingsformer:
See English version

Karakterskala:
Bestått/Ikke bestått

Sensorordning:
See English version

Utsatt eksamen (tidl. kontinuasjon):
See English version

Tillatte hjelpemidler:

Tillatte hjelpemidler (gjelder kun skriftlig eksamen):
See English version

Obligatoriske arbeidskrav:
See English version

Ansvarlig avdeling:
Avdeling for informatikk og medieteknikk

Emneansvarlig:
Dr. Katrin Franke, Associate Professor

Læremidler:
See English version

Klar for publisering:
Ja