Studieplan 2010/2011

Master of Science in Information Security

Studyprogramcode
MIS
Short description
Information technology permeates all aspects of society and has become critical to industry, government, and individual well-being. Securing these vital services and structures and the availability of trustworthy information whenever and wherever it is required has become both an area of intensive research and also of burgeoning commercial activity. A master of science in information security will provide the students with the knowledge and theoretical background as well as with the requisite skills and attitudes to succeed in this challenging yet eminently rewarding field.

Go to course table

Duration
This is a two-year master program (120 ECTS credits) which is also available part-time over three or four years. The degree awarded upon completion is “Master of Science in Information Security”.

The program has three tracks: management, technology and digital forensics. Students have to choose which track they pursue when entering the program (see the course structure below).

The program qualifies students to proceed to Ph.D. studies.

Expected learning outcomes
Upon completion of the programme, the students will have a solid understanding of the interdisciplinary field of information security. The graduated students will be proficient in core topics such as security management, computer and network security, incident responds and forensics, and will be able to understand the critical information infrastructures and the security aspects of important IT services which society depends on. The students will also have gained a particular in-depth understanding of either technology, forensics or management issues dependent on their chosen programme track.

The students will be capable of discussing main questions and issues in scientific thinking and will be able to frame research problems and questions. They will have experience in planning and conducting a scientific project and in documenting the results and scientific contributions in the form of a scientific report (through their master thesis).

Target Group
There are three focus groups for this study programme:

1. Undergraduate students entering the programme as a continuation of their bachelor degree without any prior work experience.

2. Industry students (or students in private/public sector in general) looking for a full-time or part-time masters programme which is flexible and can be adapted to their employers needs and their own

individual needs.

3. International students: full-time, part-time or exchange students arriving for only single semesters.

Admission Criteria
Applicants must have a bachelor degree in computer science or a related subject to qualify for admission. The applicants must document that they have at least 10 ECTS credits in mathematics/statistics and at least 60 ECTS credits in computer science subjects. A grade point average (GPA) of C is required. It is expected that within these credits the following topics have been covered:

- Structural and object-oriented programming
- Algorithms and data structures
- Databases and XML
- Software engineering
- Computer network (Data communication)
- Operating systems and computer architecture

Students who have not had a dedicated course in each of these topics need to be prepared for some extra studying when entering topics that require background knowledge with which they are not sufficiently familiar beforehand.

Graduate studies in information security require a somewhat different mathematical platform than the one included in most bachelor studies. To master the theoretical topics included in the master programme we therefore recommend that the students attend the preparatory courses in number theory and theoretical computer science offered during the first weeks of the fall semester.

Course Structure
The programme is offered in a flexible manner to fit well to all the three target groups of students. In general, on campus presence is *required* only three times per semester (1-3 days each time), for a start-up session, for mid-term exams/presentations (and a start-up session of second part of the semester) and for final exams/presentations. Attendance is also strongly recommended for the *initial first two weeks of the programme when two preparatory intense short-courses in number theory and theoretical computer science are offered* . All courses are available online, but there will also be sessions on a regular weekly or bi-weekly schedule. The presence on these sessions is not required.

More details for the upcoming year of study will be given here:

The program has three tracks (paths of study): management, technology and digital forensics. Students have to choose which track they pursue when entering the programme. Common to all three tracks are a set of courses covering the core topics in both information security technology, forensics and management: introduction to cryptology, applied information security, network security, IT governance, information society and security, and legal aspects of information security. In addition, each track has a set of specific courses and the students have to choose at least 15 credits of courses from the track-specific pool of electives. Students also have to choose their master thesis topic within their chosen track.

Ordinary mandatory courses from the other track of the programme and courses from the masters programme in media technology and the CIMET (Color in Informatics and Media Technology) master can be included as electives. Students can also use *up to 20 ECTS of courses at the 3000 level* as part of their master programme, and are particularly encouraged to browse the course offerings of the bachelor

programmes in network and system administration, software engineering, and economics and management. Some of the courses listed above can also be mobile in time, space and teaching format upon request by students (typically a course can be taken in a different semester through self-study and individual or group supervision).

Master-level courses from other institutions can be included as electives or can substitute for mandatory courses at the discretion of the programme director.

The course structure for part-time students can be composed individually as long the track-specific requirements mentioned above and any course interdependencies are respected. The most important course interdependencies are the following: 1. Students should enter their master thesis in the semester following the research project planning course, 2. All previous course work has to be completed before entering the master thesis (an exception of 10 credits missing can be made at the discretion of the master thesis instructor, but only if the missing credits are not relevant for the topic of the master thesis).

Students entering the programme from the bachelors programme in information security will be offered greater flexibility in the course structure due to potential overlap with some of the contents in the bachelors programme.

Study methods

Lectures
Exercises
Project work
Essay/Article writing
Independent study
Group exercises
Lab exercises

Technical Prerequisites
Students, who choose to participate in the study program on distance, need a relatively new computer and a broadband Internet connection. Software that is needed is mostly freely available on the Internet. In some courses commercial products, such as MatLab, are required.

For practical computer skills, it is expected that students can use any common operating system (GNU/Linux, Microsoft Windows, MacOS or Solaris) both with a graphical user interface and a command line interface.

Students who have not had a dedicated course on each of these topics should not worry, they just need to be prepared for a little bit of extra studying when entering topics that require background knowledge with which they are not sufficiently familiar beforehand.

Graduate studies in information security requires a somewhat different mathematical platform than the one included in most bachelor studies. To master the theoretical topics included in the master programme we therefore recommend that you attend the preparatory courses in number theory and theoretical computer science offered during the first two weeks of the fall semester.

Internal/external examiner
Most courses have internal examiner. The master thesis always has an external examiner.

Internationalization
Students can travel abroad to do their master thesis. The information security group has strong links to many of the leading international academic groups within the field, and students are encouraged to contact their instructor in the course «research project planning» to ask for relevant travel opportunities.

Publiser
Yes
Degree
Mastergrad

Master of Science in Information Security 2010-2012 Technology full-time track

Coursecode	Course name	C/E *)	ECTS each. semester			
			S1(A)	S2(S)	S3(A)	S4(S)
IMT4421	**Scientific Methodology**	C	5			
IMT4541	**Foundations of Information Security**	C	5			
IMT4532	**Cryptology 1**	C	5			
IMT4552	**Cryptology 2**	C	5			
IMT4571	**IT Governance**	C	5			
IMT4561	**Applied Information Security**	C	5			
IMT4591	**Legal Aspects of Information Security**	C		5		
IMT4581	**Network Security**	C		10		
IMT4481	**Information Society and Security**	C		5		
	Elective course, 5 ECTS	E		5		
	Elective course, 5 ECTS	E		5		
IMT4601	**Research Project Planning**	C			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
IMT4901	**Master's Thesis**	C				30
		Sum:	30	30	30	30

*) C - Compulsory course, E - Elective course

Master of Science in Information Security 2010-2012 Digital Forensics full-time track

Coursecode	Course name	C/E *)	ECTS each. semester			
			S1(A)	S2(S)	S3(A)	S4(S)
IMT4421	Scientific Methodology	C	5			
IMT4012	Digital Forensics I	C	5			
IMT4532	Cryptology 1	C	5			
IMT4571	IT Governance	C	5			
IMT4561	Applied Information Security	C	5			
IMT4022	Digital Forensics II	C		10		
IMT4581	Network Security	C		10		
IMT4641	Computational Forensics	C		5		
IMT4612	Machine Learning and Pattern Recognition I	C		5		
IMT4591	Legal Aspects of Information Security	C		5		
IMT4601	Research Project Planning	C			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
IMT4901	Master's Thesis	C				30
		Sum:	25	35	30	30

*) C - Compulsory course, E - Elective course

Master of Science in Information Security 2010-2012 Management full-time track

Coursecode	Course name	C/E *)	ECTS each. semester			
			S1(A)	S2(S)	S3(A)	S4(S)
IMT4651	Security as Continuous Improvement	C	5			
IMT4661	Security Management Dynamics	C	5			
IMT4421	Scientific Methodology	C	5			
IMT4561	Applied Information Security	C	5			
IMT4532	Cryptology 1	C	5			
IMT4571	IT Governance	C	5			
IMT4591	Legal Aspects of Information Security	C		5		
IMT4841	Security Planning and Incident Management	C		10		
IMT4581	Network Security	C		10		
IMT4481	Information Society and Security	C		5		
IMT4601	Research Project Planning	C			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
	Elective course, 5 ECTS	E			5	
IMT4901	Master's Thesis	C				30
		Sum:	30	30	30	30

*) C - Compulsory course, E - Elective course

Master of Science in Information Security 2010-2013 Technology part-time track (three years)

Coursecode	Course name	C/E *)	ECTS each. semester					
			S1(A)	S2(S)	S3(A)	S4(S)	S5(A)	S6(S)
IMT4532	Cryptology 1	C	5					
IMT4552	Cryptology 2	C	5					
IMT4421	Scientific Methodology	C	5					
IMT4571	IT Governance	C	5					
IMT4591	Legal Aspects of Information Security	C		5				
IMT4481	Information Society and Security	C		5				
IMT4581	Network Security	C		10				
IMT4601	Research Project Planning	C			5			
IMT4541	Foundations of Information Security	C			5			
IMT4561	Applied Information Security	C			5			
	Elective course, 5 ECTS	E			5			
	Elective course, 5 ECTS	E				5		
	Elective course, 5 ECTS	E				5		
	Elective course, 5 ECTS	E				5		
	Elective course, 5 ECTS	E				5		
	Elective course, 5 ECTS	E					5	
	Elective course, 5 ECTS	E					5	
IMT4904	Master's Thesis	C					10	20
		Sum:	20	20	20	20	20	20

*) C - Compulsory course, E - Elective course

Master of Science in Information Security 2010-2013 Digital Forensics part-time track (three years)

Coursecode	Course name	C/E *)	ECTS each. semester					
			S1(A)	S2(S)	S3(A)	S4(S)	S5(A)	S6(S)
IMT4012	Digital Forensics I	C	5					
IMT4561	Applied Information Security	C	5					
IMT4532	Cryptology 1	C	5					
IMT4421	Scientific Methodology	C	5					
IMT4581	Network Security	C		10				
IMT4641	Computational Forensics	C		5				
IMT4612	Machine Learning and Pattern Recognition I	C		5				
IMT4571	IT Governance	C			5			
IMT4601	Research Project Planning	C			5			
	Elective course, 5 ECTS	E			5			
	Elective course, 5 ECTS	E			5			
IMT4022	Digital Forensics II	C				10		
IMT4591	Legal Aspects of Information Security	C				5		
	Elective course, 5 ECTS	E				5		
	Elective course, 5 ECTS	E					5	
	Elective course, 5 ECTS	E					5	
IMT4904	Master's Thesis	C					10	20
		Sum:	20	20	20	20	20	20

*) C - Compulsory course, E - Elective course

Master of Science in Information Security 2010-2013 Management part-time track (three years)

Coursecode	Course name	C/E *)	ECTS each. semester					
			S1(A)	S2(S)	S3(A)	S4(S)	S5(A)	S6(S)
IMT4661	Security Management Dynamics	C	5					
IMT4651	Security as Continuous Improvement	C	5					
IMT4571	IT Governance	C	5					
IMT4421	Scientific Methodology	C	5					
IMT4591	Legal Aspects of Information Security	C		5				
IMT4481	Information Society and Security	C		5				
IMT4841	Security Planning and Incident Management	C		10				
IMT4601	Research Project Planning	C			5			
IMT4561	Applied Information Security	C			5			
IMT4532	Cryptology 1	C			5			
	Elective course, 5 ECTS	E			5			
IMT4581	Network Security	C				10		
	Elective course, 5 ECTS	E				5		
	Elective course, 5 ECTS	E				5		
	Elective course, 5 ECTS	E					5	
	Elective course, 5 ECTS	E					5	
IMT4904	Master's Thesis	C					10	20
		Sum:	20	20	20	20	20	20

*) C - Compulsory course, E - Elective course

Electives

Coursecode	Course name	C/E *)	ECTS each. semester	
			S1(A)	S2(S)
IMT3491	Ethical Hacking and Penetration Testing	E	5	
IMT3761	Information Warfare	E	5	
IMT3551	Digital Forensics	E	5	
IMT4882	Specialization Course II	E	10	10
IMT4721	Authentication	E	5	
IMT4632	Machine Learning and Pattern Recognition II	E	5	
IMT4671	Organizational and Human Aspects of Information Security	E	5	
IMT4772	Risk Management II	E	5	
IMT4881	Specialization Course	E	5	5
IMT4741	Intrusion detection and prevention	E	5	
IMT4751	Wireless communication security	E	5	
IMT4762	Risk Management I	E	5	
IMT3511	Discrete Mathematics	E		10
IMT4621	Biometrics	E		5
IMT4612	Machine Learning and Pattern Recognition I	E		5
IMT4641	Computational Forensics	E		5
		Sum:	0	0

*) C - Compulsory course, E - Elective course

NTNU

Emneoversikt

IMT4651 Security as Continuous Improvement - 2010-2011

Course code:
IMT4651

Course name:
Security as Continuous Improvement

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
Second part of autumn semester

Language of instruction:
English

Prerequisite(s):
IMT4661 - Security Management Dynamics

Expected learning outcomes:
Already the BS7799/ISO17799 standards encouraged viewing security as quality improvement. Some years later and after the extensions to the ISO27000 family, security as a continuous improvement process is not yet a mainstream activity.

The emphasis of this course is on identifying the systemic obstacles in the implementation path of continuous improvement of processes (“the quality improvement paradox”). Then, to apply this insights to redesign security management to achieve continuous improvement.

Topic(s):
The quality improvement paradox

Security and quality improvement processes

Improving the Performance of Computer Security Incident Response Teams (CSIRTs)

Incident reporting systems and Learning from incidents

Security risks in the transition to Integrated Operations

Security-dependent safety. Continuous improvement of security in Critical Infrastructure

Teaching Methods:
Lectures
Exercises
Project work

Teaching Methods (additional text):
Web-enabled course with forum

Form(s) of Assessment:
Multiple Choice Test(s)
Evaluation of Project(s)

Form(s) of Assessment (additional text):

- Two multiple choice exams counting each 15%
- Two individual projects (papers) counting each 35%
- Each part must be individually approved of

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
The whole subject must be repeated

Tillatte hjelpemidler:

Coursework Requirements:
The course requires active participation in projects – both in class and outside class.

Hands-on modelling exercises during class are best carried out in computer lab.

Students are encouraged to bring laptops to the classroom.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Jose Gonzalez

Teaching Materials:
Written material will be given/sent to the students during the semester.

Publish:
Yes

IMT4661 Security Management Dynamics - 2010-2011

Course code:
IMT4661

Course name:
Security Management Dynamics

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First half of autumn semester

Language of instruction:
English

Expected learning outcomes:
The emphasis of this course is on the *dynamics* of security management. This is a much neglected aspect that it is becoming increasingly important.

Security is a highly interdisciplinary challenge, involving Man, Technology and Organization – the famous MTO challenge. Some people would add Economics as a new and important aspect.

Addressing the dynamics of security management provides several bonuses:

- Understand why many managers fail to achieve a satisfactory state of security;
- understand why some important security failures occur as unintended side-effects of management actions;
- and others, such as the increasing importance of employing System Dynamics to manage dynamic complexity.

Topic(s):
Foundations – Security standards from the perspective of change and dynamics

Introduction to qualitative system dynamics: Causal loop diagrams; System archetypes

Modelling security management dynamics using system archetypes and causal loop diagrams

Introduction to quantitative system dynamics: Causal structure and dynamic behaviour. Introduction to stocks and flows. Time delays.

Basic system dynamics models of security management.

Teaching Methods:
Lectures
Exercises
Project work

Teaching Methods (additional text):
Web-enabled course with forum

Form(s) of Assessment:
Multiple Choice Test(s)
Evaluation of Project(s)

Form(s) of Assessment (additional text):

- Two multiple choice exams counting each 15%
- Two individual projects (papers) counting each 35%
- Each part must be individually approved of

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
The whole subject must be repeated.

Tillatte hjelpemidler:

Coursework Requirements:
The course requires active participation in projects – both in class and outside class.

Hands-on modelling exercises during class are best carried out in computer lab.

Students are encouraged to bring laptops to the classroom.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Jose Gonzalez

Teaching Materials:
Literature:

Maani, Kambiz E.; Cavana, Robert Y. Systems Thinking And Modelling. Pearson Education. 9781877371035.

Lectures, exercises and projects by Jose J. Gonzalez in Classfronter

Replacement course for:
IMT4111 Sikkerhetsledelse

Publish:
Yes

IMT4421 Scientific Methodology - 2010-2011

Course code:
IMT4421

Course name:
Scientific Methodology

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Language of instruction:
English

Expected learning outcomes:
After completing the course, the student shall be familiar with and shall be capable of discussing main questions and issues in scientific thinking. The student shall be able to frame research problems and questions, to develop a plan for conducting a scientific project and to report the results from scientific projects.

Topic(s):
- Introduction to scientific research and scientific theory
- What characterises good research
- Ethics in research
- Developing a research topic
- Quantitative and qualitative research designs
- State of the art and literature studies
- Designing and analysing studies and experiments

Teaching Methods:
Essay
Lectures
E-learning
Project work
Tutoring

Teaching Methods (additional text):
The course will be offered both as an ordinary campus course and as a course that is offered in a flexible way to off-campus students. Lecture notes, e-lectures and other types of e-learning material will be offered through an LMS. Communication between the teachers and the students, and among the students, will be facilitated by the LMS.

Form(s) of Assessment:
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
External and internal examiner.

Re-sit examination:
Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
English dictionary.

Coursework Requirements:
Essay

Participation in project work

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Førstelektor Frode Volden

Teaching Materials:
Books:

- Leedy, P D, and Ormrod, J E: "Practical Research, -Planning and design, 8th ed."Pearsopn Educational Int. ISBN: 0-13-124720-4

Other:

- Additional handouts and material made available on Fronter.

Publish:
Yes

IMT4561 Applied Information Security - 2010-2011

Course code:
IMT4561

Course name:
Applied Information Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
Second half of autumn semester

Language of instruction:
English

Expected learning outcomes:
Students who have passed this course should:
- have acquired good knowledge of the common terminology in information security
- have working knowledge of security analysis methods
- have a good understanding of selected attack mechanisms and techniques and their employment by malicious software
- have working knowledge of database security
- have good understanding of design principles for secure information systems

Topic(s):
- Core terminology for information security
- Authentication and authentication techniques
- Security analysis methods
- Design principles for secure information systems
- Case studies of secure system design
- Database security
- Attack mechanisms and techniques
- Malicious software

Teaching Methods:
Lectures
Exercises
Project work
Other

Teaching Methods (additional text):
Annet - Tutorials

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
Written examination, 3 hours, (67%) in conjunction with term paper (33%). Pass decision is on the cumulative grade.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer.

Re-sit examination:
A new term paper must be provided next autumn. For the exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Examination support:
Simple calculator

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Stephen Wolthusen

Teaching Materials:
Books:

- M. Bishop: Computer Security: Art and Science. Addison-Wesley, Reading, MA, USA (2002)
- D. Gollmann: Computer Security, 2nd ed. John Wiley & Sons, New York, NY, USA (2006)
- M. Gasser: Building a Secure Computer System. Van Nostrand Reinhold, New York, NY, USA (1988)
- R. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Chichester, UK (2001)
- A. K. Jain, P. J. Flynn, and A. A. Ross: Handbook of Biometrics. Springer-Verlag, Berlin, Germany (2007).

Replacement course for:
IMT4162 Information Security and Security Architecture

Publish:
Yes

IMT4532 Cryptology 1 - 2010-2011

Course code:
IMT4532

Course name:
Cryptology 1

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First part of autumn semester

Language of instruction:
English

Expected learning outcomes:
In the course the students will acquire:

- Advanced level of understanding of methods of analysis and synthesis of cryptographic systems

- Deep understanding of modern cryptographic theory

Topic(s):
1. Classical cryptography

2. Symmetric ciphers

3. Asymmetric ciphers

4. Hash functions and digital signatures.

Teaching Methods:
Lectures
Exercises

Teaching Methods (additional text):
Lectures

Exercises

Form(s) of Assessment:
Written exam, 3 hours

Form(s) of Assessment (additional text):
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
Ordinary re-sit examnination.

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. 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

Replacement course for:
IMT4531 Introduction to Cryptology

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

Publish:
Yes

Home page:
http://www.hig.no/imt/emnesider/imt4532

IMT4571 IT Governance - 2010-2011

Course code:
IMT4571

Course name:
IT Governance

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
Second half of autumn semester

Language of instruction:
English

Expected learning outcomes:
Calder and Watkins define IT Governance as ”the framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organization’s information systems support and enable the achievement of its strategies and objectives”. IT Governance is of crucial importance for organizations owing to the need to best safeguard critical information and, through the increasing requirements from national and international regulations. Central to IT Governance in Europe is the ISO 27001 / ISO 27002 standard.

This course provides an overview of IT Governance and the basic concepts of the ISO 27001 / ISO 27002 standard.

The candidate should after attending the course

- fully understand the main principles of IT Governance.
- fully understand the basic concepts of the ISO 27001 / ISO 27002 standard
- master the principles for designing & implementing an ISO 27001 ISMS
- be fully aware of the difference between security technology and the management of secure systems
- have a thorough understanding of security management as a continuous improvement process.
- possess awareness of security certification schemes (BS7799, ISO 15408, …)

Topic(s):

- Reasons for IT Governance: Compliance, liability, stability
- Organizing information security
- Information security policy and scope
- The risk assessment and statement of applicability
- Identification of risks related to external parties
- Asset management
- Human resources security
- Physical and environmental security
- Equipment security
- Communications and operations management
- Controls against malicious software (malware) and back-ups
- Network security management and media handling
- Exchanges of information
- Electronic commerce services
- E-mail and internet use
- Access control
- Network access control
- Operating system access control
- Application access control and teleworking
- Systems acquisition, development and maintenance
- Cryptographic controls
- Security in development and support processes
- Monitoring and information security incident management
- Business continuity management
- Compliance
- Principles of auditing

Teaching Methods:
Other

Teaching Methods (additional text):
Lectures, exercises and projects.

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):

- 1-2 Multiple Choice Tests (weight: 20%)
- 1-2 Group Assignments (weight: 20%)
- Digital Final Exam, 2 hours (weight: 50%)
- All three parts are mandatory and must be passed!

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
For the final exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Forskningssjef Åsmund Skomedal

Teaching Materials:
Literature:

Alan Calder & Steve Watkins. IT Governance : IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002. Fourth Edition. Kogan Page. 2008.

Anderson, Ross (1999) Why cryptosystems fail, University Computer Laboratory,University of Cambridge, Cambridge, UK, http://www.cl.cam.ac.uk/~rja14/wcf.html.

Publish:
Yes

IMT4591 Legal Aspects of Information Security - 2010-2011

Course code:
IMT4591

Course name:
Legal Aspects of Information Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Language of instruction:
Norsk, alternativt engelsk

Expected learning outcomes:
The students should be able to account for legal aspects especially relevant for information security.

Topic(s):
E-government, information society and information security

Legal aspects according to personal dataprotection

Teaching Methods:
Lectures
Group works
Exercises

Form(s) of Assessment:
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal + external examiner

Re-sit examination:
Ordinary re-sit examnination.

Tillatte hjelpemidler:

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Lise Nilsen

Teaching Materials:
See information in Fronter.

Publish:
Yes

IMT4841 Security Planning and Incident Management - 2010-2011

Course code:
IMT4841

Course name:
Security Planning and Incident Management

Course level:
Master (syklus 2)

ECTS Credits:
10

Duration:
Vår

Language of instruction:
Norsk, alternativt engelsk

Expected learning outcomes:
The student shall after the course be able to create policies and procedures for contingency plans, as well as lead the planning process. This requires that the student must achieve a thorough understanding of why incident reporting systems are needed, how they work and how to plan and conduct investigations. Furthermore, the student should have a good overview over the most well known organizational problems within incident reporting systems. The student should also be able to plan for and handle large and small disasters. To handle disasters the students also need to know business continuity planning.

Topic(s):
1. Introduction and Overview of Contingency Planning
2. Planning for Organizational Readiness: Risk management, limits to risk management, incident reporting systems, business impact analysis
3. Incident Response: Preparation, organization, prevention, detection, notification, reaction, recovery, maintenance, operational problems for CSIRTS and organizational models for CSIRTs
4. Disaster Recovery: Preparation, implementation, operation and maintenance
5. Business Continuity: Preparation, implementation, operations and Maintenance
6. Crisis Management and Human Factors

Teaching Methods:
Lectures
Project work

Form(s) of Assessment:
Written exam, 3 hours
Evaluation of Project(s)

Form(s) of Assessment (additional text):
Assessment: An overall evaluation based on a 100 point scale, where project work counts 50 points and final written exam counts 50 points. A minimum of 18 points have to be gained on the final exam. Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, emneansvarlig can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
External examiner

Re-sit examination:
For the final exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
Dictionary: English-Norwegian or English-other language

Coursework Requirements:
One project (the exam project).

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Finn Olav Sveen

Teaching Materials:
Michael Whitman og Herbert Mattord: Principles of Incident Response and Disaster Recovery. Thomson, 2007.

Additional litterature will be handed out.

Publish:
Yes

IMT4581 Network Security - 2010-2011

Course code:
IMT4581

Course name:
Network Security

Course level:
Master (syklus 2)

ECTS Credits:
10

Duration:
Vår

Language of instruction:
English

Prerequisite(s):
Some knowledge of cryptology course.

Expected learning outcomes:
The student shall gain insight into:
• why network security is important and why it should not be neglected
• which mechanisms are required and available for protection of networked systems
• how these mechanisms are used to solve security challenges in particular systems

The course will provide the student with the foundation required for implementing protection systems and for continuing research in the field.

Topic(s):
Part I Introduction :
• Network infrastructure and security threats

Part II Protection methods :
• Encryption, device authentication, message authentication and protection of integrity.
• Key management: symmetric keys, public key infrastructure, certificates, revocation, and key escrows.
• Distributed access control
• Anatomy of attacks, firewalls, and protection against attacks

Part III Applications of security mechanisms
• Internet security (PGP, IPsec, NLS)
• Mobile security (GSM/UMTS architectures and security objectives, security functions of USIM, management of anonymity in mobile networks, use of USIM security to protect other systems)
• Non-repudiation (principles, collection of evidence, example of protocols)
• Payment systems (CyberCash, NetBill, Ecash)

Teaching Methods:
Essay
Lectures

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation is based on a 100 point scale, where the essay counts 50 points and the final exam (3 hours) counts 50 points. Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, emneansvarlig can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
For the final exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
None

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor II Jan Audestad

Teaching Materials:
Available via Fronter.

Replacement course for:
IMT4101

Publish:
Yes

IMT4481 Information Society and Security - 2010-2011

Course code:
IMT4481

Course name:
Information Society and Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Duration (additional text):
First half of spring semester

Language of instruction:
English

Expected learning outcomes:
The students shall primarily understand the evolution that has taken place within ICT during the last ten years that has led us toward a vulnerable society, and what vulnerability means in such a broad context. The students shall get sufficient insight to identify, evaluate and implement countermeasures that can protect businesses and organisations.

This includes knowledge of the following items:

- how ICT systems are designed and are used in industrial production, in public and private service provision, and in the infrastructure of the society
- why ICT systems and administrative infrastructures can be described as scale-free networks and which consequences scale-freeness has on vulnerability and robustness
- classical reliability theory, including the reliability of software and networks.

Topic(s):

- Introduction to the concept of risk as it is used in technology, insurance and finance.
- Causes of increased risk: overoptimistic belief in market growth, numerical illiteracy, insufficient knowledge of statistics and probability calculus, and the theories of Kahneman and Tversky (anchoring and prospect theory).
- Design and operations of distributed ICT systems, including telecommunications technology and distributed processing.
- Classic reliability theory for hardware and software.
- The theory of random graphs (networks) and their properties with particular emphasis on scale-free graphs. The main concepts of combinatorial complexity and computability are introduced.
- Scale-free networks of the society (technical, administrative and social) and their impact on the vulnerability of the society are identified.

Teaching Methods:
Lectures

Form(s) of Assessment:
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

Re-sit examination:
Ordinary re-sit examnination.

Tillatte hjelpemidler:

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Jan Arild Audestad

Teaching Materials:
Jan A Audestad, *E-Bombs and E-Grenades: The Vulnerability of the Computerized Society* , HiG, 2009 (Available via Fronter)

- Related articles

Publish:
Yes

IMT4601 Research Project Planning - 2011-2012

Course code:
IMT4601

Course name:
Research Project Planning

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn
Vår

Duration (additional text):
The course is offered in the autumn. However, for the spring semester, students can do the course as supervised self study without any lectures, subject to the availability of a supervisor.

Language of instruction:
English

Prerequisite(s):
IMT 4421 Scientific Methodology

Expected learning outcomes:
The Pre-project shall prepare the students to complete their master thesis on time, and with the expected quality.

The course contributes towards the following learning outcomes:

Knowledge

- Possesses advanced knowledge within the area covered by the Master Programme.
- Possesses specialized insight and good understanding of the research frontier in a selected part of the topic covered by the Master Programme.
- Possesses thorough knowledge of professional and scientific theory and methodology of relevance to the topics covered by the Master Programme.
- Is able to apply the knowledge and understanding from the topics covered by the Master Programme to new and unfamiliar settings.

Skills

- Is able to handle theoretical issues, and solve complex practical problems, independently in the area covered by the Master Programme.
- Is able to use relevant and suitable methods when carrying out research and development activities in the area covered by the Master Programme.
- Is able to critically review relevant literature when solving new or complex problems and is able to integrate the findings into the proposed solution.
- Is able to plan and complete an independent and limited research or development project with guidance and in adherence to research ethics.

General competence

- Is able to analyze relevant ethical issues (technological, professional, and scientific)

Having completed the course, the students should have acquired:

- An understanding of academic writing style and documentation structure.
- The ability to formulate a research problem and research questions.
- An understanding of ethical issues in research.

Topic(s):

1. Problem description and choice of methods
2. Identifying, collecting and structuring published research results relevant for the project. Use of library resources
3. Project planning

Teaching Methods:
Lectures

Teaching Methods (additional text):
There are no lectures in the spring semester.

Form(s) of Assessment:
Evaluation of Project(s)

Form(s) of Assessment (additional text):
Mid term report counts 30%. Final report counts 70%. Each student must hand in his/her own individual report. To ensure fairness, course deliverable grading will depend on deliverable quantity, quality and the number of contributing students. Scores can be normalized at the discretion of the instructor/examiner.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner will assess the mid term report. The supervisor is required to provide input to the mid term assessment process. External and internal examiner on the final report.

Re-sit examination:
The whole course must be repeated.

Tillatte hjelpemidler:

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Einar Snekkenes

Publish:
Yes

Home page:
http://www.hig.no/imt/emnesider/imt4601

Elective course, 5 ECTS - 2010-2011

Course name:
Elective course, 5 ECTS

Course level:
Bachelor (syklus 1)

ECTS Credits:
5

Duration:
Autumn and spring

Language of instruction:
Norwegian

Expected learning outcomes:
.

Topic(s):
.

Teaching Methods:
Group works

Form(s) of Assessment:
Exercises

Grading Scale:
Pass/Failure

Tillatte hjelpemidler:

Academic responsibility:
Faculty of Technology, Economy and Management

Course responsibility:
.

Publish:
No

IMT4901 Master's Thesis - 2011-2012

Course code:
IMT4901

Course name:
Master's Thesis

Course level:
Master (syklus 2)

ECTS Credits:
30

Duration:
Autumn
Vår

Duration (additional text):
The duration of the work with the Master's Thesis is limited to 6 working months.

Language of instruction:
Norsk, alternativt engelsk

Prerequisite(s):
All other courses in the study program (90 credits) must be passed before the work on the master thesis can be started.

Expected learning outcomes:
After successfully completing the master thesis, the students are capable of:

- clearly and independently, but with guidance from a supervisor, defining a significant and complex research and development (R&D) problem relevant to the master program
- analyzing existing literature, theories, methods, and interpretations
- independently acquiring new knowledge necessary to complete the project
- planning and conducting necessary studies or experiments, organizing and analyzing data acquired, drawing defensible conclusions, and making recommendations based on these
- documenting the results achieved in a scientific project, mastering the terminology of the field
- presenting the results in oral form.

Topic(s):
The student shall pick a specific problem of relevance to the master's program. The topic must represent a challenge within the specific area and must require that the student adheres to practises that are common within the area. The topic must be preapproved by the supervisor.

Teaching Methods:
Project work
Meeting(s)/Seminar(s)
Tutoring

Teaching Methods (additional text):
Formative feedback from staff and fellow students at the master thesis presentation seminar.

Form(s) of Assessment:
Evaluation of Project(s)

Form(s) of Assessment (additional text):
Evaluation of Project

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
External examiner and internal examiners

Re-sit examination:
After failure, a student may submit a new or a revised thesis once. If the student chooses to submit a revised version of the thesis, this must be submitted in the following semester.

Tillatte hjelpemidler:

Coursework Requirements:
The student must participate in the supervision as a supervisee. The student must continuously be able to present project status to the supervisor and demonstrate that the project can be completed according to the current project plan or, alternatively, adjust the plan accordingly to ensure a successful outcome. The student is required to review the work of one fellow student and to present this review during the student's defense. Each student is also required to participate in the oral presentation held by at least four other fellow students.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Prodekan/Vicedean Rune Hjelsvold

Publish:
Yes

IMT3491 Ethical Hacking and Penetration Testing - 2011-2012

Course code:
IMT3491

Course name:
Ethical Hacking and Penetration Testing

Course level:
Bachelor (syklus 1)

ECTS Credits:
5

Duration:
Autumn

Language of instruction:
English

On the basis of:
IMT2282 Operating systems

Expected learning outcomes:
The student will address the methodology of penetration testing, learning how penetration tests are constructed and experimenting with penetration testing tools in the laboratory. The student will look at vulnerabilities in software both at server and client side, with a high focus on network applications.

The students should after the end of the course have a good overview of how an effective penetration test should take place and of the threats that exists towards software, networks, and network services. A deeper analysis and a set of practical exercises will be the foundation for a deeper understanding into some specific security vulnerabilities that exists.

Topic(s):

- Ethical Hacking and Penetration Testing – definitions
- Penetration Testingx¨ Methodologies
- Password attacks
- Privilege escalation
- Network mapping
- Software vulnerabilities
- Web application problems
- XSS, parameters, persistence
- SQLinjection
- Data mining
- Fuzzing

Teaching Methods:
Lectures
Group works
Laboratory work
Exercises

Form(s) of Assessment:
Written exam, 2 hours
Evaluation of Project(s)

Form(s) of Assessment (additional text):

- Written exam (51%), depending on the number of students the exam might be oral
- Project work (49%)
- Both parts must be passed

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluation by internal and external examiner

Re-sit examination:
Ordinary re-sit examination

New project(s) at next course dates

Tillatte hjelpemidler:

Examination support:
None

Coursework Requirements:
2 approved exercises

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Førsteamanuensis Lasse Øverlier

Teaching Materials:
Articles and book chapters. Specifics to be announced at course start.

Additional information:
In case there will be less than 5 students that will apply for the course, it will be at the discretion of the responsible for the study programme whether the course will be offered or not an if yes, in which form.

Publish:
Yes

IMT3761 Information Warfare - 2011-2012

Course code:
IMT3761

Course name:
Information Warfare

Course level:
Bachelor (syklus 1)

ECTS Credits:
5

Duration:
Autumn

Language of instruction:
Norwegian

Expected learning outcomes:
After completed course the students should have solid understanding of information warfare: computer crime, corporate espionage, and information terrorism.

Topic(s):

- Introduction; Offensive and Defensive Information Warfare
- Cybercrime
- Insider Threat; Corporate Espionage
- Awareness
- Information terrorism
- Information warfare tactics by businesses and government

Teaching Methods:
Lectures
Group works

Form(s) of Assessment:
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
Ordinary re-sit examination

Tillatte hjelpemidler:

Coursework Requirements:
Reports

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Major Roger Johnsen

Teaching Materials:
Books:

- Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages, Andy Jones / Gerald L. Kovacich / Perry G. Luzwick, Auerbach Pub, utgave 1 (ISBN: 0849311144)
- Påvirkning. Teori og praksis., Robert B. Cialdini, utgave 2003 (ISBN: 82-7935-107-8)

Replacement course for:
IMT5051- Information Warfare

Publish:
Yes

IMT3551 Digital Forensics - 2011-2012

Course code:
IMT3551

Course name:
Digital Forensics

Course level:
Bachelor (syklus 1)

ECTS Credits:
5

Duration:
Autumn

Language of instruction:
Norsk, alternativt engelsk

On the basis of:

- IMT2282- Operating Systems
- IMT2431- Data Communication and Network Security

Expected learning outcomes:
Students are able to explain the fundamental principles of digital forensics. The students are able to survey a digital crime scene and to acquire, analyze and present digital evidence in a forensically sound manner.

Topic(s):

- Digital investigations and evidence
- Chain of custodu and forensic soundness
- Timeline analysis
- Live system forensics
- File system forensics
- Forensic reconstructions
- Advanced topics if time permits

Teaching Methods:
Lectures
Laboratory work

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation based on a 100 point scale, where project work counts 50 points and final exam (3 hours) counts 50 points (at least 18 MUST be obtained). Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, the course responsible can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
For the final exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Coursework Requirements:
Will be announced later

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Associate Professor André Årnes (andre.arnes@hig.no)

Teaching Materials:

- Dan Farmer and Wietse Venema: Forensic Discovery, Addison-Wesley, 2005
- Presentation material and selected academic papers

Replacement course for:
IMT3711 Digital Forensic Science

Additional information:
Knowledge of Linux is an advantage

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.

Publish:
Yes

IMT4882 Specialization Course II - 2011-2012

Course code:
IMT4882

Course name:
Specialization Course II

Course level:
Master (syklus 2)

ECTS Credits:
10

Duration:
Autumn
Vår

Duration (additional text):
Can run any time during the full year. Deliveries can be done at any moment, but there will be deadlines for latest deliveries in spring and fall semester.

Language of instruction:
English

Prerequisite(s):
Must be determined by the supervisor based upon the particular assignment.

Expected learning outcomes:
Knowledge:

- The candidate possesses advanced knowledge in a particular research topic.
- The candidate is capable of applying and updating his/her knowledge in a particular research topic.

Skills:

- The candidate is capable of using relevant scientific methods in independent research and analysis in a particular research topic.
- The candidate is capable of performing critical analysis of various literature sources on a particular research topic.
- The candidate knows relevant methods and terminology in a particular research topic.

General competence:

- The candidate is capable of taking part in debates in national and international fora within a particular research topic.
- The candidate is capable of working independently within the field of a particular research topic and knows relevant terminology.
- The candidate is capable of analyzing relevant professional and research publications in a particular research topic.

Objectives:
The student will learn how to master a particular research topic individually and report on this topic at an academic level.

Topic(s):
The student and the supervisor will agree on a topic together. The supervisor is responsible for the fact that the workload for the student should be equivalent to other 10 ECTS courses. The student will work as much as possible independently under supervision of the supervisor.

Teaching Methods:
Other

Teaching Methods (additional text):
The teaching methods depend on the particular topic agreed upon by the student and the supervisor

Form(s) of Assessment:
Evaluation of Project(s)

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Can be both internal and external.

Re-sit examination:
The whole subject must be repeated.

Tillatte hjelpemidler:

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Førsteamanuensis Patrick Bours

Teaching Materials:
Depending on the particular agreed upon topic

Additional information:
This course is intended for students who want to work independently on a particular topic of his/her interest. The student needs to find a supervisor by him/herself. The supervisor and the student will need to agree on a topic together. Topics can be for example (list is not exclusive):
* studying a particular topic from literature
* investigating a particular open research problem
* performing experiments on a research topic
In general the student will write a report on his studies or findings that can be evaluated either by the supervisor or by an external examiner. Another option for the evaluation could be writing an article for a publication or a presentation at a conference or an oral exam with the supervisor or a third person. Generally speaking, the work must have academic merits as can be expected from a master student.

Students are not allowed to take both IMT4881 Specialization course 5 ECTS and IMT4882 Specialization course II 10 ECTS (either IMT4881 or IMT4882).

Publish:
Yes

IMT4721 Authentication - 2011-2012

Course code:
IMT4721

Course name:
Authentication

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Language of instruction:
English

On the basis of:
The course content will be complementary to the course IMT4621 Biometrics

Expected learning outcomes:
Knowledge:

- The candidate possesses thorough knowledge of the security of knowledge based authentication systems.
- The candidate possesses advanced knowlegde in the theory, design and evaluation of Behavioural Biometric Systems.
- The candidate is capable of applying his/her knowledge in the field of IT-security.
- The candidate is capable of updating his/her own knowledge in authentication related topics.

Skills:

- The candidate is capable of using relevant scientific methods in independent research and analysis in biometrics.
- The candidate is capable of performing critical analysis of various literature sources on authentication methods.
- The candidate know relevant authentication methods and terminology.

General competence:

- The candidate is capable of taking part in debates in national and international fora within the field of authentication and behavioural biometrics.
- The candidate is capable of working independently in the field of biometrics and is familiar with biometric terminology.
- The candidate is capable of analyzing relevant professional and research publications in behavioural biometrics.

Objectives:
Give the students an improved understanding of

- Different general authentication mechanisms
- Selected authentication methods: passwods/PIN, gait, signature, keystroke dynamics.
- Technics to test autentication methods

Topic(s):

- Authentication methods in general
- Password security
- (Behavioural) Biometric system evaluation
- Gait recognition
- Keystroke dynamics
- Signature verification

Teaching Methods:
Lectures
Project work
Tutoring

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation based on a 100 point scale, where project work counts 50 points and final exam (3 hours) counts 50 points. Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, emneansvarlig can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner.

Re-sit examination:
For the final exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Examination support:
Calculator and dictionary

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Førsteamanuensis Patrick Bours

Teaching Materials:
There exists a reader written by the professor. The reader is given to the students at the beginning of the course.

Additional information:
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.

Publish:
Yes

IMT4632 Machine Learning and Pattern Recognition II - 2011-2012

Course code:
IMT4632

Course name:
Machine Learning and Pattern Recognition II

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First half of the semester

Language of instruction:
English

Prerequisite(s):
IMT4612 Machine Learning and Pattern Recognition II

Expected learning outcomes:
Knowledge

- The candidate possesses advanced knowledge in pattern recognition systems (symbolic and statistical learning, artificial neural networks, support vector machines, clustering, fuzzy techniques in artificial intelligence, as well as evolutionary computation and hybrid intelligent methods in artificial intelligence).
- The candidate possesses thorough knowledge about theory and scientific methods relevant for machine learning and pattern recognition.
- The candidate is capable of applying his/her knowledge in new fields of machine learning and pattern recognition.

Skills

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of machine learning and pattern recognition and working independently on solving theoretical and practical problems.
- The candidate can use relevant scientific methods in independent research and development in machine learning and pattern recognition.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in the field of machine learning and pattern recognition.
- The candidate is capable of carrying out an independent limited research or development project in machine learning and pattern recognition under supervision, following the applicable ethical rules.

General competence

- The candidate is capable of analyzing relevant professional and research ethical problems in machine learning and pattern recognition.
- The candidate is capable of applying his/her machine learning and pattern recognition knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with terminology in the field of machine learning and pattern recognition.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of machine learning and pattern recognition, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

Topic(s):
1. Symbolic Learning

2. Statistical Learning

3. Artificial Neural Networks

4. Support Vector Machines

5. Cluster Analysis

6. Fuzzy Logic

7. Evolutionary Computation

8. Hybrid Intelligent Methods

Teaching Methods:
Lectures
Group works
Laboratory work
Exercises
Other

Teaching Methods (additional text):
Annet - homework

Form(s) of Assessment:
Written exam, 3 hours
Other

Form(s) of Assessment (additional text):
* Written exam, 3 hours (60%)

* Homework evaluation (4x10%)

All parts must be passed.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
For the written exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
Approved calculator

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke

Teaching Materials:
Basic Textbook: Machine Learning and Data Mining: Introduction to Principles and Algorithms (Paperback) by Igor Kononenko (Author), Matjaz Kukar (Author)
+ selected research papers

Additional Literature for interested readers:
Pattern Recognition and Machine Learning (Information Science and Statistics) by Christopher M. Bishop
Pattern Classification (2nd Edition) by Richard O. Duda, Peter E. Hart, and David G. Stork
Machine Learning by Tom M. Mitchell

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

Publish:
Yes

IMT4671 Organizational and Human Aspects of Information Security - 2011-2012

Course code:
IMT4671

Course name:
Organizational and Human Aspects of Information Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First half of autumn semester

Language of instruction:
English

On the basis of:
Basic understanding of risk analysis and risk assessment. Basic knowledge in technical configuration of security devices such as firewall, IDS, IAM etc

Expected learning outcomes:
In general, this course gives a very practical view of the main task of a corporate security office. The experience of the security office of more than five fortune 500 enterprises is woven in the content and exercises and project work. The influence of the corporate security office on security implementation and configuration will be studied using typical real situations.

Having completed the course, the student should have:

- a sound understanding of corporate organisations and policies, and how the security is embedded into organisation, processes and corporate documentation framework. He/she will be able to plan the set of required security documentations and to implement enterprise specific security organisation and security policies
- an understanding practical awareness and the ability to plan a corporate awareness campaign
- an understanding of security culture and its meaning. The student will be enabled to describe a target security culture and to make an implementation plan for a turn around
- the ability to distinguish between responsibility and delegation. The student will be enabled to provide security in an unfriendly environment with budget constraints and “lack of enthusiasm” for security.
- an understanding of security strategy, security innovation process and its implementation.
- an understanding of future research topic identification and its processes as implemented in European Commission (www.parsicfalproject.eu www.ci2rco.org)

Topic(s):
The course will cover a selection the following or similar topics:

- overview of practical information security management with special focus on human and organisational aspects
- case studies of practical information security policy, strategy, culture, organisation
- defining the various key roles in corporate security management and how they interact
- planning of key elements of corporate security framework
- Security innovation process in enterprises and research.

Teaching Methods:
Other

Teaching Methods (additional text):
Lectures, seminars or guided self study, role games, project work, depending on the number of students: Term paper(s)

Form(s) of Assessment:
Oral exam, individually
Other

Form(s) of Assessment (additional text):

- Oral examination: for 20-25 minutes, if the number of students is too big, it will be turned to a written exam: (65%)
- Term paper(s): (35%)
- Pass decision is on the cumulative grade.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
A new term paper must be provided and the examination must be re-sat.

Tillatte hjelpemidler:

Coursework Requirements:
Two presentation in respect to the term paper will take place during the semester:

- In the second week each students presents a concept of the term paper (content), the methodical approach and the resources which will be used during work. Presentation lasts 5 Minutes. Each student will receive comments from the class and the teacher.

- In the last lectures of the Semester a presentation of the term paper (about 30 minutes) as a coaching for a mini presentation at the oral exam is given by the students.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Prof. Bernhard Hammerli

Teaching Materials:
TBA

Additional information:
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.

Publish:
Yes

IMT4772 Risk Management II - 2011-2012

Course code:
IMT4772

Course name:
Risk Management II

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
Second half of autumn semester

Language of instruction:
English

Expected learning outcomes:
The course contributes towards the following learning outcomes:

Knowledge

- Possesses advanced knowledge within the area covered by the Master Programme.
- Possesses specialized insight and good understanding of the research frontier in a selected part of the topic covered by the Master Programme..

Skills

- Is able to analyze existing theories, methods and interpretations and to challenge established knowledge and practice in the media technology area.
- Is able to use relevant and suitable methods when carrying out research and development activities in the area of media technologyF4: Is able to critically review relevant literature when solving new or complex problems and is able to integrate the findings into the proposed solution.
- Is able to plan and complete an independent and limited research or development project with guidance and in adherence to research ethics.

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.

Topic(s):

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

Teaching Methods:
Lectures
Exercises

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):

- Written exam 3 hours (alternatively oral exam): 51%
- Projects: 49%.
- Both parts must be passed.

To ensure fairness, course deliverable grading will depend on deliverable quantity, quality and the number of contributing students.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by external and internal examiner.

Re-sit examination:
For the written exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
Approved calculator

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Einar Snekkenes

Teaching Materials:
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

Replacement course for:
IMT4771

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

Publish:
Yes

IMT4881 Specialization Course - 2011-2012

Course code:
IMT4881

Course name:
Specialization Course

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn
Vår

Duration (additional text):
Can run any time during the full year. Deliveries can be done at any moment, but there will be deadlines for latest deliveries in spring and fall semester.

Language of instruction:
English

Prerequisite(s):
Must be determined by the supervisor based upon the particular assignment.

Expected learning outcomes:
Knowledge:

- The candidate possesses advanced knowledge in a particular research topic.
- The candidate is capable of applying and updating his/her knowledge in a particular research topic.

Skills:

- The candidate is capable of using relevant scientific methods in independent research and analysis in a particular research topic.
- The candidate is capable of performing critical analysis of various literature sources on a particular research topic.
- The candidate knows relevant methods and terminology in a particular research topic.

General competence:

- The candidate is capable of taking part in debates in national and international fora within a particular research topic.
- The candidate is capable of working independently within the field of a particular research topic and knows relevant terminology.
- The candidate is capable of analyzing relevant professional and research publications in a particular research topic.

Objectives:
The student will learn how to master a particular research topic individually and report on this topic at an academic level.

Topic(s):
The student and the supervisor will agree on a topic together. The supervisor is responsible for the fact that the workload for the student should be equivalent to other 5 ECTS courses. The student will work as much as possible independently under supervision of the supervisor.

Teaching Methods:
Other

Teaching Methods (additional text):
The teaching methods depend on the particular topic agreed upon by the student and the supervisor

Form(s) of Assessment:
Evaluation of Project(s)

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Can be both.

Re-sit examination:
The whole subject must be repeated.

Tillatte hjelpemidler:

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Førsteamanuensis Patrick Bours

Teaching Materials:
Depending on the particular agreed upon topic

Additional information:
This course is intended for students who want to work independently on a particular topic of his/her interest. The student needs to find a supervisor by him/herself. The supervisor and the student will need to agree on a topic together. Topics can be for example (list is not exclusive):
* studying a particular topic from literature
* investigating a particular open research problem
* performing experiments on a research topic
In general the student will write a report on his studies or findings that can be evaluated either by the supervisor or by an external examiner. Another option for the evaluation could be writing an article for a publication or a presentation at a conference or an oral exam with the supervisor or a third person. Generally speaking, the work must have academic merits as can be expected from a master student.

Students are not allowed to take both IMT4881 Specialization course 5 ECTS and IMT4882 Specialization course II 10 ECTS (either IMT4881 or IMT4882).

Publish:
Yes

IMT4741 Intrusion detection and prevention - 2011-2012

Course code:
IMT4741

Course name:
Intrusion detection and prevention

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

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

Language of instruction:
English

Expected learning outcomes:
Knowledge

The candidate possesses advanced knowledge in detection and prevention of intrusions in modern computer systems and networks.

The candidate possesses thorough knowledge about theory and scientific methods relevant for intrusion detection.

The candidate is capable of applying his/her knowledge in new fields of intrusion detection and prevention.

Skills

The candidate is capable of analyzing existing theories, methods and interpretations in the field of intrusion detection and working independently on solving theoretical and practical problems.

The candidate can use relevant scientific methods in independent research and development in intrusion detection.

The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in the field of intrusion detection and prevention.

The candidate is capable of carrying out an independent limited research or development project in intrusion detection under supervision, following the applicable ethical rules.

General competence

The candidate is capable of analyzing relevant professional and research ethical problems in the field of intrusion detection.

The candidate is capable of applying his/her knowledge and skills in new fields, in order to accomplish advanced tasks and projects.

The candidate can work independently and is familiar with terminology in the field of intrusion detection and prevention.

The candidate is capable of discussing professional problems, analyses and conclusions in the field of intrusion detection and prevention, both with specialists and with general audience.

The candidate is capable of contributing to innovation and innovation processes.

Topic(s):
1. Definition and classification of IDS systems

2. Basic elements of attacks against data networks and their detection

3. Misuse-based IDS

4. Anomaly-based IDS

5. Testing IDS and measuring their performances

Teaching Methods:
Lectures
Laboratory work
Exercises
Project work

Teaching Methods (additional text):
Lectures

Laboratory exercises

Numerical exercises

Project work

Form(s) of Assessment:
Written exam, 3 hours
Evaluation of Project(s)

Form(s) of Assessment (additional text):
Written Exam, 3 hours (counts 70% of the final mark)

Project evaluation (counts 30% of the final mark)

Both parts must be passed.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
Ordinary re-sit examination.

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:
Obligatory literature:
None.
Recommended literature:
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.

Replacement course for:
IMT5151 Intrusion detection and prevention

Additional information:
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 and if yes, in which form.

Publish:
Yes

IMT4751 Wireless communication security - 2011-2012

Course code:
IMT4751

Course name:
Wireless communication security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

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

Language of instruction:
English

Prerequisite(s):
The student is required to have some knowledge of cryptography equivalent to IMT4532 (Cryptology 1)

Expected learning outcomes:
Knowledge

The candidate possesses advanced knowledge in the field of wireless communication security, which includes the following topics: security in RFID, wireless LAN, Bluetooth, 2G and 3G mobile telephony.

The candidate possesses thorough knowledge about theory and scientific methods relevant for wireless communication security.

The candidate is capable of applying his/her knowledge in new fields of wireless communication security.

Skills

The candidate is capable of analyzing existing theories, methods and interpretations in the field of wireless communication security and working independently on solving theoretical and practical problems.

The candidate can use relevant scientific methods in independent research and development in wireless communication security.

The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in the field of wireless communication security.

The candidate is capable of carrying out an independent limited research or development project in wireless communication security under supervision, following the applicable ethical rules.

General competence

The candidate is capable of analyzing relevant professional and research ethical problems in the field of wireless communication security.

The candidate is capable of applying his/her knowledge and skills in new fields, in order to accomplish advanced tasks and projects.

The candidate can work independently and is familiar with terminology in the field of wireless communication security.

The candidate is capable of discussing professional problems, analyses and conclusions in the field of wireless communication security, both with specialists and with general audience.

The candidate is capable of contributing to innovation and innovation processes.

Topic(s):
1. Basic radio-frequency communications

2. RFID, Wireless LAN, Bluetooth security

3. Security of 2G mobile telephony systems

4. Security of 3G mobile telephony systems

Teaching Methods:
Lectures
Project work

Teaching Methods (additional text):
Lectures

Project work

Form(s) of Assessment:
Written exam, 3 hours
Evaluation of Project(s)

Form(s) of Assessment (additional text):
Written exam, 3 hours (counts 70% of the final mark)

Project evaluation (counts 30% of the final mark)

Both parts must be passed.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
Ordinary re-sit examination

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. 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

Replacement course for:
IMT5171 - Wireless communication security

Additional information:
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 and if yes, in which form.

Publish:
Yes

IMT4762 Risk Management I - 2011-2012

Course code:
IMT4762

Course name:
Risk Management I

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First part of the semester

Language of instruction:
English

Expected learning outcomes:
When the course is completed, the student will be able to:

- Give a detailed description of the process of risk assessment
- Explain how to plan and organize a risk assessment project in general
- Analyse details in one method/ framework in risk assessment
- Practice and use one method/ framework for Risk Assessment in a practical case working in a team
- Discuss the challenges facing the IS Risk Analyst through teamwork in a practical case

Topic(s):
Risk Assessment in the context of an Information Security Management system
Study of a method/framework for risk assessment

Teaching Methods:
Lectures
Group works
Net Support Learning
Project work
Meeting(s)/Seminar(s)
Tutoring

Teaching Methods (additional text):
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 assessment 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.

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

Form(s) of Assessment (additional text):
The project counts 49% and oral exam counts 51% towards the final grade.
Students are recommended to work in groups with the project. Every group must have no more than 3 members. It is also possible to complete the project individually. To ensure fairness, course deliverable grading will depend on deliverable quantity, quality and the number of contributing students.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by external and internal examiner.

Re-sit examination:
Not allowed.

Tillatte hjelpemidler:

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Høgskolelektor Tone Hoddø Bakås

Teaching Materials:
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

Publish:
Yes

IMT3511 Discrete Mathematics - 2011-2012

Course code:
IMT3511

Course name:
Discrete Mathematics

Course level:
Bachelor (syklus 1)

ECTS Credits:
10

Duration:
Spring and autumn

Duration (additional text):
In principle this course will be given in the spring semester, but in case there is enough interest, then it can also be given in the fall semester.

Language of instruction:
English

Expected learning outcomes:
Knowledge:

- The candidate possesses knowledge of important topics within abstract algebra.
- The candidate possesses knowlegde of important topics within combinatorics.
- The candidate possesses knowlegde of fundamental topics within graph theory.

Skills:

- The candidate knows relevant methods and terminology in discrete mathematics.
- The candidate is capable of applying his/her knowledge in different courses.

General competence:

- The candidate is capable of understanding and analyzing problems related to abstract algebra, combinatorics and graph theory.

Objectives:
After the course, the students should acquire:

- Understanding of the most important topics of abstract algebra
- Understanding of the most important topics of combinatorics, including fundamentals of graph theory.

Topic(s):
General concepts:
* Logic, proofs, sets, algorithms, induction and recursion, combinatorics, discrete probabilities

Graphs:
* Connectivity, shortest path, (minimal) spanning trees

Modeling computation:
* Finite-state machines, Turing machines

Abstract algebra:
* Groups, rings, fields

Teaching Methods:
Lectures
Exercises
Tutoring

Teaching Methods (additional text):
The course is given as a self reading course, where there is time for the students during lectures to raise questions on the theory and/or the exercises.

Form(s) of Assessment:
Oral exam, individually

Form(s) of Assessment (additional text):
Candidates will get an oral exam (max 30 minutes) with written preparation (max 60 minutes). Candidates will be given a number of assignments within the topics of the course and 60 minutes to prepare written answers. After this the candidates will be questioned about their answer in the oral part.

If the number of students is too high, then the oral exam is replaced by a 3 hour written exam. The students will be notified about this one month prior to the exam at the latest.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer.

Re-sit examination:
The whole subject must be repeated.

Tillatte hjelpemidler:

Examination support:
Ordinary calculator and dictionary

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Førsteamanuensis Patrick Bours

Teaching Materials:
- Kenneth H. Rosen:
Discrete Mathematics and its Applications, 6th ed.
McGraw-Hill International Edition (2007).
- William J. Gilbert and W. Keith Nicholson
Modern Algebra with Applications, 2nd ed.
Wiley (2004).

Additional information:
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.

Publish:
Yes

IMT4621 Biometrics - 2011-2012

Course code:
IMT4621

Course name:
Biometrics

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Duration (additional text):
First half of spring semester

Language of instruction:
English

Prerequisite(s):
None

On the basis of:
The course content will be complementary to the course IMT4721 "Authentication".

Expected learning outcomes:
Knowledge:

The candidate possesses advanced knowledge in Biometrics.

The candidate possesses thorough knowledge about theory and scientific methods relevant for design, development and operation of biometric access control systems.

The candidate is capable of applying his/her knowledge in new fields of IT-security systems.

Skills

The candidate is capable of analyzing existing theories, methods and interpretations in the field of biometrics and working independently on solving theoretical and practical problems.

The candidate can use relevant scientific methods in independent research and development in biometrics.

The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in biometrics.

The candidate is capable of carrying out an independent limited research or development project in biometrics under supervision, following the applicable ethical rules.

General competence

The candidate is capable of analyzing relevant professional and research ethical problems in biometrics.

The candidate is capable of applying his/her biometric knowledge and skills in new fields, in order to accomplish advanced tasks and projects.

The candidate can work independently and is familiar with biometric terminology.

The candidate is capable of discussing professional problems, analyses and conclusions in the field of biometrics, both with specialists and with general audience.

The candidate is capable of contributing to innovation and innovation processes.

Objectives:

After the course, the students should have acquired:

1. Knowledge about common statistical tools for biometrics

2. Insight into advantages and disadvantages of biometric characteristics

3. Understanding of multimodal biometrics

4. Knowledge of ethical and privacy issues in biometrics.

5. Understanding of the threats and protection mechanisms for biometric data

Topic(s):
• Fingerprint recognition

• Vein recognition

• Face recognition specifically focused on three dimensional data

• Iris recognition

• Multimodal biometrics

• Attack mechanisms

• Privacy Enhancing Technologies

Content

In this course, several key aspects of biometrics are covered. The course begins with an overview of applied statistics and hypothesis tests as well as other common statistical tools for biometrics, and then covers selected biometric concepts, particularly fingerprint recognition, vein recognition, face recognition and iris recognition. To this end, the relevant physiological characteristics, their variability, and potential problems are discussed before analyzing different approaches for each of the attributes to be investigated. In each case, not only benign applications are covered but also potential bottlenecks such as insufficient sample quality along the entire processing chain. The use of multi-biometrics including data fusion is discussed both in the context of robustness against attacks and improving the overall accuracy of the recognition process. The course continues with a discussion of the ethical and privacy-related issues in biometrics, along with possible limitations and technical mitigation mechanisms. Special attention is given to privacy enhancing technologies that provides protection of sensitive biometric data. In this line the course concludes with comparison-on-card approaches and template protection concepts that allow revocation of biometric references.

Teaching Methods:
Other

Teaching Methods (additional text):
Tutorial: Afternoon sessions with seminar discussion and practical tasks

Form(s) of Assessment:
Written exam, 3 hours

Form(s) of Assessment (additional text):
Written examination in English

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by an external examiner.

Re-sit examination:
Ordinary re-sit examination.

Tillatte hjelpemidler:

Examination support:
Dictionaries allowed (no calculator)

Coursework Requirements:
Students can contribute a research report (term paper) on a topic that is chosen by the student in coordination with the lecturer, which will be considered for the assessment

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Christoph Busch

Teaching Materials:
Recommended literature:

[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, 2005.

[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., SKORIC, B., KEVENAAR, T. Security with Noisy Data. Springer-Verlag, 2007

Additional information:
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.

Publish:
Yes

IMT4612 Machine Learning and Pattern Recognition I - 2011-2012

Course code:
IMT4612

Course name:
Machine Learning and Pattern Recognition I

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Language of instruction:
English

Prerequisite(s):
BSc level basics in statistics and mathematics, Image analysis and processing course (1st semester)

On the basis of:
Expected prior-knowledge: Understanding of basic statistics like probability density function, variance, etc. Basic analysis and matrix algebra. Digital image Processing with
Mathlab (a student should be able to do some basic manipulations of images)

Expected learning outcomes:
The studentsdevelops understanding of use of statistical analysis for multidimensional data. It also give fundamentals to understand data analysis from raw measurement values
to higher level decision making in color and image context. The students develops basic understanding for difference between analysis with or without a priori data as well as ways to evaluate results. The methods will be learned in practical sessions, where they will be programmed and tested with real data. The course is practice oriented, where students learn basics of data analysis useful in color, color image and spectral image analysis and processing. In lectures basics of methods are lectures and in practical session, their usage is practices. The aim is not to get deep theoretical understanding and derivation of methods.

On completion of this course the students will be able to:

- Understand principles how multidimensional statistical methods differ from one dimensional methods.
- Program some basic clustering and classification methods and test their validity.
- Program some basic Neural networks methods and test their validity.
- Extract features from raw, measured values of data to be analysed.
- Understand the distribution of information in statistical analysis and meaning in data representation.
- To apply basic statistical and data analysis methods to color and image data.

Topic(s):
Basics of multidimensional statistical analysis.

- Principal component analysis.
- Data classification: Bayesian classifier, k-NN classifier, basics of neural networks.
- Data clustering: k-means clustering, Self-Organizing map.
- Classification and clustering validity testing: leave-one-out, ground truth.

Practical Laboratory Sessions:

- Write spectral color and image data reading and writing routines by Matlab
- Produce PCA component images and reconstruct spectral images from PCA eigenimages
- Realize some classification methods by Matlab
- Realize some clustering methods by Matlab
- Make simple tests of spectral image segmentation, spectral image categorization etc. using learned methods

Teaching Methods:
Lectures
Laboratory work
Net Support Learning
Exercises

Form(s) of Assessment:
Written exam, 3 hours
Exercises

Form(s) of Assessment (additional text):

- Exam (70%
- Exercises (30%)
- Each part must be individually approved of

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
One internal and one external examiner

Re-sit examination:
For the exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke

Teaching Materials:
Literature and study materials: Handouts of the material covered in the lectures will be distributed.

- R.O.Duda, P.E. Hart, and D.G. Storck: Pattern Classification. 2nd ed., Wiley, 2001
- Sergios Theodoridis, Konstantinos Koutroumbas. “Pattern Recognition”, third edition. Academic Press.

Replacement course for:
IMT4611

Additional information:
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.

Publish:
Yes

IMT4641 Computational Forensics - 2011-2012

Course code:
IMT4641

Course name:
Computational Forensics

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Duration (additional text):
Second half of spring semester

Language of instruction:
English

Expected learning outcomes:

- ability to work with the original scientific literature
- understanding of cutting-edge problems in computational and forensic sciences as well as their applications

Topic(s):
Forensic Imaging,

Signal and Video Processing,

Computer Visualization,

Forensic Statistics and Intelligence,

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.

Teaching Methods:
Project work

Teaching Methods (additional text):
Annet - Face-to-Face Meetings Assignments.

Form(s) of Assessment:
Evaluation of Project(s)

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
The whole subject must be repeated.

Tillatte hjelpemidler:

Examination support:
Approved calculator

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke

Teaching Materials:
Scientific Articles related to the field of Specialization.

Additional information:
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.

Publish:
Yes

IMT4541 Foundations of Information Security - 2010-2011

Course code:
IMT4541

Course name:
Foundations of Information Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First half of autumn semester

Language of instruction:
English

Expected learning outcomes:
Having completed the course, the student should have

- understood the key modelling techniques used for secure computer systems and reasoning about them
- good understanding of models and mechanisms for identification and authentication and access control
- obtained a solid understanding of security analysis and developmental assurance techniques and issues

Topic(s):

- 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

Teaching Methods:
Other

Teaching Methods (additional text):

- Lectures
- Term paper

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):

- Written exam, 3 hours, (alternatively oral exam): 67%
- Term paper: 33%
- Pass decision is on the cumulative grade

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by external and internal examiner.

Re-sit examination:
A new term paper must be provided next autumn. For the exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Examination support:
Dictionary, simple calculator

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Stephen Wolthusen

Teaching Materials:
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

Replacement course for:
IMT4162 Information Security and Security Architecture

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

Publish:
Yes

IMT4552 Cryptology 2 - 2010-2011

Course code:
IMT4552

Course name:
Cryptology 2

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
Second part of autumn semester

Language of instruction:
English

Prerequisite(s):
IMT4531 Cryptology 1

Expected learning outcomes:
In the course the students will acquire:

- Advanced level of understanding of methods of analysis and synthesis of cryptographic systems

- Deep understanding of modern cryptographic theory

Topic(s):
1. Stream ciphers

2. Block ciphers

3. Public key ciphers with applications.

Teaching Methods:
Lectures
Exercises

Teaching Methods (additional text):
Lectures

Problem solving exercises

Form(s) of Assessment:
Written exam, 3 hours

Form(s) of Assessment (additional text):
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
Ordinary re-sit examination.

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. 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

Replacement course for:
IMT4551 Selected Topics in Cryptology

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

Publish:
Yes

Home page:
http://www.hig.no/imt/emnesider/imt4552

IMT4541 Foundations of Information Security - 2011-2012

Course code:
IMT4541

Course name:
Foundations of Information Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
First half of autumn semester

Language of instruction:
English

Expected learning outcomes:
Having completed the course, the student should have

- understood the key modelling techniques used for secure computer systems and reasoning about them
- good understanding of models and mechanisms for identification and authentication and access control
- obtained a solid understanding of security analysis and developmental assurance techniques and issues

Topic(s):

- 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

Teaching Methods:
Other

Teaching Methods (additional text):

- Lectures
- Term paper

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):

- Written exam, 3 hours, (alternatively oral exam): 67%
- Term paper: 33%
- Pass decision is on the cumulative grade

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by external and internal examiner.

Re-sit examination:
A new term paper must be provided next autumn. For the exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Examination support:
Dictionary, simple calculator

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Stephen Wolthusen

Teaching Materials:
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

Replacement course for:
IMT4162 Information Security and Security Architecture

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

Publish:
Yes

IMT4561 Applied Information Security - 2011-2012

Course code:
IMT4561

Course name:
Applied Information Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
Second half of autumn semester

Language of instruction:
English

Expected learning outcomes:
Students who have passed this course should:

- have acquired good knowledge of the common terminology in information security
- have working knowledge of security analysis methods
- have a good understanding of selected attack mechanisms and techniques and their employment by malicious software
- have working knowledge of database security
- have good understanding of design principles for secure information systems

Topic(s):

- Core terminology for information security
- Authentication and authentication techniques
- Security analysis methods
- Design principles for secure information systems
- Case studies of secure system design
- Database security
- Attack mechanisms and techniques
- Malicious software

Teaching Methods:
Lectures
Exercises
Project work
Other

Teaching Methods (additional text):
Annet - Tutorials

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
Written examination, 3 hours, (67%) in conjunction with term paper (33%). Pass decision is on the cumulative grade.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer.

Re-sit examination:
A new term paper must be provided next autumn. For the exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Examination support:
Simple calculator

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Stephen Wolthusen

Teaching Materials:
Books:

- M. Bishop: Computer Security: Art and Science. Addison-Wesley, Reading, MA, USA (2002)
- D. Gollmann: Computer Security, 2nd ed. John Wiley & Sons, New York, NY, USA (2006)
- M. Gasser: Building a Secure Computer System. Van Nostrand Reinhold, New York, NY, USA (1988)
- R. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Chichester, UK (2001)
- A. K. Jain, P. J. Flynn, and A. A. Ross: Handbook of Biometrics. Springer-Verlag, Berlin, Germany (2007)

Replacement course for:
IMT4162 Information Security and Security Architecture

Publish:
Yes

IMT4904 Master's Thesis - 2012-2013

Course code:
IMT4904

Course name:
Master's Thesis

Course level:
Master (syklus 2)

ECTS Credits:
30

Duration:
Autumn
Vår

Duration (additional text):
The duration of the work with the Master's Thesis is limited to 6 working months.

This course description is valid from **spring 2013.**

Language of instruction:
Norsk, alternativt engelsk

Prerequisite(s):
All other courses in the study program (90 credits) must be passed before the work on the master thesis can be started.

- See here for course home page

Expected learning outcomes:
After successfully completing the program, students:

Knowledge

- Possess specialised insight into a scientific area and relevant scientific work
- Possess knowledge of theories and methods being used in the area of specialisation

Skills

- Are capable of defining a significant and complex research and development (R&D) problem relevant to the master program, clearly and independently, but with guidance from a supervisor
- Are capable of analyzing existing literature, theories, methods, and interpretations
- Are capable of planning and conducting necessary studies or experiments, organizing and analyzing data acquired, drawing defensible conclusions, and making recommendations based on these
- Are capable of documenting the results achieved in a scientific project, mastering the terminology of the field

General Competence

- Are capable of acquiring new knowledge
- Are capable of presenting scientific work and results in oral form

Topic(s):
The student shall pick a specific problem of relevance to the master's program. The topic must represent a challenge within the specific area and must require that the student adheres to practises that are common within the area. The topic must be preapproved by the supervisor.

Teaching Methods:
Project work
Meeting(s)/Seminar(s)
Tutoring

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

Form(s) of Assessment (additional text):
All of the following parts will be assessed individually:

- The written thesis accounts for 80% of the final grade
- An oral presentation accounts for 15%
- An oral examination of each student accounts for the remaining 5%.
- All parts need to be passed.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
External examiner and internal examiners

Re-sit examination:
After failure, a student may submit a new or a revised thesis once. If the student chooses to submit a revised version of the thesis, this must be submitted in the following semester. The resubmitted thesis will be subject to a new oral presentation and a new oral examination.

Tillatte hjelpemidler:

Coursework Requirements:
The student must participate in the supervision as a supervisee. The student must continuously be able to present project status to the supervisor and demonstrate that the project can be completed according to the current project plan or, alternatively, adjust the plan accordingly to ensure a successful outcome.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Prodekan/Vicedean Ivar Farup

Publish:
Yes

IMT4532 Cryptology 1 - 2011-2012

Course code:
IMT4532

Course name:
Cryptology 1

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

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

Language of instruction:
English

Expected learning outcomes:
Knowledge

- The candidate possesses advanced knowledge in classical cryptography, as well as fundamentals of stream ciphers, block ciphers and public key ciphers.
- The candidate possesses thorough knowledge about theory and scientific methods relevant for cryptology.
- The candidate is capable of applying his/her knowledge in new fields of cryptology.

Skills

- The candidate is capable of analyzing existing theories, methods and interpretations in the field of cryptology and working independently on solving theoretical and practical problems.
- The candidate can use relevant scientific methods in independent research and development in cryptology.
- The candidate is capable of performing critical analysis of various literature sources and applying them in structuring and formulating scientific reasoning in cryptology.
- The candidate is capable of carrying out an independent limited research or development project in cryptology under supervision, following the applicable ethical rules.

General competence

- The candidate is capable of analyzing relevant professional and research ethical problems in cryptology.
- The candidate is capable of applying his/her cryptographic knowledge and skills in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with cryptographic terminology.
- The candidate is capable of discussing professional problems, analyses and conclusions in the field of cryptology, both with specialists and with general audience.
- The candidate is capable of contributing to innovation and innovation processes.

Topic(s):
1. Classical cryptography - history of cryptography, fundamentals of information theory and its application in cryptography

2. Symmetric ciphers - stream and block ciphers

3. Asymmetric ciphers - fundamentals, RSA

4. Hash functions and digital signatures.

Teaching Methods:
Lectures
Exercises

Teaching Methods (additional text):
Lectures

Numerical exercises

Form(s) of Assessment:
Written exam, 3 hours

Form(s) of Assessment (additional text):
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
Ordinary re-sit examination.

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. 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

Replacement course for:
IMT4531 Introduction to Cryptology

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

Publish:
Yes

Home page:
http://www.hig.no/imt/emnesider/imt4532

IMT4581 Network Security - 2011-2012

Course code:
IMT4581

Course name:
Network Security

Course level:
Master (syklus 2)

ECTS Credits:
10

Duration:
Vår

Language of instruction:
English

On the basis of:
Some knowledge of cryptology course.

Expected learning outcomes:
The student is expected to have insight into:

- why network security is important and why it should not be neglected
- which mechanisms are required and available for protection of networked systems
- how these mechanisms are used to solve security challenges in particular systems

The course will provide the student with the foundation required for implementing protection systems and for continuing research in the field.

Topic(s):
Part I Introduction :

- Network infrastructure and security threats

Part II Protection methods :

- Encryption, device authentication, message authentication and protection of integrity.
- Key management: symmetric keys, public key infrastructure, certificates, revocation, and key escrows.
- Distributed access control
- Anatomy of attacks, firewalls, and protection against attacks

Part III Applications of security mechanisms

- Internet security (PGP, IPsec, NLS)
- Mobile security (GSM/UMTS architectures and security objectives, security functions of USIM, management of anonymity in mobile networks, use of USIM security to protect other systems)
- Non-repudiation (principles, collection of evidence, example of protocols)
- Payment systems (CyberCash, NetBill, Ecash)

Teaching Methods:
Essay
Lectures

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation is based on a 100 point scale, where the essay counts 50 points and the final exam (3 hours) counts 50 points. Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, emneansvarlig can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
For the final exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
None

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Adjunct Professor Jan Audestad

Teaching Materials:
Available via Fronter.

Replacement course for:
IMT4101

Publish:
Yes

IMT4012 Digital Forensics I - 2010-2011

Course code:
IMT4012

Course name:
Digital Forensics I

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Language of instruction:
English

Prerequisite(s):
BSc level basics in operating systems, data communication and network security.

Expected learning outcomes:
The course develops detailed understanding in the methodology of digital forensics. It also introduces the core principles and common terminology in digital forensics. Students will be expected to gain advanced knowledge in order to survey a digital crime scene as well as to acquire, analyze, and present digital evidence in a forensically sound manner.

The course is oriented towards practice, where the students learn advanced techniques of digital evidence analysis useful in computer, network and Internet forensics. In the lectures, advanced digital forensics methods are taught and in the laboratory sessions, their usage in practice is exercised thoroughly.

Topic(s):

- Digital investigations and evidence
- Chain of custody and forensic soundness
- Timeline analysis
- Live system forensics
- File system forensics
- Forensic reconstructions
- Advanced topics if time permits

Teaching Methods:
Lectures
Laboratory work

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation based on a 100 point scale, where project work counts up to 50 points and final exam (3 hours) counts up to 50 points (at least 18 at the written exam MUST be obtained). Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, the course responsible can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
For the final exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Coursework Requirements:
None

Academic responsibility:
Faculty of Technology, Economy and Management

Course responsibility:
Adjunct Associate Professor André Årnes (andre.arnes@hig.no)

Teaching Materials:
Dan Farmer and Wietse Venema: Forensic Discovery, Addison-Wesley, 2005 (ISBN 0-201-63497-x)

Presentation material and selected academic papers

Additional information:
Knowledge of Linux is an advantage.

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

The policy of the Gjøvik University College is that a student that takes a subject at the 3000 level cannot take the subject with the same name at the 4000 level. 100% overlap between IMT3551 and IMT 4012.

Publish:
Yes

IMT4022 Digital Forensics II - 2010-2011

Course code:
IMT4022

Course name:
Digital Forensics II

Course level:
Master (syklus 2)

ECTS Credits:
10

Duration:
Vår

Language of instruction:
English

Prerequisite(s):

- BSc level basics in operating systems, data communication and network security
- IMT4012 Digital Forensics I or IMT3551 Digital Forensics or equivalent.

Expected learning outcomes:
The course develops deep understanding in the methodology, technology and application of digital forensics. Students are expected to reach an advanced level of knowledge in the broad spectrum of digital evidence, analysis methods and tools.

The course is oriented towards profound theoretical background, where the students learn contemporary techniques and advanced research topics.

Topic(s):

- Forensics and Incident Response
- Microsoft Windows Host Forensic
- Unix and Linux Host Forensics
- Live Forensics and RAM Analysis
- Network and Cloud Forensics
- Botnet and Malware Analysis
- Mobile and Embedded Device Analysis
- Securing Evidence, Cryptanalysis and Anti-Forensics
- Steganography
- eDiscovery: Fingerprinting, Correlation, and Search

Teaching Methods:
Lectures
Laboratory work

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation based on a 100 point scale, where project work counts up to 50 points and final exam (3 hours) counts up to 50 points (at least 18 at the written exam MUST be obtained). Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, the course responsible can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
For the final exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke (katrin.franke@hig.no) /Adjunct Associate Professor André Årnes (andre.arnes@hig.no)

Teaching Materials:
Keith J. Jones, Richard Bejtlich, Curtis W. Rose: Real Digital Forensics: Computer Security and Incident Response. Addison-Wesley, 2005, (0-321-24069-3)

Dan Farmer and Wietse Venema: Forensic Discovery, Addison-Wesley, 2005 (ISBN 0-201-63497-x)

Presentation material and selected academic papers

Additional information:
Knowledge of Linux is an advantage

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

Publish:
Yes

IMT4641 Computational Forensics - 2010-2011

Course code:
IMT4641

Course name:
Computational Forensics

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Duration (additional text):
Second half of spring semester

Language of instruction:
English

Expected learning outcomes:
* ability to work with the original scientific literature

* understanding of cutting-edge problems in computational and forensic sciences as well as their applications.

Topic(s):
Forensic Imaging,

Signal and Video Processing,

Computer Visualization,

Forensic Statistics and Intelligence,

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.

Teaching Methods:
Project work

Teaching Methods (additional text):
Annet - Face-to-Face Meetings Assignments.

Form(s) of Assessment:
Evaluation of Project(s)

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer(s)

Re-sit examination:
The whole subject must be repeated.

Tillatte hjelpemidler:

Examination support:
Approved calculator

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke

Teaching Materials:
Scientific Articles related to the field of Specialization.

Additional information:
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.

Publish:
Yes

IMT4612 Machine Learning and Pattern Recognition I - 2010-2011

Course code:
IMT4612

Course name:
Machine Learning and Pattern Recognition I

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Language of instruction:
English

Prerequisite(s):
BSc level basics in statistics and mathematics, Image analysis and processing course (1st semester)

On the basis of:
Expected prior-knowledge: Understanding of basic statistics like probability density function, variance, etc. Basic analysis and matrix algebra. Digital image Processing with
Mathlab (a student should be able to do some basic manipulations of images)

Expected learning outcomes:
This course develops understanding of use of statistical analysis for multidimensional data. It also give fundamentals to understand data analysis from raw measurement values
to higher level decision making in color and image context. The course develops basic understanding for difference between analysis with or without a priori data as well as ways to evaluate results. The methods will be learned in practical sessions, where they will be programmed and tested with real data. The course is practice oriented, where students learn basics of data analysis useful in color, color image and spectral image analysis and processing. In lectures basics of methods are lectures and in practical session, their usage is practices. The aim is not to get deep theoretical understanding and derivation of methods.

On completion of this course the students will be able to:
- Understand principles how multidimensional statistical methods differ from one dimensional methods.
- Program some basic clustering and classification methods and test their validity.
- Program some basic Neural networks methods and test their validity.
- Extract features from raw, measured values of data to be analysed.
- Understand the distribution of information in statistical analysis and meaning in data representation.
- To apply basic statistical and data analysis methods to color and image data.

Topic(s):
Basics of multidimensional statistical analysis.
- Principal component analysis.
- Data classification: Bayesian classifier, k-NN classifier, basics of neural networks.
- Data clustering: k-means clustering, Self-Organizing map.
- Classification and clustering validity testing: leave-one-out, ground truth.

Practical Laboratory Sessions:
- Write spectral color and image data reading and writing routines by Matlab
- Produce PCA component images and reconstruct spectral images from PCA eigenimages
- Realize some classification methods by Matlab
- Realize some clustering methods by Matlab
- Make simple tests of spectral image segmentation, spectral image categorization etc. using learned methods

Teaching Methods:
Lectures
Laboratory work
Net Support Learning
Exercises

Form(s) of Assessment:
Written exam, 3 hours
Exercises

Form(s) of Assessment (additional text):

- Exam (70%
- Exercises (30%)
- Each part must be individually approved of

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
One internal and one external examiner

Re-sit examination:
For the exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Examination support:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke

Teaching Materials:
Literature and study materials: Handouts of the material covered in the lectures will be distributed.

- R.O.Duda, P.E. Hart, and D.G. Storck: Pattern Classification. 2nd ed., Wiley, 2001
- Sergios Theodoridis, Konstantinos Koutroumbas. “Pattern Recognition”, third edition. Academic Press.

Replacement course for:
IMT4611

Additional information:
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.

Publish:
Yes

IMT4571 IT Governance - 2011-2012

Course code:
IMT4571

Course name:
IT Governance

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Autumn

Duration (additional text):
Second half of autumn semester

Language of instruction:
English

Expected learning outcomes:
Calder and Watkins define IT Governance as ”the framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organization’s information systems support and enable the achievement of its strategies and objectives”. IT Governance is of crucial importance for organizations owing to the need to best safeguard critical information and, through the increasing requirements from national and international regulations. Central to IT Governance in Europe is the ISO 27001 / ISO 27002 standard.

This course provides an overview of IT Governance and the basic concepts of the ISO 27001 / ISO 27002 standard.

The candidate should after attending the course

- fully understand the main principles of IT Governance.
- fully understand the basic concepts of the ISO 27001 / ISO 27002 standard
- master the principles for designing & implementing an ISO 27001 ISMS
- be fully aware of the difference between security technology and the management of secure systems
- have a thorough understanding of security management as a continuous improvement process.
- possess awareness of security certification schemes (BS7799, ISO 15408, …)

Topic(s):

- Reasons for IT Governance: Compliance, liability, stability
- Organizing information security
- Information security policy and scope
- The risk assessment and statement of applicability
- Identification of risks related to external parties
- Asset management
- Human resources security
- Physical and environmental security
- Equipment security
- Communications and operations management
- Controls against malicious software (malware) and back-ups
- Network security management and media handling
- Exchanges of information
- Electronic commerce services
- E-mail and internet use
- Access control
- Network access control
- Operating system access control
- Application access control and teleworking
- Systems acquisition, development and maintenance
- Cryptographic controls
- Security in development and support processes
- Monitoring and information security incident management
- Business continuity management
- Compliance
- Principles of auditing

Teaching Methods:
Other

Teaching Methods (additional text):
Lectures, exercises and projects.

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):

- 1-2 Multiple Choice Tests (weight: 20%)
- 1-2 Group Assignments (weight: 30%)
- Digital Final Exam, 2 hours (weight: 50%)
- All three parts are mandatory and must be passed!

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Evaluated by the lecturer

Re-sit examination:
For the final exam: Ordinary re-sit examnination.

Tillatte hjelpemidler:

Coursework Requirements:
None.

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Forskningssjef Åsmund Skomedal

Teaching Materials:
Literature:

Alan Calder & Steve Watkins. IT Governance : IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002. Fourth Edition. Kogan Page. 2008.

Anderson, Ross (1999) Why cryptosystems fail, University Computer Laboratory,University of Cambridge, Cambridge, UK, http://www.cl.cam.ac.uk/~rja14/wcf.html.

Publish:
Yes

IMT4022 Digital Forensics II - 2011-2012

Course code:
IMT4022

Course name:
Digital Forensics II

Course level:
Master (syklus 2)

ECTS Credits:
10

Duration:
Vår

Language of instruction:
English

Prerequisite(s):

- BSc level basics in operating systems, data communication and network security
- IMT4012 Digital Forensics I or IMT3551 Digital Forensics or equivalent.

Expected learning outcomes:
The course develops deep understanding in the methodology, technology and application of digital forensics. Students are expected to reach an advanced level of knowledge in the broad spectrum of digital evidence, analysis methods and tools.

The course is oriented towards profound theoretical background, where the students learn contemporary techniques and advanced research topics.

Topic(s):

- Forensics and Incident Response
- Microsoft Windows Host Forensic
- Unix and Linux Host Forensics
- Live Forensics and RAM Analysis
- Network and Cloud Forensics
- Botnet and Malware Analysis
- Mobile and Embedded Device Analysis
- Securing Evidence, Cryptanalysis and Anti-Forensics
- Steganography
- eDiscovery: Fingerprinting, Correlation, and Search

Teaching Methods:
Lectures
Laboratory work

Form(s) of Assessment:
Other

Form(s) of Assessment (additional text):
An overall evaluation based on a 100 point scale, where project work counts up to 50 points and final exam (3 hours) counts up to 50 points (at least 18 at the written exam MUST be obtained). Conversion from 100 point scale to A-F scale according to recommended conversion table. In specific circumstances, the course responsible can slightly adjust the limits in the conversion table to enforce compatibility with the qualitative descriptions on the A-F scale.

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal examiner

Re-sit examination:
For the final exam: Ordinary re-sit examination.

Tillatte hjelpemidler:

Coursework Requirements:
None

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Professor Katrin Franke (katrin.franke@hig.no) /Adjunct Associate Professor André Årnes (andre.arnes@hig.no)

Teaching Materials:
Keith J. Jones, Richard Bejtlich, Curtis W. Rose: Real Digital Forensics: Computer Security and Incident Response. Addison-Wesley, 2005, (0-321-24069-3)

Dan Farmer and Wietse Venema: Forensic Discovery, Addison-Wesley, 2005 (ISBN 0-201-63497-x)

Presentation material and selected academic papers

Additional information:
Knowledge of Linux is an advantage

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

Publish:
Yes

IMT4591 Legal Aspects of Information Security - 2011-2012

Course code:
IMT4591

Course name:
Legal Aspects of Information Security

Course level:
Master (syklus 2)

ECTS Credits:
5

Duration:
Vår

Language of instruction:
Norsk, alternativt engelsk

Expected learning outcomes:
Knowledge

- The candidate possesses advanced knowledge in legal aspects especially relevant for information security. This applies particularly to the legal regulation of matters of importance to safeguarding confidentiality, integrity, access and quality.

Skills

- The candidate is capable of performing critical analysis of various literature sources regarding legal aspects of information security.
- The candidate is capable of carrying out an independent limited research or development project in legal aspects of information security under supervision, following the applicable ethical rules.

General competence

- The candidate is capable of analyzing relevant professional and research ethical problems in legal aspects of information security.
- The candidate is capable of applying his/her knowledge about legal aspects of information security in new fields, in order to accomplish advanced tasks and projects.
- The candidate can work independently and is familiar with legal terminology.

Topic(s):
General requirement according to privacy and information security, especially e-government.

Teaching Methods:
Lectures
Group works
Exercises
Meeting(s)/Seminar(s)

Form(s) of Assessment:
Written exam, 3 hours

Grading Scale:
Alphabetical Scale, A(best) – F (fail)

External/internal examiner:
Internal + external examiner

Re-sit examination:
No re-sit examnination.

Tillatte hjelpemidler:

Academic responsibility:
Faculty of Computer Science and Media Technology

Course responsibility:
Timelærer Lise Nilsen

Teaching Materials:
See information in Fronter.

Additional information:
There are two differens student groups in the course.

Publish:
Yes