

NordSecMob

Master's Programme in Security and Mobile Computing

- Mobile computing
- Information security
- Computer science
- Double degree
- Scholarships



Coordinator:

Aalto University (Finland)

Partners:

KTH Royal Institute of Technology – KTH (Sweden)

The Norwegian University of Science and
Technology – NTNU (Norway)

The Technical University of Denmark – DTU (Denmark)

University of Tartu – UT (Estonia)

<http://nordsecmob.tkk.fi>

NordSecMob

<http://nordsecmob.tkk.fi>

NordSecMob - Master's Programme in Security and Mobile Computing

NordSecMob - Erasmus Mundus Programme

NordSecMob - Master's Programme in Security and Mobile Computing is one of the European top-quality Masters Programmes selected by the European Commission Erasmus Mundus Programme. Erasmus Mundus is a co-operation and mobility programme, promoting the European Union (EU) as a centre of excellence in higher education around the world and supporting European top-quality Masters Courses. Erasmus Mundus programmes offer culturally enriching higher education opportunities for both European and non-European students. Students from any country can apply to the NordSecMob - Master's Programme in Security and Mobile Computing. Both European and non-European students have the opportunity to apply for the Erasmus Mundus Scholarships. The NordSecMob-programme gives the students a chance to experience the cultures of two northern European countries.

The five universities jointly offering this programme are Aalto University, Finland (Aalto); KTH Royal Institute of Technology, Sweden (KTH), The Norwegian University of Science and Technology, Norway (NTNU), The Technical University of Denmark (DTU) and University of Tartu, Estonia (UT).

Read more: http://ec.europa.eu/education/programmes/mundus/index_en.html

EU Member States (27): Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Sweden, United Kingdom, Spain **EEA States:** Iceland, Norway, Liechtenstein, **EU Candidate countries (presently):** Croatia, former Yugoslav Republic of Macedonia, Iceland, Turkey

"The most valuable experiences in the NordSecMob programme were the knowledge gained, the relocation and getting to know different cultures and very important - the people from the program that I met. The friendships and contacts we've made is something that makes an impact on an individual and is something we'll always carry with us."

NordSecMob student, graduated 2008



Objectives of the NordSecMob-programme

NordSecMob — Master's programme in Security and Mobile Computing allows students with strong computer science backgrounds to specialize in mobile computing technologies. The mobile computing and communications industry provides the user with tools that make data and communication available anywhere and at any time. This programme is about the technologies and techniques needed to allow the user to benefit from these pervasive technologies in a secure and safe manner. New mobile devices extend mobile communication with powerful computing, enabling new services in new markets.

Future internet and mobile computing technologies

The NordSecMob curriculum covers a broad range of engineering and theoretical topics giving the students a solid understanding of fundamental mobile computing technologies and an opportunity to choose their own focus areas. The technical basis of the programme consists of the current and future

Internet and wireless network technologies, mobile devices, and general software engineering skills. The subject areas include key architectural and management issues in future online services such as mobility, quality of service, security, usability, charging and business models, as well as tools for safe software development and formal and mathematical validation and analysis.

Information security

Throughout the programme, special attention is paid to the information security, which is a critical requirement when developing and deploying services on public networks. Students are required to both study current technologies and emergent topics in the research community and to apply this knowledge in practical implementation projects. Beyond technology, the curriculum is designed to develop the students' problem-solving skills, ability to find solutions and opportunities from the latest scientific research, and independent initiative and technical leadership in a project-oriented workplace.



Sebastián Domancich (Argentina)

I applied to the NordSecMob programme with two objectives: Firstly, I wanted to enhance my professional skills in the fascinating area of security in mobile computers. Considering that this area has grown a lot in the last years, this specific Master's programme could provide me the tools to be better qualified in my professional career. Secondly, I wanted to grow as a person. I had never been anywhere outside my home continent, South America, and I felt a strong desire to get to know people from different cultures, learn and interact with them, as well as living in a unique area like the Scandinavian countries. I am happy to say that thanks to the invaluable help of many people, I could accomplish both objectives. From the academic point of view, I had the chance to study at Aalto and KTH. I could dramatically improve my skills in security and mobile technologies by making use of state of the art technology available in the Scandinavian universities. From the personal point of view, this experience allowed me to grow as a person. I still remember the first day when I was getting introduced to some of my new NordSecMob classmates: They were from all over the world, with fascinating stories behind, so different in some ways, but with many things in common with me. Nowadays, I am proud to say that these great people are my close friends. We spent many unforgettable moments together and I believe that we somehow became ambassadors of our own country. The Scandinavian culture is unique and is also a highlight of my experience: being based on trust, tidiness and respect, there is always someone willing to help whenever a problem arises. I can conclude that this lifetime experience is highly recommendable for any IT professional planning to work (or already working) in the security area, who wishes to study and live in a truly international atmosphere and enjoy the fascinating Scandinavian culture.

Practical and theoretical skills

The programme gives students a broad knowledge of different aspects of modern data communications architectures and their evolution. The students will gain both practical engineering skills and theoretical insight, including capability to follow and apply the latest scientific research. The graduates will be able to design and develop their own solutions for the mobile Internet. The aim of the programme is to grow graduate engineers who will take responsibility for creating the next generations of products and services for the European ICT industry.

International career: industry or academic world

The NordSecMob graduates are equipped to be employed internationally in a wide range of industrial and academic jobs, including expert roles, R&D, research and management positions. The programme also gives a solid basis to continue academic career towards the doctoral level.

Be Mobile – Join NordSecMob!

Apply for the NordSecMob programme and help shape the future! Not only will you gain in-depth knowledge and practical know-how of the mobile revolution, but at the same time you will have a chance to experience the cultures of two northern European countries. ■



Double Degree

NordSecMob – Two Universities – Double Degree

NordSecMob is a two-year Master of Science degree Programme (120 ECTS credits). During the programme, the students will study at two of the five Nordic partner universities: Aalto University in Finland, KTH Royal Institute of Technology (KTH) in Sweden, the Norwegian University of Science and Technology (NTNU), the Technical University of Denmark (DTU) and the University of Tartu (UT) in Estonia. The NordSecMob joint curriculum has been developed to take advantage of the strengths and research specialization of each member university. Student mobility is implemented by dividing the time of each student between two of the universities, a

'home' university and a 'host' university. The student takes courses focusing on advanced topics in a selected area of specialization, which are:

- **Aalto: Technical Information Security and Network services**
- **KTH: Communications Systems Design**
- **NTNU: Information Security**
- **DTU: Reliable Software Systems**
- **UT: Mathematical Foundations of Cryptography**

The 120 ECTS credits will be divided into two blocks: 1-2 semesters of teaching (30-60 ECTS credits) will be provided by the home university and 1-2 semesters of teaching (30-60 ECTS credits) by the host university. The programme includes three semesters of courses followed by a fourth research semester (Master's thesis, 30 ECTS).

During the first autumn term studies are taken at one of the three home universities: Aalto, KTH or NTNU. Students with the specialization option "Reliable Software Systems" transfer from home university to DTU for the first spring and second autumn semester. Also students with the specialization "Mathematical Foundations of Cryptography"

move from the home university to UT for the first spring and second autumn semester. Students with other specialization tracks relocate after first year studies to other host universities (Aalto, NTNU, KTH) for the second autumn semester.

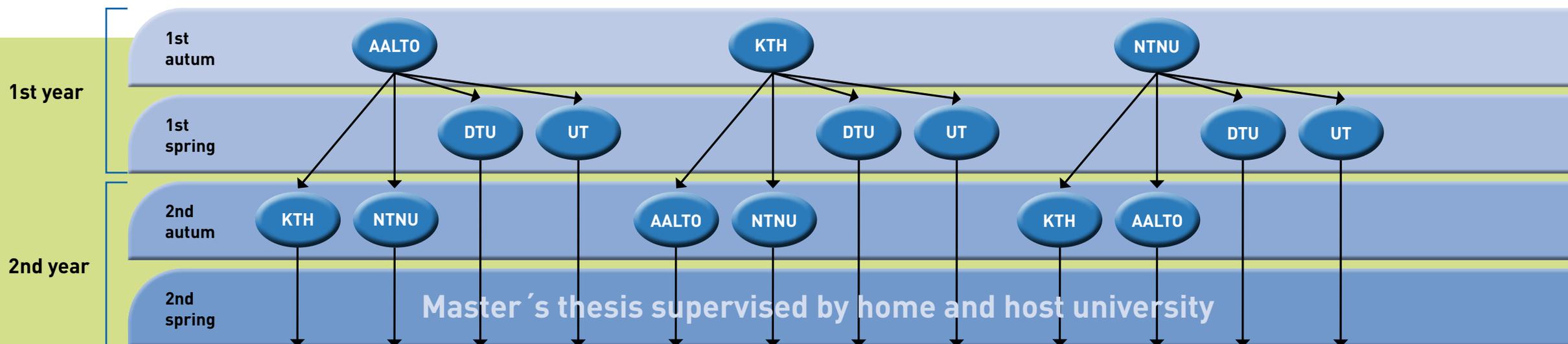
The fourth semester is dedicated for thesis writing under supervision of both home and host university. The thesis is usually written in research projects either at the university or in industry. After completing the two-year programme, successful students will be awarded two officially recognized M.Sc. degrees: one from each university where they studied. ■

Degrees Awarded

This two-year NordSecMob-programme leads to two officially recognized M.Sc. degrees (120 ECTS) issued by the home and host university (double degree).

Institution	Title of Degree Awarded
Aalto University	Master of Science (Technology), Security and Mobile Computing
KTH	Master of Science (two years)
NTNU	Master of Science in Security and Mobile Computing
DTU	Master of Science in Engineering, Security and Mobile Computing
UT	Master of Science in Engineering (Computer Science)

Joint Study Programme



Content of NordSecMob-programme

Focus of each semester and learning outcomes

AALTO: Technical Information Security and Network Services

FIRST AUTUMN: FOCUS Foundational knowledge and skills for becoming an expert in security and mobile computing

LEARNING OUTCOME In the first semester, students build a body of skills and knowledge that puts them on a fast track to becoming specialists in communications security and mobile computing. They will know the fundamental principles and concepts of information security and cryptography, and have an up-to-date picture of the latest wireless and mobile networking and service delivery technologies. They will have applied this knowledge in hands-on exercises and will have developed advanced software for distributed systems. Through tailored methodology and English language courses, the students will also have systems engineering skills: modeling, simulations, data analysis, as well as writing and presentation skills, which are needed for the rest of the Master's studies.

FIRST SPRING: FOCUS Advanced courses in mobile computing, security, and services including interactive courses, project works and research assignments.

LEARNING OUTCOME Building on the foundations laid in the autumn, the students learn advanced topics in areas of their choice and continue to improve their research and hands-on skills. They will have in-depth understanding of some specialized topics in mobility, network services development and communications security. The topics include advanced services in distributed systems, network application frameworks, network services business models and value chains, embedded systems development, and latest research in internetworking technologies. The students are able to apply their knowledge and present technical information in written and spoken form.

SECOND AUTUMN: FOCUS Advanced courses in mobile computing, security, and services including interactive courses, project works and research assignments

LEARNING OUTCOME Taking into account their personal specialization, the students learn advanced topics in areas of their choice and continue to improve their research and hands-on skills. They will have an up-to-date picture of the latest wireless and mobile networking and service delivery technologies, and in-depth understanding of some specialist topics in mobility, network services development and communications security. The topics include next generation wireless networks, new protocols in computer networks, and latest research in communications security. The students are able to apply their knowledge and present technical information in written and spoken form.

KTH: Communications Systems Design

FIRST AUTUMN: FOCUS Communication security, including advanced topics in networking and security, theory and laboratory exercises.

LEARNING OUTCOME During the first semester, students will develop in-depth knowledge in the fundamental areas of communication systems and networks. Students will be able to critically evaluate current and new protocol designs for internetworking, routing, and network security. They will also learn to describe functionality and design principles of network devices and systems, and will be able to design, set up and operate TCP/IP networks and services. Students will also understand the fundamental components and techniques for building secure networks, be able to critically evaluate new and existing protocols for authentication, authorization, and integrity, describe network security threats and attacks, and be able to evaluate and how systems are designed to protect against such attacks. During this semester, students will also gain theoretical insight and practical skills required to plan, implement, analyze and report a scientific experiment in the area of communication systems.

FIRST SPRING: FOCUS Advanced operator-related topics, including network management, technology management, mobile services and networks.

LEARNING OUTCOME The spring semester offers rich opportunities for students to specialize in the area of secure and mobile computing, by selecting a mix of elective courses. Through elective courses, the students will be able to:

- Understand, compare and contrast architectures for mobile and wireless networks, and different types of mobility.
- Design, implement and test applications for small, mobile devices.
- Describe and discuss methods and systems for switched wireless and wired networks.
- Design, configure and manage local area networks (wireless and Ethernet).
- Apply queuing theory methodology for solving practical dimensioning problems for communication systems and networks.

SECOND AUTUMN: FOCUS Problem-oriented, project-driven learning in teams addressing real-life problems in the communication systems area, with external project owners optionally in parallel with business management/creation.

LEARNING OUTCOME The autumn semester for second-year students is devoted to courses that are problem-oriented in nature. In these courses, through work that is self-directed and project-based, students learn to apply skills earned from the first year in order to address real-world problems that come from external project owners. The students learn to analyze and research a problem area, to plan and perform the work as a project team, and to disseminate the results through presentations and exhibitions. The overall goal is that students should acquire the skills to design, build and operate communication applications, services and networks in innovative ways.

NTNU: Information Security

FIRST AUTUMN: FOCUS Basic networking courses, dependability, performance and simulation, basic cryptography

LEARNING OUTCOME Students will gain basic knowledge in classical cryptography and public key cryptography. They will also learn about fundamental and necessary components, functions and principles needed to build mobile and fixed access and transport networks. Additionally they will learn the principles on software security and how to develop more secure software systems. Via concrete examples taken from computing and communication (ICT) systems the students will gain knowledge how to perform discrete event simulation, and how to use the probability theory and Markov models as tools for modeling, analysis, measurements and dimensioning of computing and communication systems with respect to dependability and performance. They will also gain a clear understanding of the various mechanisms used in the Internet protocols, their strengths and weaknesses, and possible alternatives. They will be able to engineer small networks including configuration of the network nodes and to do performance measurements and Internet traffic analysis.

FIRST SPRING: FOCUS laboratory exercises and topics on technology management and business management/creation.

LEARNING OUTCOME The students will deepen their knowledge and will get practical skills in information security technologies. Students shall gain knowledge of methodology for engineering distributed real-time systems, a basic knowledge of ASN.1, CCS, UML, MSC and SDL, and will be able to specify and simulate systems using these languages and corresponding tools. The students will get the ability to design and manage systems, based on information and communication technologies (ICT), to meet availability, reliability and safety requirements. Furthermore, they will get a firm conceptual insight into important dependability aspects of hardware, software and networks as well as knowledge for management of network resources and services in communication networks. (i.e. installation, deployment, adaptation, operation and removal/de-installation).

SECOND AUTUMN: FOCUS Advanced topics in networking and security with a minor thesis on a specialization topic, security management

LEARNING OUTCOME The students will gain knowledge of, and best practice skills for information security technology and methods in distributed systems providing services for mobile users and users of wireless networks. They will learn how to acquire specialized knowledge in a specific area of information security by applying scientific methods for gaining knowledge of principles, methods, protocols, algorithms and contemporary tools for securing information in distributed systems and telecommunication networks. The students will also learn how to work independently with a project, present a project plan with milestones, report partial results on a regular basis, and write a project report in accordance with accepted standards. Students will get a specialized knowledge about problems and solutions relevant for the information security area.



DTU: Reliable Software Systems

FIRST SPRING AND SECOND AUTUMN: FOCUS Safe and Secure IT-Systems: - methods, tools and techniques for design, implementation, and validation of safe and secure IT-systems, - covering Network Technology (privacy and intrusion detection) as well as Language Based Technology (program analysis, operational semantics, process calculi, and software validation).

LEARNING OUTCOME Students work on specialized aspects of security and mobility, and deepen their knowledge of both theoretical foundations and practical approaches. They enhance their skills of how to model and analyze systems, and learn how to critically judge both existing techniques as well as new ones. Students get the ability to engineer and manage robust and safe systems using these techniques, and are enabled to analyze system requirements, and to argue why a system fulfills these. Furthermore, they gain deep understanding of how a mobile application operates in a network system, and how this influences the overall system.

LEARNING OUTCOME The students gain knowledge of theoretical foundations of modeling and analyzing security and robustness properties of information systems. Students acquire specialized skills in security and mobility, learn how to analyze a given problem and to select the right approach. The problems come from fundamental areas for security of mobile information systems, guaranteeing a broad understanding of the problem facets. Often, a combination of theoretical foundations and practical solutions is required for solving the problems. The students learn how to reach a goal as a part of a group, how to organize a group in order to do so, and how to communicate project work and results in form of reports or articles.

UT: Mathematical Foundations of Cryptography

FIRST SPRING AND SECOND AUTUMN: FOCUS Number-theoretic and complexity-theoretic foundations of cryptographic primitives and protocols - their construction and working principles, meaning and derivation of security. The elective courses allow a deeper study of related mathematical subjects, or possible application areas of security in computer science and IT.

LEARNING OUTCOME Through the courses given in UT, students will comprehend the mathematical and complexity-theoretical foundations of secret- and public-key cryptography, as well as the meaning of security and analysis methods for cryptographic protocols. Students acquire knowledge of the foundations of complexity theory, the construction, working and attack principles of most important contemporary and historic cryptographic algorithms and protocols, different security goals of protocols and primitives and relationships between them, the principles of reducing the security of one construction to the security of another one. The graduates will be able to recall that knowledge in a mathematically rigorous manner. They will also be able to recognize whether an argument provides a proof that a system satisfies some security property.

LEARNING OUTCOME The main learning outcome of the courses offered in UT is the ability to analyze the security of systems, construct secure systems and to be precise in the justification of one's choices and findings. This outcome is supported by the ability of the graduates to perform security reductions at the various levels of detail and abstraction, the comprehension of different security properties and ways of achieving them, the ability to make use of cryptographic libraries in constructing standards-compliant systems, the ability to perform searches of scientific literature pertaining to a specific topic and to report one's findings.

Second spring: thesis (30 ects)

LEARNING OUTCOME For the last semester, the most research oriented component of the programme is thesis writing (30 ECTS). The thesis is jointly supervised by home and host university professors. With jointly supervised thesis, the student is expected to acquire following skills:

- analyze and define the scope of a given problem in the area of security and mobile computing;
- identify and evaluate the applicable tools and approaches, and to perform a qualified selection of suitable tools and approaches;
- identify shortcomings of the tools and approaches chosen, and if necessary develop them further;
- evaluate the achieved solution, and to compare it with the original goal and other approaches;
- reflect on, evaluate, and critically assess one's own and others' scientific results;
- report on the problem, the problem's background, the work performed, the achieved solution and its evaluation, arguing for the decisions taken, in a coherent way following academic and scientific standards.

Consortium partners

The consortium is made up of renowned research and educational institutions in Europe and top-ranking universities of technology in the Nordic countries.

Aalto University

The Aalto University is the oldest and premier research university in Finland (formerly Helsinki University of Technology TKK) and a pioneer in the field of technology in the country. It received university status in 1908. The campus is located in Otaniemi in Espoo, neighbor city of the capital Helsinki. The responsible unit for NordSecMob-teaching activities is the Department of Computer Science and Engineering. This department employs 15 professors, 100 other teachers and researchers with doctoral degrees. The key academics involved in NordSecMob-programme are Professor **Antti Ylä-Jääski** and Professor **Tuomas Aura**.

The research focus of the NordSecMob-programme at Aalto is on the evolution of the Internet technologies as well as on the design, implementation, and verification of IP-based systems. In addition to the Internet technologies, research addresses mobile networks and specifically the development of applications and services in heterogeneous network environments. Focal areas for both Internet and mobile networks are security, service architectures and subjects related to

service management such as mobility, quality-of-service and charging. Security issues including privacy, trust and identity management are central for this research group.



KTH Royal Institute of Technology – KTH



KTH Royal Institute of Technology (KTH), is responsible for one-third of Sweden's capacity for engineering studies and technical research at postsecondary level. The university has over 12,000 undergraduate students, 1,600 active postgraduate students and a staff of 3,000 people. KTH was founded in 1827. There are four campuses with the main campus in central Stockholm.



The key academics involved in the programme at KTH are Professor **Gerald Maguire**, Professor **Sead Muftic**, Professor **Björn Pehrson**, Associate professor **Peter Sjödin** and Assistant professor **Markus Hidell**.

The ICT school of KTH conducts research on communication systems, including their use, policy and regulation of communication markets, design and implementation of applications, services and network systems. In the area of communication systems design, the main research topics are network architectures and protocols for the future Internet, the integration of IP and optics, as well as architectures for network systems with particular focus on decentralized, modularized approaches to network system design. Security aspects related to distributed service architectures, proxy systems, and secure voice over IP communication are important areas of research. TSLab is a department at the KTH School of ICT in Kista, Stockholm.

The Norwegian University of Science and Technology – NTNU

The Norwegian University of Science and Technology (NTNU) is Norway's primary institution for educating the nation's future engineers and scientists. NTNU's cross-disciplinary research delivers creative innovations that have far-reaching social and economic impact and has a broad academic scope with its main focus on technology and the natural sciences. NTNU is Norway's second largest university. The university has about 20 000 students and 4800 staff. NTNU is located in Trondheim, on the western coast of Norway.

The Department of Telematics ITEM is responsible for the teaching of the courses

in the NordSecMob-programme at NTNU. The key academics involved in the NordSecMob programme at NTNU are Professor **Danilo Gligoroski**, Professor **Svein Johan Knapskog**, Professor **Rolv Bræk** and Professor **Peter Herrmann**.

The Department of Telematics focuses its information security research on two main topics: Security as a pivotal ingredient of Quantitative Quality of Service and cryptographic protocols. Modelling, design, analysis and evaluation of information security for ICT systems, services and protocols have in the past most frequently been performed by using

qualitative principles, methods and measures. However, in the present transition into an end user environment dominated by ubiquitous computing power and service realization, the information security research needs to be focused on the quantitative aspects of description and negotiation of perceived QoS. Cryptographic Protocols can be considered as distributed algorithms that employ cryptographic functions for securing distributed computerized communication systems, their goals being to restrict, establish and pre-

serve the security properties of information. A specific long-standing inquiry in the field of crypto-protocols is that of defining and constructing information privacy, for instance in digital cash and e-voting schemes. Digital Tracks is another research activity which addresses both privacy and forensic concerns.

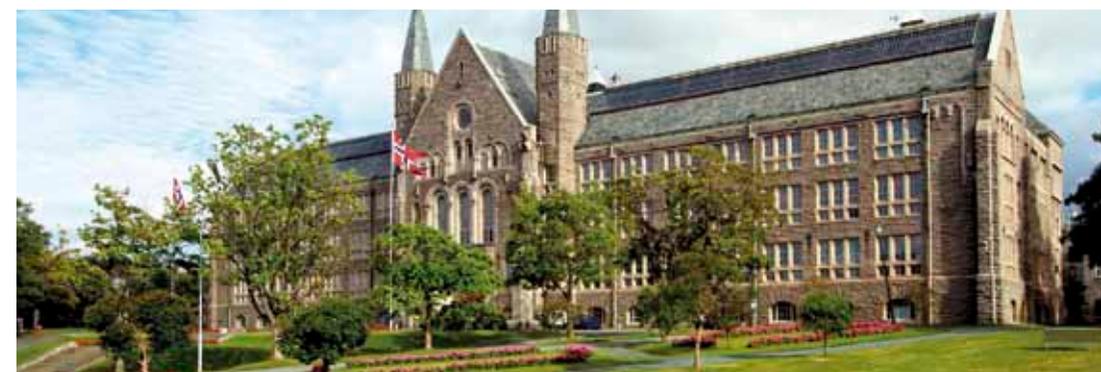


Photo: Mentz Indergaard

The Technical University of Denmark – DTU



The Technical University of Denmark (DTU) is Denmark's leading centre for engineering education and research. DTU currently has about 7000 BSc, MSc and PhD students and 1500 scientific personnel. DTU campus is in Kongens Lyngby, the Copenhagen Metropolitan area. The Department of Informatics and Mathematical Modelling (DTU Informatics) carries out teaching and research within computer science and information processing. The department comprises 9 sections covering various research areas within these fields.

The key academics in NordSecMob-programme at DTU are Professor **Flemming Nielson**, Professor **Hanne Riis Nielson**, Associate professor **Flemming Stassen**, Associate professor **Christian W Probst** and Associate professor **Christian D. Jensen**.

In the DTU NordSecMob-programme there are two main research components. The first line of research deals with software security and focuses on techniques that can be used to validate designs of systems for the absence of security flaws and to develop systems that can be relied upon to adhere to given security policies. To be specific, research on communication protocols using static analysis, originally developed in the EU-project DEGAS, has successfully used to validate a number of voting and single-sign on protocols; research on

access control and information flow, including the Decentralised Label Model, gives concrete techniques for constructing software systems where code is guaranteed to satisfy given confidentiality, integrity or authenticity properties. The second line of research deals with system security and network security. One focus is on how to construct systems that are likely to give users privacy and anonymity; another focus is the study of intrusion detection systems and how they can best be configured to protect the user.



University of Tartu – UT

University of Tartu, founded in 1632, is the largest and most significant higher education institution, and the only classical university in Estonia. The university has an enrollment of 18000 students, and employs about 3500 staff, among them 180 professors in 9 faculties. The unit responsible for the execution of NordSecMob programme, Institute of Computer Science in the Faculty of Mathematics and Computer Science traces its history back to 1993, but the history of computer science in Estonia starts with the arrival of the first electronic computer in Tartu in 1959. The



Estonian research activities in information security and cryptology started in mid-90s, in response to the needs of the newly independent country. Initially, the activities took place in Cybernetica AS, but soon afterwards, and by the same people, teaching of cryptology and information security courses started in University of Tartu, Faculty of Mathematics. The close connections between computer science and mathematics in University of Tartu have also shaped the cryptology-related activities ever since.

The key academic personnel involved in the NordSecMob activities at UT are Professor **Peeter Laud**, Professor **Ahto Buldas** and Researcher **Sven Laur**.

The main NordSecMob-related research areas in Tartu University are data security and cryptography. The interests of the working group reach from practical security analysis to foundations of cryptographic primitives. The main research topics are the following: security models based on attack trees, economics of security, privacy preserving data mining, formal proof systems for cryptographic protocols and properties of hash functions and applications of hash functions in digital time-stamping. ■



NordSecMob

Associated members

The NordSecMob-programme is strongly integrated into the scientific and socio-economic community via the contacts and networks of the key academics, who have also a long-term professional background in industry, too. We have collaboration for example with the following companies and organizations:

Companies

Nokia Corp <http://www.nokia.com>

Nokia Siemens Networks <http://www.nokiasiemensnetworks.com/>

OY LM ERICSSON AB (Finland and Sweden) <http://www.ericsson.com/>

Elisa Corp (Finland) <http://www.elisa.com/en/>

Cybernetica AS (Estonia) <http://www.cyber.ee/cms-en>

There Corp (Finland) <http://therecorporation.com/>

Research institutes in Finland, Sweden and France:

Helsinki Institute for Information Technology (HIIT, Finland) <http://www.hiit.fi/>

Eurecom (France) <http://www.eurecom.fr/>

Swedish Institute of Computer Science (Sweden) <http://www.sics.se/>

Collaboration with non-European higher education institution:

Tsinghua University – MobiLab (China) <http://www.tsinghua.edu.cn/eng>

Collaboration with other organizations

NordSec-conference <http://nordsecmob.tkk.fi/associated.html>

NordSecMob-programme is built on existing research co-operation between the consortium organizations and NordSec-conference is an important link between our programme and experts in this field. Since 1996, the NordSec workshops have brought together computer security researchers and practitioners from the Nordic countries, Northern Europe, and elsewhere. The workshop is focused on applied computer security and is intended to encourage interchange and cooperation between research and industry. See <http://www.ce.chalmers.se/research/conference/nordsec/contents.html>

With changing hot topics around security and mobile computing, this conference hosts talks by leading representatives from industry, academia and the government sector, as well as a panel and a press conference. This conference offers an excellent opportunity for students for networking and gaining new information and knowledge in the area of their studies. ■

NordSecMob

Admission Requirements

The NordSecMob-programme is targeted for top-quality students of all nationalities. Admission to the programme is granted on a competitive basis.

University Background

Successful applicants should hold a bachelor's degree from a university fulfilling the following requirements:

- The university must be an official and recognized part of the national education system.
- The university has to be found on a official list or in an international handbook that is completed by some international organization (e.g. UNESCO)

Student Background

Admission criteria to the programme is a high quality Bachelor's degree encompassing a minimum of 180 ECTS credits in Engineering (Computer Science or Information technology) or equivalent studies i.e. a degree consisting of at least three years of full-time studies. The applicants should have solid knowledge of mathematics (discrete mathematics), programming skills, data structures and algorithms, computer architecture and basics of computer networks. In addition, basic knowledge of the following subject areas will be an advantage: databases and database management, principles of theoretical computer science, logic in computer science, software engineering, operating systems, concurrent programming.

Language Requirements

The language of instruction in the NordSecMob-programme is English. The applicants must have an excellent command of English and they must present an official language test report. The acceptable tests are TOEFL, IELTS, Cambridge Certificate in Advanced English (CAE) or Cambridge Certificate of Proficiency in English (CPE).

TOEFL

TOEFL minimum scores are:

- 580 / writing 4,0 (paper-based test)
- 237 / writing 4,0 (computer-based test)
- 92 / writing 22 (internet-based test)

IELTS

- IELTS minimum score is 6,5 / writing 5,5

Cambridge Certificate in Advanced English (CAE) or Cambridge Certificate of Proficiency in English (CPE)

- grade B or A

The language test requirement (TOEFL, IELTS, CAE, CPE) is waived for those students who have obtained a university degree (minimum 3 years of full-time higher education studies) taught in English with physical presence in one of the following countries: USA, Canada, Australia or New Zealand or in EU/EEA countries. The language test requirement is also waived for EU/EEA citizens from partner universities (Erasmus/TIME/Cluster/NordTek/Nordic 5 Tech-partners) of the NordSecMob-consortium universities. A certificate from the partner university stating the student's good level of English will be enough.

For details, check NordSecMob-website.

<http://nordsecmob.tkk.fi>

Application deadline and selection criteria

The annual application deadline is in December-January. Details of required application documents, the exact deadlines and the on-line application form are available on the NordSecMob-website. ■

NordSecMob

Scholarships for Students and Staff

Erasmus Mundus-scholarships

All students can apply for generous EU-funded Erasmus Mundus scholarships.

There are two categories of Erasmus Mundus scholarships:

Category A: (non-EU/EEA nationals): can be awarded to masters students who are not residents nor have carried out their main activity (studies, work, etc.) for more than a total of 12 months over the last five years in EU/EEA countries

Category B: EU/EEA-nationals and other nationalities who have been more than 12 months in Europe for studying or working purposes.

Erasmus Mundus scholarship amounts:

EU scholarship contribution	Category A scholarships	Category B scholarships
Contribution to travel, installation and any other type of costs	8000 € (total in two years)	-
Monthly allowance	1000 € / month (total 24 000 €)	500 € / month (total 12 000 €)
Maximum contribution to the programme fee (including insurance coverage)	16 000 € / two-year programme	maximum of 8000 € / two-year programme
Total	48 000 € for the two years of study	20 000 € for the two years of study

The number of Erasmus Mundus-scholarships is very limited and the scholarships will be allocated only to the most excellent students. Therefore, we also strongly encourage students to look for some other financing possibilities in order to be able to join the programme with their own financial contribution (self-funded students). The NordSecMob-consortium offers a limited number of NordSecMob-consortium scholarships, too.

Erasmus Mundus scholarships for Non-European scholars (visiting academics)

A scholar is an academic and/or professional of outstanding experience who carries out teaching or research assignments and scholarly work in the institutions participating in the NordSecMob-programme. Erasmus Mundus scholarships allow non-European scholars to perform the tasks defined by the consortium for maximum of three months. The amount of scholarship for the visiting scholars is 1200€/week for a maximum duration of 3 months per scholar (total maximum of 14800 Eur). The criteria concerning all scholar positions at NordSecMob-consortium:

The applicants should have a PhD in Computer Science, teaching and research experience in the research areas of the programme. The visiting

scholar is also expected to be mobile during his visit i.e., visit at least two consortium universities (Aalto, KTH, DTU, NTNU, UT) during the stay. The selected scholars are expected to participate in the research activities of the universities and to provide some teaching in their areas of expertise to advanced graduate students and postgraduate students (e.g., seminars, tutoring and/or intensive short courses). For further information see <http://nordsecmob.tkk.fi/scholars.html>

Programme fee

There is no programme fee for EU/EEA-students. The programme fee is charged from any other than EU-member state and EEA-nationals. The programme fee is announced on the NordSecMob-website. ■



Education and Culture DG

ERASMUS MUNDUS



norden

Nordplus



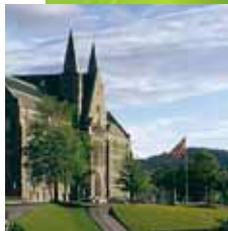
Aalto University

<http://www.aalto.fi>



**KTH Royal Institute
of Technology**

<http://www.kth.se/>



**The Norwegian
University of Science
and Technology**

<http://www.ntnu.no/>



**The Technical
University of Denmark**

<http://www.dtu.dk/>



University of Tartu

<http://www.ut.ee/>

Contact Information

NordSecMob Consortium

Aalto University
street Konemiehentie 2 (P.O. Box 15400)
FI-00076 AALTO (city: Espoo)
Finland

email: nordsecmob@tkk.fi

tel: +358-9-4702 4773

+358-9-4702 6016

fax +358-9-4702 3015

<http://nordsecmob.tkk.fi>

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.