The Norwegian Information Security Laboratory (NISlab) at Gjøvik University College (GUC) is Europe's second largest academic research group in Information Security with a strong focus on high quality publication and national and international cooperation. The laboratory has research activities in all areas of Information Security and offers study programs in information security on Bachelor, Master and PhD level. It collaborates with the Media Technology Laboratory and the Faculty of Engineering and Business Administration at GUC, as well with law enforcements, the Norwegian Army, and companies and universities both nationally and abroad.
GUC has about 2600 students and 290 members of staff from over 26 nationalities. It works hard to be dynamic in educational matters and at the same time close to both students and local activities, and has been awarded a prize for its good working conditions.
GUC is centrally located in Gjøvik, a pleasant town in beautiful countryside along Lake Mjøsa, only about 1½ hour from Oslo International Airport, Norway's main airport. It offers excellent outdoors activities in all seasons, with cross-country tracks "at your door steps" and major alpine facilities accessible in an hour. GUC is working closely with regional businesses and other university colleges in the region to establish a merged university of 12,000 students by 2015.

PhD research position

Adaptive Security, Smart Internet of Things, Adaptive Risk Management, Estimation and Predication

within the ASSET (Adaptive Security for Smart Internet of Things in eHealth) project in Gjovik, Norway

Location:	Gjøvik, Norway
Application deadline:	15.03.2012
Start:	Mid-August 2012
Duration:	3 years.

Gjøvik University College (GUC) is looking for a PhD candidate to work in the ASSET project. The ASSET project is a cooperation between GUC, the **Norwegian Computing Center** (NR) and international partners. The PhD candidate is required to register in GUC's Information Security PhD program. The funding is available for three years in the ASSET project, financed by the research Council of Norway. The project will run from January 2012 until June 2015.

Research in ASSET

Emerging technologies for the Internet of Things (IoT) have the potential to provide many benefits to improve eHealth where the Things include smart phones, sensors, sensor nodes and actuator nodes. The IoTs successful deployment depends on ensuring security and privacy that need to adapt to their processing capabilities and resource use. IoTs are, however, vulnerable to attacks since communications are mostly wireless, unattended things are usually vulnerable to physical attacks, and most IoT components are constrained by energy, communications, and computation capabilities necessary for the implementation of complex security-supporting schemes. Most current security models and mechanisms that address the IoT's problems and allow a system to detect and recover from errors or attacks are hard to change, reuse, and analyze; thus making infrastructures that are inflexible, causing lost investments and damage as result from mechanisms not matching the threats, etc. Therefore, ASSET will build risk-based adaptive security methods and mechanisms that increase security to an appropriate level. The security methods and mechanisms will adapt to the dynamic changing conditions of IoT, including usability, threats, diversity, and heterogeneity. ASSET's case study will lead to the design of adaptive strategies for the dynamic interplay between security and data transmission in a mobile patient monitoring system. In order to achieve this overall goal the project will

- Build models for estimating and predicting risk and benefits using game theory and context awareness for adaptive security in IoT.
- Build security metrics using innovative reasoning techniques for sufficient and credible evidence gathering for validating the effectiveness of adaptation
- Prototype risk based adaptive methods for authentication and access control for IoT and use them in a simulation experiment in two patient monitoring scenarios in Oslo University Hospital.
- Build light-weight self-abilities in smart IoT that will allow them to detect in real-time unknown security and privacy threats, respond to them, and adapt to the environment and changing degree of threats.

The PhD candidate will be expected to define a research topic relating to the ASSET project in conjunction with his or her advisers, and to participate in the project work, including conceptual work, implementation, evaluation, publication and presentations. Possible research topics can, for example, cover these areas:

- Estimation and predication of security and privacy risk and impacts for IoT in eHealth using game theory and context awareness;
- The capturing and inclusion of epistemic uncertainty using e.g. info-gap, p-box or byesian techniqueues in the game theoretic risk model.
- Theories and methods for security measurement and metrics for validating the effectiveness of the adaptation;

The ASSET project has international partners, thus occasional travel to meetings and conferences is required. The project language is English.

The ideal candidate has a master-level background in computer science, computer engineering, mathematics or statistics combined with practical skills in programming, software design, office software and groupware. Experience in the following topics will be an advantage: information security, risk management, privacy enhancing technology, game theory, modeling and simulation

Applicants are expected to have an outstanding academic record, be highly motivated and proactive, have excellent organisation and communication skills, and be eager to disseminate research results through publications and presentations at international conferences and seminars. Fluency in English is a prerequisite.

The application shall include:

- A complete CV;
- Academic records, including grades and an explanation of grades in terms of percentiles.
- A letter of motivation elaborating the reason for seeking a PhD;
- A description (short abstract) of the Master thesis;
- List of scientific applications and articles, if available;
- List of participation in research projects, if available;
- Proof of English skills, if available;
- Other relevant experience, e.g. from a professional career.

For further information, please consult the following web pages, and take contact with the persons listed below:

- The ASSET project:
  http://asset.nr.no/
- Gjøvik University College, Norwegian Information Security Laboratory - NISlab
  http://www.nislab.no
- GUC PhD in Information Security program:
  http://www.hig.no/studietilbud/it/master/phd

The GUC work contract is offered under the condition of a successful acceptance into the GUC PhD program within two months after signing the work contract with GUC.

General information

The positions are remunerated according to salary level 48 in the Norwegian national salary scheme, gross NOK 391 300 per annum (ca. EUR 52000).

Gjøvik University College is an equal opportunity employer and strongly invites female applicants.

For employment conditions, contract details etc. please contact
Jan Kåre Testad, jan.testad@hig.no

For inquiries on the ASSET project and research topics:
Professor Einar Snekkenes, einar.snekkenes@hig.no

All applications must be submitted via the following url:
http://english.hig.no/about/vacancies

We expect this url to be operational by January 30, 2012.