Study/Scholarship Report

For Zühlke Engineering AG

Andreas Grünert

March 25, 2010

1 Motivation

This report is on behalf of Zühlke Engineering to justify their scholarship and give statement of my master studies that it supported. The report is structured in five sections. Section 1 describes the scope of the document and the foregoing events that lead to my scholarship application. Section 2 gives an overview over the chosen university and course; section 3 focuses on the student life and the study development so far. Section 4 states the original aims in terms of research, networking and learning and analyzes how well they were and will be met. Finally an outlook on my prospective moves and aims is given in Section 5.

1.1 Causes

End of 2007 I took the chance to go to Thailand for a three month internship. I was working at a university laboratory focusing on knowledge, information and data management. The work was highly interesting. It was not about doing assistance work for the researchers as assumed beforehand but I was given the task to design and implement a solution to help exchanging and storing the accumulated research knowledge. I got a good view on how the university works. My focus when developing the solution was not just to satisfy the functional requirements but also to guarantee security to the information processed and stored. Information security consists of all the means that guarantee privacy, confidentiality, availability and integrity of information assets. Doing my work I became aware that information security was not yet a big concern within the research group and the university. I know it to be of major importance now and even more so in the future, when more and more of our daily life becomes digital. It became my aim to gain and spread knowledge on information security, their implications to our life and also the connection to politics, law and regulations.

The experience there and my interest in information security let to the decision that I wanted to continue studying after graduating from my bachelor degree in Switzerland. Originally I planned to continue the studies in Thailand, after earning some money in a gap working year. Because of recommendation and own research in where the best courses are offered, I decided to apply for a master course at Royal Holloway, University of London. I gave up the initial idea of doing the master in Thailand because London seems to offer a much better course in the area of information security. Thus the new plan was to go to Thailand after graduating in London, to apply the new skills and knowledge.

Studying in London is expensive, not only because of the cost of living, but also because the study fees are astronomical compared to other countries. Going to London meant to take a financial risk. The risk is even higher since repayment of a loan will be difficult due to low salaries in Thailand. To reduce this risk I applied for the Zühlke scholarship.

In June 2009 I got the acceptance of the university as well as the acceptance for a flat in Goodenough College, a residence college in the centre of London. In July 2009, after presenting my plans to a jury, I was awarded the „Zühlke Ausslandsstipendium“.

Since September 2009 I am living in London and follow my master studies.

2 Royal Holloway and the Information Security Group

The course of my choice was the msc. in information security at the information security group (ISG) at Royal Holloway, University of London. Royal Holloway is a campus university based in Egham, a small town to the west of London. The studies offered at the university are diverse. They are split into three faculties: faculty of arts, faculty of history and social sciences and the faculty of sciences. The ISG is part of the mathematical department in the faculty of sciences.

The group, introduced in 1992, is the oldest research group in information security. Although theory is a major component of the studies and the research, the master course is also focused on the practical and management aspects necessary when working on security in an organisational environment. The master course is offered as one year full time course and in different part time arrangements allowing people currently working in companies to be part. This leads to an interesting mix of about 200 Master students from different backgrounds and allows the exchange of knowledge between practitioners as well as theorists.

The course consists of three parts: A set of core modules on either technical topics (technical pathway) or business related (business pathway) information security, a set of optional modules in a wide range of areas associated to information security and the master project.

2.1 Core Modules

- Security Management
- Introduction to Cryptography and Security Mechanisms
- Network Security
- Computer Security
- Legal and Regulatory Aspects of Electronic Commerce
- Security Technologies

2.2 Compulsory Modules

- Application & Business Security Developments
- Standards and Evaluation Criteria
- Advanced Cryptography
- Database Security
- Computer Crime
- Smart Cards / Token Security & Applications
- Software Security
- Digital Forensics

3 Student Life and Study Development

Although I study in Egham, Surrey, westwards adjacent to London, I chose to live in the centre of the city in the Goodenough College[1], a residence college for international postgraduate students. Living in London and surrounded by many academic people is inspiring. My student life is therefore split between the residence and the university campus where lectures, seminars and other study related activities take place. Trying to benefit maximally from both is the aim behind this. This sometimes though results in having to choose between different interesting extracurricular events.

In the term of study development, my interests in information security lies on the technical, theoretical side, thus I chose to follow the technical pathway of the studies having network security and computer security as technical core modules. Additional core modules were cryptography and security management. Each course was taught by a highly qualified lecturer, with exception for security management: this subject is given by a number of people responsible for security in companies. The optional modules I currently take in the second term are digital forensics, smart cards and advanced cryptography. Digital forensics is concerned about evidence gathering, identification and extraction of

[1] http://www.goodenough.ac.uk/

digital information. In the smart card module the technology, environment and application of smart card systems are analyzed. And lastly, advanced cryptography discusses the mathematics used in cryptographic techniques and algorithms. These modules were adjoined by weekly industrial seminars, tutorial and other activities related to the field of study.

For my master thesis, I decided to do a project in the area of smart cards; in particular I wanted to know how authentication protocols based on zero-knowledge proof of knowledge protocols can be used for dynamic card authentication. This authentication is necessary for smart cards (e.g. ATM cards) to prove not to be a clone. For this purpose today most cards use a traditional approach based on RSA[2] signatures. Zero-knowledge techniques could be more efficient but are not widely deployed. The reason for that is diverse: There are still US-patents blocking inovation in this area, the protocols itself are not trivial to understand and implement and exising standards and management infrastructures are not aware of them. Analyzing the situation and benchmarking the efficiency of such protocols are the main targets. My supervisor for the project is Dr. Keith Mayes, director of the smart card centre at the university.

I enjoy the study, my project and my extracurricular activities. It is the right course to get proficient in information security for further research or for taking responsibilities in a company. The lectures are outstanding in quality. The only negative aspect of the course is the low quality of the facilities such as lecture theatres or labs on the campus. It though does not stop one from learning.

4 Aims, Expectations and Performance

I did not set specific aims concerning the concentration of study before I came to Royal Holloway. Some general non-quantifiable aims were to get a thorough understanding what information security consists of, get a deeper technical knowledge and better understand the management of information. Quantifiable aims are in particular to graduate from the course with distinction and to write an interesting master thesis upon I might do more research in a future position. For the former aim, performance cannot be measured at the time of this writing. The exams deciding on a distinction will be held in May 2010. The latter aim is, to my opinion on its way. Working in the field of efficiency of cryptographic protocols on smart cards and therefore building up knowledge, may allow me to work in the respective area later on. I will work with sole focus on the thesis between June and September 2010.

Secondary aims were to build up a network with people of similar interest and build links between Royal Holloway and my former university, Bern University of applied sciences. Surely I was able to find friends here and people with similar interests, most importantly though the university itself offers all alumni a network that may be used in the future to get important connections – for business or research. Building up links between the universities is not as easy as I thought it may be. But I keep an eye on possible collaborations

Personal aims are always coupled with expectations. In this case the expectations in the quality of lectures, in support, facilities and the organisation. Except for the quality of the campus facilities, all expectations excelled. The course and student organisation was good and helpful for effective learning, the lecturers are highly qualified and pedagogical skilled.

My aims and expectations were well met. I increased my knowledge and understanding in different aspects such as technical, social as well as management and from diverse views. In terms of research outcome, I planned to publish an article for a conference later this year on the topics I currently research for the master project. An article co-authored with the security research group at Bern University of applied sciences was submitted last month and is currently under review. End of March 2010 we should be notified if it got accepted.

5 Outlook

The taught courses are soon ending, next comes the exam term and the master thesis. In the next month until September 2010, I will therefore focus on finishing my studies.

[2] RSA is a public key cryptographic system named after the researchers Ron Rivest, Adi Shamir and Len Adleman

It is already important though to look into the future. What will happen after graduating? As mentioned in Section 1 of this report, I plan to move to Thailand. The idea is to get work or a research position there to spread knowledge on information security and gain more experience for whatever follows afterwards in my life.