DOCTORAL PROGRAMME ON ICS SECURITY AT THE UNIVERSITY OF THE AEGEAN

Sokratis K. Katsikas
Laboratory of Information & Communication Systems Security, Dept. of Information & Communication Systems Engineering, University of the Aegean, Karlovassi GR-83200, Greece
ska@aegean.gr

Abstract: The paper presents the doctoral programme of study on information and communication systems security at the University of the Aegean, in Samos, Greece.

Key words: Doctoral Programme, Information & Communication Systems Security Education

1. INTRODUCTION

The purpose of this paper is to present the doctoral programme of study on information and communication systems security at the University of the Aegean, in Samos, Greece, in order to contribute to the discussion within IFIP WG 11.8 towards the definition of an international doctorate programme in the field.

The doctoral programme of study on information and communication systems security at the University of the Aegean is a research doctorate programme, which has been offered since the initial operation of the Department in 1998 and is still being offered.

2. PROGRAMME AIMS AND OBJECTIVES

The main objectives of the doctoral programme are:

- To give all interested students the opportunity to take advantage of the results of the joint effort of several Universities worldwide to develop a modular - but integrated - doctoral Programme in the areas of Information and Communication Systems Security.
- To further support the establishment of a wide, international network of experts who teach, consult and conduct research in the fields of information and communication systems security, as well as the closely related fields of dependability and safety.
- To support, enhance, stimulate and utilise the mobility of University students, researchers and teaching staff among different European Union Member States.
- To provide interested industrial and governmental institutions and bodies with a unique point of contact and co-operation with several centers of excellence in research on information and communication systems security, with a real European flavour.

3. DURATION, ADMISSION AND DEGREE REQUIREMENTS

The duration of the program, when undertaken as a full-time program varies with several factors, such as, for example, the entrance actual qualifications, the student's actual research capabilities etc.; the duration can vary between a minimum of 3 years and a maximum of 6 years.

For admission to the programme, an M.Sc. in Information Systems, Communications, Informatics, Engineering, Sciences or Business Administration is required. An M.Sc. in Information and Communication Systems Security is highly desirable.

Formally, the sole doctoral degree requirement is the successful defense of the doctoral thesis before the jury. There is no formal requirement for having completed a specific number of course credits, nor for having undertaken any coursework, as in all Greek Universities. However, doctoral students that do not hold an M.Sc. in Information and Communication Systems Security are strongly advised to attend as many M.Sc. courses as possible, during the course of their doctoral study.

4. COURSES

The following courses are offered in the winter semester (in parentheses the subjects covered): *Cryptography I* (Introduction; Mathematical background: Probability theory, Information theory, Complexity theory, Number theory, Algebra, Finite fields; Crypto services; User authentication; Data authentication; Data integrity; Data origin authentication; Non-repudiation of origin; Data confidentiality; Basic cryptographic principles; Cryptography; Symmetric and asymmetric systems; Principles of authentication; One-way functions and hash functions; Message authentication codes; Digital signatures; Crypto protocols; User authentication protocols; Key management protocols), *Network Security I* (The necessity for network security; Attack types; Basic network security concepts; Technologies and services offered by Certification Service Providers and PKI; Case studies; Security architecture in the ISO/OSI model; Threats; Services and mechanisms; The Internet security architecture; Security protocols at the Internet layer; Security protocols at the transport layer; Security protocols at the application layer; Security protocols above the application layer; Applications, Firewalls; Censorship and context-dependent access control technologies; Privacy enhancing technologies: Anonymous Browsing, Anonymous Publishing), *Database Systems Security* (Database systems architecture; Database models; confidentiality and integrity; security services; authorization; access control, auditing; database security examples; security in SQL environments, secure multilayer databases; privacy protection in databases; logical inferencing; security in object-oriented databases; security in distributed databases; security in federated databases; security in data mining systems; Medical database security; case studies: Oracle RDBMS etc.), *Crypto algorithms implementation techniques* (Implementing crypto algorithms in software and in hardware; Secure systems design; Java security and Java crypto extensions; Security token technology: Smartcards; Case studies). The following courses are offered in the spring semester: *Cryptography II* (Modular arithmetic; discrete logarithms; prime factoring; P, NP, NP-complete problems; probabilistic polynomial time algorithms; next-bit checks, random cryptography; zero-knowledge protocols; obvious transfer. LFSRs: shift registers, m-sequences, linear equivalence, Berlekamp-Masey; Shannon Theory: Entropy, probability, random ciphers, perfect secrecy; Combinatorics: authentication, thresholds schemes, secret sharing schemes, key distribution; Design criteria: Non-linearity, correlation properties, Boolean functions, discrete Fourier transform; crypto algorithms evaluation; identification, authentication and digital signature schemes), *Network Security II* (Generalised application layer security systems; Distributed

authentication systems: Kerberos, SESAME; Network management security: Network management services in OSI networks and in the Internet model: SNMP, CMIP/TMN, JMX; Mobile code security models: Java, ActiveX, SafeTcl; Intrusion Detection Systems; Digital Rights Protection Technologies; Middleware security models; Financial transaction systems security: Electronic Cash Systems, Electronic Checks, Electronic Credit Card Payments, Micropayment Systems; Electronic voting systems security; Wireless network security: Wireless LAN and 802.11, wireless Ad hoc Networks and Bluetooth, wireless Handheld Devices and PDA, Smartphone; Crypto protocols and formal analysis and design methods: The AAPA2 tool), *Standardisation – Certification – Evaluation* (Access control: ISO/IEC 10181-3, ISO/IEC 10181-n; Security mechanism standards: Encipherment algorithm register (ISO/IEC 9979), block cipher mode (ISO/IEC 10116), cryptographic check function (ISO/IEC 9797), digital signatures (ISO/IEC 9796), hash functions (ISO/IEC 10118), key management (ISO/IEC 11770), security management (ISO 17799); Evaluation criteria: TCSEC (Orange Book), ITSEC, US Federal Criteria, Common Criteria, Canadian CTSPEC; Security evaluation: ITSEM, industry standards: ECMA, Posix; Quality standards: ISO 9000; National and international standards in banking: key management, hash functions, digital signatures, data integrity mechanisms, PIN management etc.), *Social and ethical issues* (Computers and society: IT as a revolution and an evolution, the future with IT, knowledge and machines: AI, VR, user interfaces, usability and IT, issues related to the new work environment, change management; privacy and security oriented systems design; ethical issues: wotk monitoring, surveillance, social control, creativity issues, work transformations, quality of work and life, the new capitalism model; new technologies and economic development; using IT in politics and in elections; deontology and ethical codes; case studies: ACM, BCS, IEEE, IFIP; ethical issues related to hacking; IT security social impact; scientific, research and professional liability; Computer crime; Computing Forensics).

5. THESIS

The doctoral thesis must reflect original research work, undertaken by the candidate him/herself, that promotes scientific knowledge in the field. There is no formal requirement on the actual size of the thesis itself, but the average size is approximately 200 A4, single spaced, 12 font pages.

6. POTENTIAL FUNDING SOURCES

The best potential source of funding for qualified students is the European Union, through its numerous funded research framework programmes. Some possibilities also may arise within national programs of funded research. Potential non-academic partners include the European industry as well as the national industry. Finally, some scholarships are offered, but these are limited to Greek nationals only.

7. CONCLUSIONS

The doctoral programme of study on information and communication systems security at the University of the Aegean, in Samos, Greece has been presented, with a view towards contributing to the discussion for the definition of a, international similar programme in the field. The Department would be very keen to cooperate with institutions of a similar standing towards the definition, as well as the implementation of the international doctorate. To this end, some possible areas of curriculum specialization that the Department could contribute to a possible international partnership include Security management, network security, legal – social – ethical issues.