Cryptography and Information Security
MAP-I Curricular Unit – 2011/2012

Summary

This document describes a Ph.D. level course, corresponding to a Curriculum Unit credited with 5 ECTS. It is offered in the MAP-I doctoral program jointly by the CCTC/Departamento de Informática at Universidade do Minho, IT/Departamento de Ciência de Computadores at Faculdade de Ciências da Universidade do Porto, and IEETA/Departamento de Electrónica, Telecomunicações e Informática at Universidade de Aveiro.

The objective of this course is to introduce students to the theoretical principles that underly current research in modern cryptography. The focus is on a rigorous *approach to information security, emphasizing the central role of definitions and formal proofs of security, resorting to simple and precisely stated assumptions.*

Coordinator: Manuel Barbosa (HASLab/CCTC/DI-UM)

Context

This document describes a Ph.D. level course, corresponding to a Curriculum Unit credited with 5 ECTS. It is offered in the MAP-I doctoral program jointly by the CCTC/Departamento de Informática at Universidade do Minho, IT/Departamento de Ciência de Computadores at Faculdade de Ciências da Universidade do Porto, and IEETA/Departamento de Electrónica, Telecomunicações e Informática at Universidade de Aveiro.

This proposal aims to instantiate the Curricular Unit in Theory and Foundations of Computer Science or, alternatively, the Curricular Unit in Technologies.

This proposal is, for the most part, a re-edition of the CU with the same designation that was offered in the 2010/2011 edition of the MAP-i doctoral program.

Course Description

The objective of this course is to introduce students to the theoretical principles that underly current research in modern cryptography and information security. The focus is on a *rigorous* approach to information security, emphasizing the central role of definitions and formal proofs of security, resorting to simple and precisely stated assumptions.

Prerequisites

Students are expected to have an undergraduate background in Computer Science. In particular, familiarity with basic discrete mathematics and the concept of a mathematical proof is important, as well as background knowledge on algorithms. Prior knowledge of cryptography and complexity theory are desirable, but not necessary. Students who have not previously taken courses in these topics may have to work harder and do more outside reading in order to keep up.

Textbooks and Other Required Materials

The course is at a similar level and covers overlapping material with the following advanced modules taught at leading academic institutions in the information security area, namely:

- Modern Cryptography, Mihir Bellare, UCSD.
- Introduction to Cryptography, Yevgeniy Dodis, NYU.
- Introduction to Cryptography, D. Boneh, Stanford.

Recommended reading materials include:

- Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell, Chapman & Hall/CRC.
- Foundations of cryptography Vol. 1 and 2, Oded Goldreich, Cambridge University Press.
- Lecture Notes on Cryptography, M. Bellare and S. Goldwasser (available on-line)
- Introduction to Modern Cryptography, Mihir Bellare and Phillip Rogaway (available on-line)
- A Computational Introduction to Number Theory and Algebra, Victor Shoup, Cambridge University Press
- Handbook of Applied Cryptography, A.J. Menezes, P.C. van Ooorschot, and S.A. Vanstone (available on-line)

Course Objective

The course will cover theoretical issues in cryptography with important applications in information security, and students are expected to acquire the following skills:

- Familiarity with scientific challenges in cryptography and information security.

- Ability to extract information from scientific papers in the area.
- Technical writing and presentation skills.
- Comfortability with security proofs and ability to think abstractly about information security problems.

Topics Covered

1. Introduction: Basic Principles of Modern Cryptography, Perfectly-Secret Encryption, One-Time Pad, Limitations of Perfect Secrecy.
2. Symmetric Cryptography: Computationally-Secure Encryption, Stream Ciphers and Multiple Encryptions, Permutations and Block Ciphers, Modes of Operation, Practical Constructions of Pseudorandom Permutations, Message Authentication Codes, MAC Constructions, Cryptographic Hash Functions.
3. Constructions of Pseudorandom Objects: One-Way Functions, Hard-Core Predicates, Pseudorandom Generators, Pseudorandom Functions, Computational Indistinguishability.
4. Number Theory and Cryptographic Hardness Assumptions: Algebraic Background, Factoring Assumption, RSA Assumption, Discrete Logarithm and Diffie-Hellman Assumptions, Introduction to Elliptic Curves, Bilinear Pairings and Related Computational Assumptions.
5. Public-Key Cryptography: Security against Chosen-Plaintext Attacks, Hybrid Encryption, RSA and ElGamal, Security Against Chosen-Ciphertext Attacks, Digital Signatures, RSA Signatures, "Hash-and-Sign" Paradigm, One-Time Signatures, Public-Key Cryptosystems in the Random Oracle Model.
6. Identity Based Cryptography: Concept, Identity Based Signatures and Encryption, Concrete Schemes in The Random Oracle Model, Chosen Ciphertext Secure Public-Key Encryption from Identity Based Encryption.
7. Zero Knowledge Proofs, Proofs of Knowledge and Non-Interactive Zero Knowledge Proofs.
8. Asymmetric key management. Public key certificates. Hardware cryptographic tokens. Public key infrastructures, principles and practice.

Expected Number of Students

Expected number of students is 15.

Class Schedule

Lectures, discussions and student presentations. The course corresponds to 42 lecturing hours, during one complete semester. Tentative class schedule: 2 hour lecture + 1 hour tutorial per week, for 14 weeks.

Student Evaluation Criteria

- 50% Final exam
- 40% Written assignments and paper presentations
- 10% Class participation

A total final score under 50% means the student fails the course and must re-take a final exam which will then represent 100% of the final score.

Course Staff

Teaching workload will be evenly distributed among the following instructors:

- Manuel B. Barbosa (HASLab/CCTC/DI-UM) – Contact person (`mbb@di.uminho.pt`)
- José M. Valença (HASLab/CCTC/DI-UM)
- Luis Antunes (IT/DCC-FCUP)
- André Zúquete (IEETA/DETI-UA)

Curriculum Vitæ

FULL NAME: André Ventura da Cruz Marnôto Zúquete

BIRTHDAY: 6/Nov/1965

NATIONALITY: Portuguese

PROFESSIONAL ADDRESS:

IEETA, Campus Universitário de Santiago

3810-193 Aveiro, Portugal

PHONE: +351 234 370504

FAX: +351 234 370545

E-MAIL: andre.zuquete@ua.pt

URL: http://www.ieeta.pt/~avz

Actual Professional Activities

Professor Auxiliar at University of Aveiro, Dep. of Electronics, Telecommunications e Informatics (DETI)

Researcher at IEETA (Instituto de Engenharia Electrónica e Telemática de Aveiro), member of Laboratory of Information Systems and Telematics.

Colaborator of IT (Institute of Telecommunications).

Research Interests:

- Security algorithms, protocols and applications
- Security in distributed systems
- Security in mobile systems
- Mobile communications
- Electronic Voting Systems
- Operating Systems
- Distributed Systems
- Mobility

Education

Technical University of Lisbon, Lisbon, Portugal

- Undergraduate studies in Electrical and Computer Engineering (Oct 1983 - Jul 1988)
- MSc in Electrical and Computer Engineering (Oct 1988 - Oct 1992)
- PhD in Informatics and Computer Engineering (Oct 1994 – Apr 2001)

Curso Geral de Segurança de Matérias Classificadas, ANS, MDN, 1994

Professional Experience

Researcher at INESC in Lisboa (nowadays INESC-ID Lisboa):

- Since Apr 1985 until Jan 2003 in the Distributed Systems Group (GSD).
- From 1985 until 1988 colaborated with Prof. Isabel Cacho Teixeira in the design and implementation of simulation models for CMOS digital circuits.

Researcher at IEETA in Aveiro (ex-INESC Aveiro):

- Since Feb 2003 in the Laboratory of Information Systems and Telematics.

Collaborator of IT in Aveiro:

- Since Dec 2003.

Lecturer of IST/UTL, initially in the Dep. of Electrical and Computer Engineering (DEEC) and latter in the Dep. of Informatics Engineering (DEI), from Jan 1990 until Feb 2003:

- 1990 – 1992: Assistente estagiário
- 1992 – 2001: Assistente
- 2001-2003: Professor Auxiliar
- Courses:
  - Operating Systems (LEEC 89/90)
  - Computer Systems Architecture (LEIC 89/90, 00/01, 01/02)
  - Software Engineering (LEEC 90/91, 91/92, 92/93, 93/94, 94/95, 98/99, 99/00)
  - Distributed Systems (LEIC 97/98, 98/99, 99/00, 00/01)
  - Security Algorithms and Applications (LEIC + MEIC 01/02, 02/03)

Lecturer of UA, in the Dep. of Electronics, Telecommunications and Informatics (DETI), since Feb 2003

- 2003 - : Professor Auxiliar
- Courses:
  - Computer Systems Architecture (06/07)
  - Programming in C (02/03, LEGI 03/04, 04/05, 05/06)
  - Operating Systems (LECT+LEET 03/04)
  - Distributed Systems (LECT, 06/07)
  - Network Security (LECT, 04/05, 05/06, 06/07)
  - Network and Communication Systems Security (LEET, 04/05, 05/06, 06/07)
  - Mobile Computing (LECT, 06/07)
  - Communication and Security (Communication and Multimedia CFE, 03/04, 04/05, 05/06)
  - Advanced Topics in Information Security (MAP-I 07-08)

Consulting on Security of Informatic Systems:

1. Banco Espírito Santo (BES)
   Security evaluation of a novel multi-interface home banking authentication procedure
2. Link
   Development of and RSA-based single-sign on service on top of HTTP cookies

3. UMIC (Mission Unit for Science and Investigation):
   Auditing of the computer systems used in the pilot electronic voting experience in the European Parliament elections at Jun 13, 2004.

Other activities:

- Vice-president of the IST Informatics Center (CIIST) from Jun to Dec, 2002, being responsible for the systems and networks.

Organization of Conferences:

1. *2ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2006)*, Universidade de Aveiro, Aveiro, Portugal, Oct 10-11, 2006.

Program Chair/Co-chair

1. *3rd International Symposium on Information Security (IS'08)*. Monterrey, Mexico. Nov 2008

Member of the Technical Program Committee:

1. *NATO Information Systems Technology Symposium on Real Time Intrusion Detection*, Estoril, Portugal, May 27-28, 2002.
2. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2005)*, Florianópolis, Brasil, Sep 26-30, 2005.
3. *1ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2005)*, Universidade da Beira Interior, Covilhã, Portugal, Nov 7-8, 2005.
4. *International Conference on Security and Cryptography (SECRYPT 2006)*, Setúbal, Portugal, Aug 2006.
5. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2006)*, Santos, SP, Brasil, Aug 28-Sep 1, 2006.
6. *2ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2006)*, Universidade de Aveiro, Aveiro, Portugal, Oct 10-11, 2006.
7. *First International Workshop on Information Security (IS'06)*, Montpellier, France, Oct 29 - Nov 3, 2006.
8. *21st International Conference on Information Networking (ICOIN 2007)*, Estoril, Portugal, Jan 23-25, 2007.
9. *International Conference on Security and Cryptography (SECRYPT 2007)*, Barcelona, Spain, Jul 28-31, 2007.
10. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2007)*.
11. *2nd International Symposium on Information Security (IS'07)*, Vilamoura, Portugal, Nov 2007
12. *International Conference on Security and Cryptography (SECRYPT 2008)* , Porto, Portugal, Jul 2008
13. *Simpósio Brasileiro em Segurança de Sistemas Computacionais (SBSeg 2008)*. Gramado, Brasil, Sep 2008

Conference Reviewer:

1. *The 5th Workshop on Parallel and Distributed Scientific and Engineering Computing (PDSEC04 Workshop)*, Santa Fe, New Mexico, USA, Apr 26-30, 2004
2. *Dependable Computing and Communications Symposium, The International Conference on Dependable Systems and Networks (DCC-DSN 2004)*, Florence, Italy, Jun 28-Jul 1, 2004

3. *IEEE Wireless Communications & Networking Conference (WCNC 2005)*, New Orleans, LA, USA, Mar 13-17, 2005.
4. *5th Conference on Telecomunications (ConfTele 2005)*, Tomar, Portugal, Apr 6-7, 2005.
5. *IEEE Wireless Communications & Networking Conference (WCNC 2006)*, Las Vegas, NV, USA, Apr 3-6, 2006.
6. *2nd EuroNGI Conference on Next Generation Internet Design and Engineering (NGI 2006)*, Valencia, Spain, Apr 3-5, 2006.
7. *3rd EURO-NGI Conference on Next Generation Internet Networks (NGI 2007) – Design and Engineering for Heterogeneity*, Trondheim, Norway, May 21-23, 2007.
8. *12th IEEE Symposium on Computers and Communications (ISCC'07)*, Aveiro, Portugal, Jul 2007
9. *Mosharaka International Conference on Communication Systems and Circuits (M-ICCS'07).*
10. *6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'08)*. Berlin, Germany, May 2008

Journal Reviewer:

1. *Computer Standards & Interfaces*, Elsevier, 2002.
2. *Transactions on Dependable and Secure Computing*, Oct 2004.
3. *IEEE Communications Magazine*, Jul 2006.

Supervised Undergraduation (BSc) projects (only at UA):

1. *"Authentication in Distributed System"*, Inês Oliveira, Rui Costa, 2003-04.
2. *"Remote Services for PDAs using Wireless Networks"*, João Limas, Bruno Pereira, 2003-04.
3. *"Indoor location system using Bluetooth"*, Luís Amaral, Flávio Henriques, 2004-05.
4. *"PDA-based Application for Supporting the Management of the UA Campus Computational Infrastructure"*, André Augusto, Miguel Fernandes, 2004-05
5. *"Traffic Shaping for Internet Access"*, Tiago Domingues, Hugo Silva, 2004-05
6. *"Security and Confidentiality in Telematic Biomedical Applications"*, Victor Simões, Alexandre Albuquerque, 2004-05
7. *"Bio Check-Up Point"*, Miguel Bairos, Bruno Santos, 2005-06
8. *"Personal Module for Electronic Voting"*, Pedro Martins, Jorge Pontes, 2005-06
9. *"Internet e-Voting using IP Multicast"*, Lamanary Pina, Veridiano Silva, 2005-06
10. *"Implementation of Certification Authority"*, Christophe Pires, 2005-06
11. *"Traffic Shaping for Internet Access"*, Rui Simões, Marcos Ferreira, 2005-06
12. *"Biometric Authentication Through Brain Activity"*, Bruno Quintela, 2006-07
13. *"Electronic Voting in a Secure Interactive Terminal"*, Miguel Romão, 2006-07 (winner of the ITProjects contest of ENEI 2007 National Forum of Informatics Students)

Supervised Bolonha-style Master Thesis:

1. *"Biometric Authentication Through Brain Activity"*, Bruno Quintela, 2007-08 (ongoing)
2. *"Hacking the Electronic Passaport"*, João Nicolau Silva, 2007-08 (ongoing)
3. *"Security and Mobility in 802.11 Structured Networks"*, Rodolphe Marques, 2007-08 (ongoing)
4. *"Secure Name Service for TCP/IP"*, Sérgio Freire, 2007-08 (ongoing)
5. *"RTS-sec: Privacy and Security in Health Telematic Networks"*, Marco Alexandre Martins, 2007-08 (ongoing)

Supervised Master Thesis:

1. *"A fault tolerant voting system for the Internet"*, Rui Filipe Lopes Joaquim, Feb 2005.

2. *"Authentication in the RTS e-Health system"*, Helder Gomes, Sep 2007.

Technical Supervision of Master Thesis:

1. *"Support for Unusual Participations in Electronic Voting"*, Charlott Eliasson, Mar 2006.

Ongoing Master Thesis:

1. *"An Anonymization framework for an e-Voting System"*, Carlos Filipe Marques Almeida, initiated in 2006.

Ongoing PhD Thesis:

1. *"Secure Management of Local Area Networks"*, Hugo Rafael de Almeida e Marques, initiated in Feb 2004, co-supervised by Prof. Rui Valadas).
2. *"Secure Architectures and Trust Networks in Electronic Government"*, Fábio José Reis Luís Marques, initiated in Jun 2007, co-supervised by Prof. Gonçalo Paiva Dias).
3. *"Cellular Frustration and Applications to Immunology and Computer Security"*, Patrícia Silva, initiated in Jun 2007, co-supervised by Prof. Fernão Vístulo de Abreu).

Master Thesis Examinator:

14. *"A Hybrid Approach to Intrusion Detection"*, Nuno Miguel Navarro Teixeira da Cruz Neves, Faculdade de Ciências, Universidade de Lisboa, Apr 2002.
15. *"The PKI of the Ministry of Justice" ("Infra-estrutura de chave pública do Ministério da Justiça")*, Cláudia Isabel Polainas Mateus Carvalho, Faculdade de Ciências, Universidade de Lisboa, Apr 2003.
16. *"Security in IEEE 802.11 Wireless LANs" ("Segurança em Redes de Comunicações de Área Local não-Cabladas IEEE 802.11")*, Cristiano Martins Pereira, Universidade de Aveiro, Oct 2005.
17. *"Analysis of a Commercial e-Voting System" ("Análise de um sistema de votação electrónica comercial"*), Filipe José Silva de Campos, Universidade do Minho, Jul 2006.
18. *"Electronic Voting" ("Votação electrónicd"*), Ricardo André Fernandes Costa, Faculdade de Engenharia, Universidade do Porto, Jul 2006.
19. *"Security of Business Applications with WebServices" ("Segurança de aplicações empresariais em arquitecturas de serviços"*), Miguel Filipe Leitão Pardal, IST, UTL, Sep 2006.
20. *"Support for Authentication Requirements in Workflows" ("Suporte de Requisitos de Autenticação em Fluxos de Trabalho"*), Ricardo Filipe Gonçalves Martinho, IST, UTL, Dec 2006.
21. *"Network Behaviour Analyser" ("Analisador Comportamental de Rede")*, João Manuel Alexandre Cardana, Faculdade de Ciências, Universidade de Lisboa, Dec 2006.
22. *"Central Management of Distributed Firewalls in Heterogeneous Environment" ("Gestão Centralizada de Firewalls Distribuídas em Ambientes Heterogéneos")*, Pedro Filipe Brito Duarte Martins Monteiro, Faculdade de engenharia, Universidade do Porto, Abril de 2007.

PhD Thesis Examinator:

1. *"Towards Adjustable Lightweight Authentication for Network Access Control"*, Henric Johnson, School of Engineering, Blekinge Institute of Technology, Karlskrona, Sweden, Dec 2005.

Invited talks:

1. Seminário sobre "Prevenção e criminalidade das redes informáticas", IST, Mar 28-29, 1995 *"Correio Electrónico Seguro"*

2. Workshop Internet, IST, 1996
   "Segurança na Web"
3. V Semana Informática do IST, Mar 16-20, 1998
   "A Banca Electrónica, Bancos On-line, Transacções Seguras: Técnicas criptográficas básicas para a sua implantação"
4. VI Semana Informática do IST, Mar 15-19, 1999
   "Certificados Digitais"
5. Seminário organizado pelo Gabinete Nacional de Segurança sobre "*A actividade informática, as ameaças à segurança e a protecção dos sistemas de informação*", Instituto de Defesa Nacional, Dec 16-17, 1999
   "Mecanismos de segurança na Internet"
6. Curso sobre "*Segurança Informática: Internet e Intranet*", Instituto de Informática, Centro de Formação, May 10-11, 2001
   "*Criptografia*" e "*Comunicação segura*"
7. IX Semana Informática do IST, Mar 11-15, 2002
   "Mecanismos de Segurança para Sistemas Distribuídos"
8. Seminário organizado pelo Gabinete Nacional de Segurança sobre "*A evolução tecnológica na protecção da informação em sistemas distribuídos*", Instituto de Defesa Nacional, Oct 14-15, 2002
   "Protocolos de segurança - o acesso à rede: IPsec e VPNs"
9. III Jornadas de Engenharia Electrotécnica e de Computadores do IST, Mar 31-Apr 4, 2003
   "Segurança em WLAN: Problemas do IEEE 802.11b"
10. *Wireless Communication Symposium (WCS) 2004, Lisboa, Jan 20-22, 2004*
    "Segurança em Redes Sem Fios: Problemas do IEEE 802.11"
11. Workshop de Segurança: *"Writing Secure Code"*, Instituto Superior Técnico - Tagus Park, Apr 14, 2004
    "Buffer overflows: sua exploração e técnicas de defesa"
12. *"A segurança como valor acrescentado no acesso às redes de telecomunicações"*, Seminário da PT Inovação, Aveiro, May 5, 2004
13. Moderação/posicionamento do painel *"Segurança: como está a sua política de segurança?"*, Conferências Fórum TI, 3º Fórum anual de tecnologias de informação e comunicações, Centro de Congressos de Lisboa, Jun 1, 2004
14. Networkers Forum 2004, C. Cultural de Belém, Oct 18-22, 2004
    "WiFi Security: Mobility and ubiquitous authentication"
15. *"Segurança em Redes Móveis"*, Seminários do IST-TagusPark, Centro de Congressos do Núcleo Central do TagusPark, Mar 21-22, 2005
    " A flexible, large-scale authentication policy for WLAN roaming users using IPSec and public key certification"
16. *"Segurança Wi-Fi: Mobilidade e Autenticação"*, 1º Encontro Nacional de Estudantes de Informática (ENEI 2005), Coimbra, Apr 23-25, 2005

17. II Conferência sobre Redes de Computadores e Segurança Informática, Universidade da Beira Interior, Covilhã, May 24-25, 2005
    "Um gerador de números aleatórios eficiente e de alta qualidade para sistemas multitarefa"
18. *"Arquitectura de Autenticação baseada em Certificados para a Rede Telemática da Saúde"*, 1º Workshop do Mestrado em Informática Médica, Faculdade de Medicina da Universidade do Porto / Faculdade de Ciências da Universidade do Porto, Hospital de S. João, Porto
    "*O actual modelo de protecção a dados pessoais e clínicos: demasiado permissivo ou demasiado restritivo"*
19. *"Identity Management"*, Computer World, Hotel Vila Rica, Lisboa, 10 de Maio de 2007
    "Identidade Digital: Passaporte Electrónico Português (PEP)"

Post-Graduation Courses:

1. "*Network Security*" module of POSI (Post-Graduation in Information Systems), 1st, 2nd e 3rd Editions (1999/00, 2000/01 e 2001/2002)
2. "*Introduction to Network Security*" module of CEPEI (Informatics Engineering Professional Specialization Course) on Informatics Security, Mar 2002
3. "*Protocolos e Mecanismos de Segurança*" module of CEPEI (Informatics Engineering Professional Specialization Course) on Informatics Security, Apr 2002
4. Practical Course on TCP/IP Network Security, UNAVE (University of Aveiro Association for Professional Graduation and Research), Sep, 2004.
5. "*Security in IP Networking*", Euro-NGI Network of Excellence European Joint PhD Course, INT Evry, France, 26-30 June 2006.
6. *"Advanced Topics in Network Security"*, EuroNGI PhD Course, NYNU, Trondheim, Norway, 11-15 June 2007.

Research Projects Member

1988 – 1992: COMANDOS (Esprit I n. 367, Esprit II n. 2071)
1990 – 1992: HARNESS (Esprit II n. 5279)
1991 – 1992: Bull-DCE, between Bull and INESC, for integrating DCE (Distributed Computing Environment) in the system developed in INESC within COMANDOS e HARNESS
1993 – 1994: Joint project by SMD and INESC for porting a UNIX server-based office automation system to the novel Windows NT 3.5
1994 – 1996: ORCHESTRA (Organisational Change, Evolution, Structuring and Awareness, Esprit n. 8749)
1996 - 1998: OSIRIS (FCT/Praxis XXI - 2/2.1/TIT/1624/95)
1999 – 2001: Electronic Democracy (FCT/POSI/SRI/34392/99)
2004 - 2005: EuroNGI Network of Excellence: Design and Engineering of the Next Generation Internet (WP.JRA.6.3: Creation of Trust by Advanced Security Concepts)
2004 – 2005: SaNTA Security (European Space Agency (ESA), Contract N. 15333/01/NL/ND)
2005 - : E-Voting - A new Architectural Framework for Handling Risk in E-Voting Systems (FCT/POSI/EIA/57038/2004)

2006 - 2007: EuroFGI Network of Excellence: Design and Engineering of the Future Generation Internet (WP.JRA.6.3: Creation of Trust by Advanced Security Concepts)

2008 - : SWIFT (Secure Widespread Identities for Federated Telecommunications), FP7-ICT-2007-4 STREP

2008 - : EuroNF Network of Excellence: Design and Engineering of the Network of the Future

Most Relevant Publications

Books

1. *Segurança em Redes Informáticas*
   André Zúquete
   FCA, ISBN 972-722-399-0.
   Jan 2006.
2. *Segurança em Redes Informáticas (2ª Edição)*
   André Zúquete
   FCA, ISBN 978-972-722-565-1.
   Jan 2008.

Journal Articles

1. *Distribution and Persistence in the IK Platform: Overview and Evaluation*
   Pedro Sousa, Manuel Sequeira, André Zúquete, Paulo Ferreira, Cristina Lopes, Paulo Guedes e José Alves Marques.
   Fall 1993,*Usenix Computing Systems,* 6(4).
2. *Orthogonal Persistence in a Heterogeneous Distributed Object-Oriented Environment*
   Pedro Sousa, André Zúquete, Nuno Neves and José Alves Marques.
   The Computer Journal 37(6), 1994.
3. *Transparent Authentication and Confidentiality for Stream Sockets*
   André Zúquete and Paulo Guedes.
   IEEE Micro 16(3), Jun 1996.
4. *REVS - A Robust Electronic Voting System*
   Rui Joaquim, André Zúquete and Paulo Ferreira.
   IADIS International Journal of WWW/Internet.
   1(2), Dec 2003.
5. *An Efficient High Quality Random Number Generator for Multi-Programmed Systems*
   André Zúquete
   Journal of Computer Security.
   13(2), 2005.
6. *An electronic voting system supporting vote weights*
   Charlott Eliasson and André Zúquete
   Journal of Internet Research, 16(5), 2006.

Conference papers

1. *Transparent Authentication and Confidentiality for Datagram Sockets*
   André Zúquete and Paulo Guedes.
   ERSADS '97 - 2nd European Research Seminar on Advances in Distributed Systems.
   Mar 1997, Zinal, Switzerland.
2. *Efficient Stream Cipher with Variable Internal State*
   André Zúquete e Paulo Guedes.
   SAC '97 - 4th Annual Workshop on Selected Areas in Cryptography.
   Aug 11-12, 1997, Carleton University, Ottawa, Ontario, Canada.
3. *Efficient Error-Propagating Block Chaining*
   André Zúquete e Paulo Guedes.
   6th IMA Conference on Cryptography and Coding, LNCS 1355.
   Dec 17-19, 1997, Royal Agricultural College, Cirencester, UK.
4. *Security Policy Consistency*
   Carlos Ribeiro, André Zúquete, Paulo Ferreira e Paulo Guedes.
   First Workshop on Rule-Based Constraint Reasoning and Programming,
   First International Conference on Computational Logic (CL 2000).
   Jul 24-28, 2000, Imperial College, London, UK.
5. *SEFS: Security Module for Extensible File System Architectures*
   Luís Ferreira, André Zúquete, e Paulo Ferreira.
   Information Security Solutions Europe (ISSE 2000),
   Sep 27-29, 2000, Barcelona, Spain.
6. *SPL: An access control language for security policies with complex constraints*
   Carlos Ribeiro, André Zúquete, Paulo Ferreira e Paulo Guedes.
   Network and Distributed System Security Symposium (NDSS 2001).
   Feb 8-9, 2001, Catamaran Resort Hotel, San Diego, California, USA.
7. *Enforcing Obligation with Security Monitors*
   Carlos Ribeiro, André Zúquete, Paulo Ferreira and Paulo Guedes.
   3rd International Conference on Information and Communications Security (ICICS 2001),
   LNCS 2229.
   Nov 13-16, 2001, Xian, China.
8. *Improving the functionality of SYN cookies*
   André Zúquete.
   6th IFIP Communications and Multimedia Security Conference (CMS 2002).
   Sep 26-27, 2002, Portoroz, Slovenia.
9. REVS - A Robust Electronic Voting System
   Rui Joaquim, André Zúquete and Paulo Ferreira.
   IADIS International Conference e-Society 2003.
   Jun 3-6, 2003, Lisboa, Portugal.
10. *BERSERK: A Simple and Flexible Access Control Solution for Service-Oriented Architectures*
    Gonçalo Luiz, André Zúquete and António Rito da Silva.
    IADIS International Conference Applied Computing 2004.
    Mar 23-26, 2004, Lisboa, Portugal.
11. *Internet Voting: Improving Resistance to Malicious Servers*
    Ricardo Lebre, Rui Joaquim, André Zúquete and Paulo Ferreira.
    IADIS International Conference Applied Computing 2004.

Mar 23-26, 2004, Lisboa, Portugal.

12. *A roaming Authentication Solution for Wifi using IPSec VPNs with client certificates*
    Carlos Ribeiro, Fernando Silva and André Zúquete.
    TERENA Networking Conference.
    Rhodes, Greece, Jun 7-10, 2004.
13. *StackFences: a run-time approach for detecting stack overflows*
    André Zúquete
    1st International Conference on E-business and Telecommunication Networks (ICETE 2004).
    Setúbal, Portugal, Aug 25-28, 2004.
14. *A flexible, large-scale authentication policy for WLAN roaming users using IPSec and public key certification*
    André Zúquete and Carlos Ribeiro
    7ª Conferência sobre Redes de Computadores (CRC'2004).
    Leiria, Portugal, Oct 7-8, 2004.
15. *Satellite Network Transport Architecture (SaNTA)*
    E. Kristiansen (ESA), A. Nunes (Skysoft Portugal), J. Brázio (IT) and A. Zúquete (IT/IEETA)
    23st AIAI International Communications Satellite Systems Conference (ICSSC 2005).
    Rome, Italy, Sep 25-28, 2005.
16. *A Security Architecture for a Satellite Network Transport Architecture*
    A. Zúquete (IT/IEETA) and Ana Simões (Skysoft Portugal)
    1ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2005).
    Universidade da Beira Interior, Covilhã, Portugal, Nov 7-8, 2005.
17. *An Electronic Voting System Supporting Vote Weights*
    Charlott Eliasson and André Zúquete
    The Fourth International Workshop on Security In Information Systems (WOSIS-2006).
    Paphos, Cyprus. May 2006.
18. *A Security Architecture for Protecting LAN Interactions*
    André Zúquete and Hugo Marques
    9th Information Security Conference (ISC 2006), LNCS 4176
    Samos, Greece. Aug 30 - Sep 2, 2006.
19. *Arquitectura de Autenticação baseada em Certificados para a Rede Telemática da Saúde (RTS)*
    Hélder Gomes, André Zúquete and João Paulo Cunha
    2ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2006).
    Aveiro, Portugal, Oct 10-11, 2006.
20. *An Intrusion-Tolerant e-Voting Client System*
    André Zúquete, Carlos Costa and Miguel Romão
    1st Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS 2007).
    Lisboa, Portugal. March 2007.
21. *Flexible 802.11 Security Mechanisms*
    André Zúquete
    Workshop on Socio-Economic Aspects of Next Generation Internet in Relation with its Architecture, Design and Dimensioning (EuroFGI IA.7.6)
    Santander, Cantabria, Spain, June 2007.
22. *Mix Rings Tolerantes a Falhas para Submissão Anónima de Votos*
    Filipe Almeida and André Zúquete
    3ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO'2007)
    Lisboa, Portugal 7-8 Nov, 2007 (**Best Paper Award**)

23. *Authentication Architecture for eHealth Professionals*
    Helder Gomes, João Paulo Cunha and André Zúquete
    2nd International Symposium on Information Security (IS'07)
    Vilamoura, Portugal. November 2007 (LNCS 4804)
24. *Authentication of Professionals in the RTS e-Health System*
    André Zúquete, Helder Gomes and João Paulo Silva Cunha
    International Conference on Health Informatics (HEALTINF 2008), The International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2008)
    Funchal, Portugal. January 28-31, 2008 (**HEALTHINF / BIOSTEC 2008 Best Paper Award**)
25. *Verifiable Anonymous Vote Submission*
    André Zúquete and Filipe Almeida
    23rd Annual ACM Symposium on Applied Computing (SAC'08)
    Fortaleza, Ceará, Brasil. March 16-20, 2008
26. *Improved CSMA/CA Protocol for IEEE 802.11*
    André Zúquete
    4th EURO-NGI Conference on Next Generation Internet Networks
    Kraków, Poland. April 28-30, 2008 (to appear)
27. *A TCP-layer name service for TCP ports*
    Sérgio Freire and André Zúquete
    2008 USENIX Annual Technical Conference
    Boston, MA, USA. June 22-27, 2008 (accepted for publication)
28. *Physical-Layer Encryption with Stream Ciphers*
    André Zúquete and João Barros
    2008 IEEE International Symposium on Information Theory
    Toronto, Ontario, Canada. July 6-11, 2008 (accepted for publication)

Reports

1. *The Orchestra Project: Organisational Change, Evolution, Structuring and Awareness*
   ESPRIT 8749 Final Report, Nuno Guimarães Ed. Sep. 1996.
2. *A Report on Security Concepts for Mobile and Wireless IP Networks, A State of the Art Report on Security for Mobile Users*
   Andreas Gutscher (US), Sebastian Kiesel (US), Christiano Paris (UR), Tønnes Brekne (NTNU), Svein J. Knapsko (NTNU), Warsaw University Aneta Zwierko (WUT), Zbigniew Kotulsk (WUT), Rui Cardoso (IT), Rui Cardoso, André Zúquete Radu Lupu (UPB), Markus Fiedler (BTH), Henric Johnsson (BTH), Wee Hoc Desmond Ng (US), Haitham Cruickshank (US)
   Euro-NGI WP JRA-6.3 Deliverable 6.3.1. Dec 2004.
3. *Assessment of Different Security Concepts for Mobile and Wireless IP Networks*
   Markus Fiedler (BTH), Andreas Gutscher (UST/IKR), Sebastian Kiesel (UST/IKR), HenricJohnson (BTH), Radu Lupu (UPB), Tønnes Brekne (NTNU), André Zúquete (IT)
   Euro-NGI WP JRA-6.3 Deliverable 6.3.2. May 2005
4. *Specification of a key management protocol for mobile networks*
   Tønnes Brekne (NTNU), Svein J. Knapskog (NTNU), Aneta Zwierko (WUT), André Zúquete (IT), Radu Lupu (UPB), Markus Fiedler (BTH), Henric Johnsson (BTH), Wee Hoc Desmond Ng (US), Haitham Cruickshank (US), Euro-NGI WP JRA-6.3 Deliverable 6.3.3. May 2005

Curriculum Vitæ

1 Identificação

José Manuel Esgalhado Valença

Departamento de Informática da Universidade do Minho,
Campus de Gualtar, 4710-057 Braga, Portugal

Tel: +351 253 604460 Fax: +351 253 604471 Mov: +351 938 554582
e-mail: jmvalenca@di.uminho.pt

2 Graus Académicos

1. Agregação, Universidade do Minho, 1985
2. Doctor of Philosophy (D.Phil), Universidade de Oxford, 1977
3. Licenciatura em Engenharia Electrotécnica, Universidade de Lourenço Marques, 1971

3 Carreira Académica

1. Visiting Fellow, Universidade de Oxford, 1998-89
2. Professor Catedrático, Universidade do Minho, 1985-
3. Professor Associado, Universidade do Minho, 1980-1985
4. Research Assistant, Universidade de Oxford, 1977-1979
5. Assistente, Universidade de Lourenço Marques, 1972-1974

4 Funções Académicas

4.1 Na Universidade do Minho

1. Fundador e responsável pelo Grupo de Lógica e Métodos Formais (1988-) e pelo Grupo de Criptografia (1997-) da Universidade do Minho.
2. Director do Departamento de Informática, 1989-1998
3. Director do Centro de Investigação Algoritmi, 1989-1998
4. Fundador e director do Centro de Informática da Universidade do Minho, 1981-1986

4.2 Em outras instituições de índole académica

1. Fundação para a Ciência e Tecnologia (2002-)
   - Membro do Conselho Científica para as Ciências da Engenharia.
   - Promotor e coordenador dos painéis de avaliação das candidaturas a projectos de I&D submetidas à FCT nas áreas de Engenharia Informática e Processamento Computacional da Língua Portuguesa.
   - Membros dos painéis de avaliação das candidaturas a bolsas de doutoramento e pós-doutoramento.
2. Fundação das Universidades Portuguesas / Conselho de Reitores das Universidades Portuguesas
   - Presidente da Comissão de Avaliação Externa dos cursos de Informática - 2001-2002
   - Membro da Comissão de Avaliação Externa dos cursos de Matemática - 2000-2001
   - Membro da Comissão de Avaliação Externa dos cursos de Informática - 1998
3. Comunidade Económica Europeia (Direcção Geral XII)
   - Programa "Training and Mobility for Research - Marie Curie Grants" (1997-1998); avaliador de candidaturas a bolsas de doutoramento e pós-doutoramento.
   - Programa "Training and Mobility for Research - Networks" (1997-1998); avaliador de candidaturas às redes de excelência.
   - Programa "Training and Mobility for Research - Networks" (1997-1998); avaliador e relator externo dos "Middle Term Review Reports".
4. Junta Nacional para Investigação Científica e Tecnológica (1991-1995)
   - Membro das comissões de avaliação de várias chamadas a candidaturas de projectos de I&D e de bolsas de estudo.

5 Extensão Universitária

5.1 Cartão Comum do Cidadão

1. Fev/2001 a Nov/2001; responsável pela equipa de consultadoria que acompanhou o grupo de trabalho criado no âmbito do Ministério da Presidência por despacho do Primeiro Ministro de 8/6/01, para a definição e institucionalização do Cartão Comum do Cidadão.
2. Maio 2002; participação na redacção da Proposta de Lei 112/IX sobre a institucionalização de projectos piloto do Cartão Comum do Cidadão apresentada à Assembleia da República.
3. Apresentação pública na Assembleia da República da Proposta de Lei sobre o Cartão do Cidadão; 26/Maio/2003.
4. Várias comunicações sobre o Cartão do Cidadão em seminários organizados pela Universidade do Minho, Universidade de Coimbra e FCCN.

5.2 Outras actividades de consultadoria ao Estado Português

1. Presdência do Conselho de Ministros/Agência Nacional de Segurança (Dez 2006-): membro do Conselho Técnico de Creditação

2. Ministério dos Negócios Estrangeiros (2005-): representante de Portugal no INFOSEC Working Group, do Galileo Security Board.

3. Ministério da Administração Interna (2004); consultadoria no âmbito da instalação do sistemas de informação do Serviços de Estrangeiros e Fronteiras.

4. Ministério da Presidência (2004) Unidade de Missão para Informação e Conhecimento - consultadoria no âmbito do Projecto Piloto de Voto Electrónico para as Eleições ao Parlamento Europeu em 2004.

5. Ministério da Ciência - Agência de Inovação.
   Avaliação de candidaturas ao Programa de I&D em Consórcio POCTI/POSI; chamadas de Outubro de 2001 e Julho de 2002.

6. Ministério da Justiça (1999). Colaboração na elaboração de legislação sobre certificação digital e valor probatório dos documentos electrónicos.

5.3 Outras instituições

1. Sociedade Inter-bancária de Serviços / MULTICERT (1998-) colaboração em diversos projectos no âmbito da segurança electrónica do sistema financeiro e na certificação digital.

2. IBM Portugal (1990-); membro do júri do Prémio Científico IBM.

6 Livros

1. *Stability of Input-Output Dynamical Systems* (co-autoria com C.J.Harris), 1983, Academic Press

2. *Computação e Linguagem* (co-autoria com J.B.Barros) , 2000, Universidade Aberta

3. *Programação Funcional* (co-autoria com J.B.Barros) , 2000, Universidade Aberta

4. *Curso de Criptografia* (em preparação)

FCT SIG
SISTEMA DE INFORMAÇÃO E GESTÃO
Curriculum vitae

PT EN

Overview | Edit CV

Saturday, 08-45-2010 :: 17:45

Manuel Bernardo Martins Barbosa
End session

Overview

1. Personal data

Full Name
Manuel Bernardo Martins Barbosa

Fiscal ID number
-

ID document
10039088

Birth date
01-05-1973

National of
Portugal

Gender
M

Work address
Departamento de Informática, Escola de Engenharia, Universidade do Minho
Campus de Gualtar
4710-057 Braga
Portugal

Residential Address
Rua Martim Moniz, 199
4100-332 Porto
Portugal

Work Phone
253604458

Residential Phone
-

Email
mbb@di.uminho.pt

Fax
253604471

Cell phone
-

URL
http://www.di.uminho.pt/~mbb/

2. Academic degrees

Year: 1996

Degree: LICENCIATURA

Final grade: 17

Degree granting institution Universidade do Porto

School/College/Campus Faculdade de Engenharia

Thesis title Especialização em Automação, Controlo e Instrumentação

Supervisor:

Co-supervisor:

Scientific area Engenharia Electrotécnica e Informática

Number of curricular years 5

Program title Engenharia Electrotécnica e de Computadores

Year: 1997

Degree: MESTRADO

Final grade: First Class

Degree granting institution University of Newcastle Upon Tyne, United Kingdom

School/College/Campus n/a

Thesis title Development of a CANopen I/O Module Based on the SAB-C167-LM

Supervisor:

Co-supervisor:

Scientific area Electric and Electronic Engineering

Number of curricular years 1

Program title M.Sc. in Automation in Control

Year: 2000

Degree: DOUTORAMENTO

Final grade: N/A

Degree granting institution University of Newcastle Upon Tyne, United Kingdom

School/College/Campus n/a

Thesis title Conformance Testing Issues With Application To the CANopen Protocol

Supervisor:

Co-supervisor:

Scientific area Electric and Electronic Engineering

Number of curricular years 0

Program title Ph.D. in Electrical and Electronic Engineering

Year: 1998

Degree: Masters (Equivalence in Portugal)

Final grade: N/A

Degree granting institution Universidade do Porto

3. Previous activity and current status

Period	Position, professional rank or activity	Institution
September 2008 - March 2009	Visiting Researcher	Departamento de Ciências de Computadores, Faculdade de Ciências da Universidade do Porto. Instituto de Telecomunicações (pólo do Porto).
February 2005 - July 2005	Visiting Researcher	Cryptography and Information Security Group, Dep. Computer Science, Univ. Bristol
2001 - Present day	Professor Auxiliar	Departamento de Informática e Centro de Ciências e Tecnologias da Computação (CCTC) da Universidade do Minho
2000 - 2001	Systems Analyst	Novabase

4. Area of scientific activity

Computer Science (Engenharia Informática/Ciências da Computação).

5. Present research interest

Domain of specialization

Cryptography and Information Security.

Formal methods (model checking and software verification).

Current research interests

In the cryptography and information security area, my research interests are mainly focused on two topics:

(1) Provable Security, or the development of rigorous arguments of security for cryptographic algorithms and protocols, relying on sound theoretical assumptions and realistic formal adversarial models.

(2) Domain-specific languages and tools for cryptographic software. In particular, the development of language features and compilation techniques that bring to the hands of programmers the optimizations and counter-measures usually hand-made by experts.

In the area of formal methods, I am interested in applying software verification and model checking techniques to the validation of security properties (or security policies) in source code implementations of software with high assurance requirements.

Other professional interests/activities

Advanced functional programming, Conformance testing.

6. Experience as scientific adviser

Bárbara Vieira, ``Language Based Security for Cryptographic Software'', Ph.D., initiated in February 2008.

Miguel Marques, ``An Extension to the Eclipse IDE for Cryptographic Software Development'', terminated in December 2008.

Bárbara Vieira, Research Assistant, Pervasive Retail Project, 2007.

Miguel Marques, Research Assistant, Pervasive Retail Project, 2007.

Filipe Campos, ``Análise de Um Protocolo de Votação Electrónica Comercial'', Masters, terminated in July 2006.

7. Participation in R&D projects

Participação em projectos de investigação (coordenador/membro de equipas)

Title: Computer Aided Cryptography Engineering (CACE).
Role: Work Package Leader (Formal Verification and Validation).
Description: European project funded by the 7th Framework Programme with a total of 3.3 million Euro, of which 263000 Euro came to University of Minho. The project duration is 3 years and began in February 2008. Academic partners in the project include the cryptography research groups in the Universities of Aarhus, Bern, Bristol, Bochum, Eindhoven, Haifa and Helsinki and Minho. Industrial partners include Nokia and Sirrix. The goal of the project is an integrated domain-specific tool-box for the development of cryptographic software. More information available from (http://www.cace-project.eu).

Title: Wireless Information Theoretic Security (WITS)
Role: Researcher, Responsible for the Minho Participation.
Description: Project funded by the FCT (PTDC/EIA/71362/2006) with a total of 151000 Euro, of which 40000 Euro came to the University of Minho. The project duration is 3 years and began in January 2008. Project partners include Universidade do Minho, Instituto de Telecomunicações (Pólo do Porto) and LIACC. The project goal is to study secure communication protocols for wireless networks that take advantage of a combination of classical cryptographic techniques and physical layer security techniques.

Title: Reliable and Safe Code Execution for Embedded Systems (RESCUE)
Role: Researcher.
Description: Project funded by the FCT (PTDC/EIA/65862/2006) with a total of 161000 Euro, of which 58000 Euro came to the University of Minho. The project duration is 3 years, and it began in January 2008. Project partners include Universidade do Minho, Instituto de Telecomunicações (Pólo do Porto), LIACC and Instituto Politéctnico do Porto. The goal of the project is to develop formal methods technology for embedded systems software, addressing security and reliability requirements.

8. Prizes and awards received

Year	Name of the prize or award	Promoting entity
1996	Prémio Engenheiro Cristiano Spratley	Venerável Ordem Terceira de Nossa Senhora do Carmo do Porto/Faculdade de Engenharia da Universidade do Porto
1996	Prémio Engenheiro António Almeida	Fundação Engenheiro António Almeida/Faculdade de Engenharia da Universidade do Porto

9. Published works

Teses

"Conformance Testing Issues with Application to the CANopen Protocol"
Degree of Doctor of Phylosophy,
Department of Electrical and Electronic Engineering,
University of Newcastle Upon Tyne,
United Kingdom,
2000

"Development of a CANopen I/O Module Based on the SAB-C167-LM"
Degree of Master of Science,
Department of Electrical and Electronic Engineering,
University of Newcastle Upon Tyne,
United Kingdom,
1997

Livros (autor)

"CANopen Implementation: Application to Industrial Networks"
M. Farsi and M. Barbosa
Computers and Communications Series
Research Studies Press Ltd, 2000
ISBN 0863802478
United Kingdom.

Artigos em revistas de circulação internacional com arbitragem científica

M. Barbosa and P. Farshim
``Strong Knowledge Extractors for Public-Key Encryption Schemes''
ACISP 2010, LNCS 6168, pp. 164--181. Springer, Heidelberg (2010)

M. Barbosa and P. Farshim
``Relations among Notions of Complete Non-Malleability: Indistinguishability Characterisation and Efficient Construction without Random Oracles''
ACISP 2010, LNCS 6168, pp. 145--163. Springer, Heidelberg (2010)

J. Almeida, M. Barbosa, J. Pinto and B. Vieira
``Correctness with respect to reference implementations''
Formal Methods for Industrial and Critical Systems 2009, LNCS 5825, Springer Verlag, 2009.

M. Barbosa, P. Farshim
``Security Analysis of Standard Authentication and Key Agreement Protocols Utilising Timestamps''
Africacrypt 2009, LNCS 5580, Springer Verlag, 2009.

M. Barbosa, A. Moss, D.Page,
``Constructive and Destructive Use of Compilers in Elliptic Curve Cryptography'', Journal of Cryptology 22, Springer-Verlag, 2009.

M. Barbosa, T. Brouard, S. Cauchie, S. de Sousa,
``Secure Biometric Authentication with Improved Accuracy'',
Proceedings of Information Security and Privacy 2008, LNCS 5107, 21--36, Springer-Verlag, 2008.

M. Barbosa, P. Farshim,
``Certificateless Signcryption",
Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security (ASIACCS), 369--372, ACM, 2008.

M. Barbosa, P. Farshim,
``Randomness Reuse: Extensions and Improvements",
Cryptograpy and Coding 2007, Springer-Verlag, LNCS 4887, 261--280, 2007.

M. Barbosa, A. Moss and D. Page,
``Compiler Assisted Elliptic Curve Cryptography",
Information Security 2007, Springer-Verlag, LNCS 4804, 1785--1802, 2007.

M. Barbosa, P. Farshim,
``Secure Cryptographic Workflow in the Standard Model",
INDOCRYPT 2006, Springer-Verlag, LNCS 4329, 379--393, 2006.

M. Barbosa, D. Page,
``On the Automatic Construction of Indistinguishable Operations",
Cryptography and Coding 2005, Springer-Verlag, LNCS 3796, 233--247, 2005.

M. Barbosa, P. Farshim,
``Effcient IdentityBased Key Encapsulation to Multiple Parties",
Cryptography and Coding 2005, Springer-Verlag, LNCS 3796, 428--441, 2005.

M. Barbosa, J.M. Fernandes,
``A Model Based Approach to the Development of Distributed Control Systems",
Proceedings of MOMPES´04 - 1st International Workshop on Model-Based Methodologies for Pervasive and Embedded Software,
TUCS General Publication No 29, Maio 2004,
Turku Centre for Computer Science ISBN 952-12-1359-0, ISSN 1239-1905, 2004.

M. Farsi, K. Ratcliff, M. Barbosa,
``An overview of Controller Area Network",
Computing & Control Engineering Journal,
Institution of Electrical Engineers, Volume 10, Issue 3, 113--120, 1999.

M. Farsi, K. Ratcliff, M. Barbosa,
``An introduction to CANopen",
Computing & Control Engineering Journal,
Institution of Electrical Engineers, Volume 10, Issue 4, 161--168, 1999.

Publicações em actas de encontros científicos

10. Communications in scientific meetings

11. Communications in scientific meetings

Language	Reading	Writing	Conversation
English	Very good	Very good	Very good
French	Good	Basic	Good

Curriculum Vitae

Luís Filipe Coelho Antunes

Address

Faculdade de Ciências da Universidade Porto
Departamento Ciência de Computadores
Rua do Campo Alegre 1021/1055
4169-007 Porto
Portugal
Email: lfa@dcc.fc.up.pt
Homepage:http://www.dcc.fc.up.pt/~lfa

Personal data

Birth date: 04/08/1971
Birth place: Luanda, Angola
Nationality: PORTUGAL

Academic degrees

2002	PhD in Computer Science, Universidade do Porto.
1996	MSc in Computer Science, DI-UMinho.
1993	Degree in Computer Science, FCUP.

Academic positions

2008-	Director of the Health Informatics MSc course, a joint course between the Science and Medical Faculty of Porto University.
2002-	Assistant Professor, Computer Science Department, Science Faculty, Porto University.
1996-2002	Teaching Assistant, Grupo de Matemática e Informática da Faculdade de Economia da Universidade do Porto.
1993-1996	Teaching Assistant, Departamento de Matemática da Universidade do Minho.

Visiting positions

02/2000-07/2000	DIMACS - Center for Discrete Mathematics and Theoretical Computer Science, New Jersey, USA.
03/2001	CWI - National Research Institute for Mathematics and Computer Science.
06/2001-08/2001	NEC Research Institute, Princeton, USA. (Summer internship)
11/2001	NEC Research Institute, Princeton, USA. (Consultant)
02/2002-09/2002	CWI - National Research Institute for Mathematics and Computer Science. (Post-Doc)
02/2005	Computer Science Department, University of Chicago, Chicago, USA. (Sabbatical)

Present research interests

Computational Complexity
Criptography
Health Informatics

Master supervision

In preparation	2009	*PIRCE - Plataforma Interactiva para o Registo clínico e Comunicação em Epilepsia*, by Ângela Santos, MSc Health Informatics, FMUP/FCUP.
	2009	*Especificação para Documento Clínico Electrónico: Relatório de Imagem*, by João Janeiro, MSc Health Informatics, FMUP/FCUP (co-supervised with Manuel Eduardo Correia).
	2009	*Evaluation of a Teleradiology System: Impact and User Satisfaction*, by Carla Pereira, MSc Health Informatics, FMUP/FCUP (co-supervised with Ana Ferreira).
	2010	*Identity in eHealth: from the reality of physical identification to digital identification*, by Maria João Campos, MSc Health Informatics, FMUP/FCUP (co-supervised with Manuel Eduardo Correia).
Finished	2005	*Segurança em arquitecturas de rede para acesso sem fios (wireless)*, by Luís Manuel Cerqueira Barreto, MSc Computer Science, FCUP.

2005 *Segurança absoluta em sistemas de cifra de chave simétrica*, by Liliana da Conceição Salvador, Mestrado em Informática, FCUP (co-supervision with Armando Matos).

2006 *Medidas de conhecimento em protocolos criptográficos interactivos*, by Manuel António Ferreira, Mestrado em Informática, FCUP, (co-supervision with Armando Matos).

2007 *Complexidade de Comunicação: Relação com o Tamanho dos Rectângulos e com a Complexidade das Instâncias*, by Andreia Sofia Costa Teixeira, Mestrado em Informática, FCUP, (co-supervision with Armando Matos).

2007 *Uma Abordagem Relacional e Planeada para a Aplicação de Modelos de Gestão da Segurança na Saúde?*, by Rui Gomes, MSc Health Informatics, FMUP/FCUP (co-supervised with Luís Lapão).

2008 *Use of a Government Issued Digital Identification Card Securing a Health Information System.*, by Ricardo Filipe Sousa Santos, MSc Health Informatics, FMUP/FCUP.

2008 *Access Control in a Health Information System.*, by Pedro Ferreira Farinha Silva, MSc Health Informatics, FMUP/FCUP.

2009 *Análise de algoritmos de classificação para traçados de batimento cardíaco fetal*, by Teresa Henriques, MSc in Mathematical Engineering FCUP.

PhD supervision

In preparation 2006-09 *Interactive Protocols: Knowledge Measures*, by André Nuno Carvalho Souto.

2008-10 *Characterization of Cryptographic Primitives Based on Kolmogorov Complexity*, by Andreia Sofia Teixeira, (co-supervision with Armando Matos).

Finished 2006-09 *Modelling Access Control for Complex Information Systems*, by Ana Margarida Leite de Almeida Ferreira, (co-supervision with David Chadwick). This dissertation won the The Fraunhofer Portugal Challenge 2010, for the best PhD thesis with practical utility.

2003-07 *Applications of Kolmogorov Complexity to Cryptography*, by Alexandre Jorge Miranda Pinto, (co-supervision with Armando Matos). Now Post-Doc at Universidade do Minho.

Program Committees

Evolution, Emergence, Generation a satellite workshop of the European Conference in Complex Systems 2006.

Inforum 2009: Simpósium de Informática, Lisboa, Portugal.

Computability in Europe (CiE) 2010: Programs, Proofs, Processes. Açores, Portugal. (CiE Conference Series)

Inforum 2010: Simpósium de Informática, Braga, Portugal.

Sixth International Conference on Computability, Complexity and Randomness (CCR 2011).

Organization of Conferences

1^o Simpósio de Informática Médica, Porto, Portugal. 2008.

Computability in Europe (CiE) 2010: Programs, Proofs, Processes. Açores, Portugal. (CiE Conference Series)

IEEE Computational Complexity Conference 2012, local organizer (chair).

Participation in research projects

2010-2012	"CSI- Criptographic Security of Individual Instances", PTDC/EIA-CCO/099951/2008 (Portuguese Science Foundation), Principal Investigator.
2004-	"Computability in Europe (CiE)", European Research Network.
2005-2008	"KCrypt - Security Measures for Public-key Cryptosystems", POSC/EIA/60819/2004 (Portuguese Science Foundation), Principal Investigator.
2003-2005	"Criptography and Kolmogorov Complexity"', ICCTI/Ambassade de France au Portugal.
1999–2001	Project "CORE: Sistemas Formais e Complexidade Computacional", PRAXIS/ P/ EEI/ 14233/ 98, FCT.

Publications

Book Chapters

1. Ana Ferreira, Ricardo Cruz-Correia, Luís Antunes, David Chadwick. *Security of the Electronic Medical Record (EMR) - From legislation to practice: a people's problem?* in Handbook of Research on Distributed Medical Informatics and E-Health. IGI Global Disseminator of knowledge. In press. 2008.

2. Ana Ferreira, Luís Barreto, Pedro Brandão, Ricardo Correia, Susana Sargento, Luís Antunes. *Accessing an existing virtual electronic patient record with a secure wireless architecture.* in Mobile Health Solutions for Biomedical Applications. IGI Global Disseminator of knowledge. In press. 2008.

3. Luís Antunes. *Criptografia - Passado, Presente e Futuro. O Futuro da Internet*, ed. Centro Atlântico, pg. 251-256, Março de 1999. ISBN: 972842608-9

Papers in international scientific periodicals with referees

1. L. Antunes, L. Fortnow, D. van Melkebeek, and N. Vinodchandran. *Computational Depth: Concept and Applications.* Special issue for selected papers from the 14th International Symposium on Fundamentals of Computation Theory. **Theoretical Computer Science**, 354 (3), pp.391-404. 2006.

2. A. Ferreira, R. Cruz Correia, L. Antunes, D. Chadwick. *Access Control: how can it improve patients' healthcare?* IOS Press - Studies in Health Technology and Informatics. Volume 127, pages 65-76, 2007.

3. A. Ferreira, A. Correia, A. Silva, A. Corte, A. Pinto, A. Saavedra, A. Pereira, A. Filipa Pereira, R. Cruz-Correia, L. Antunes. *Why facilitate patient access to medical records.* IOS Press - Studies in Health Technology and Informatics. Volume 127, pages 77-90, 2007.

4. L. Antunes, L. Fortnow. *Sophistication Revisited.* **Theory of Computing Systems**, 45(1):150-161, June 2009.

5. L. Antunes, A. Matos, A. Souto and P. Vitanyi. *Depth as Randomness Deficiency.* **Theory of Computing Systems**, 45(4):724-739, 2009.

6. A. Pinto, A. Souto, Armando Matos and L. Antunes. *Commitment and Authentication Systems.* **Designs, Codes & Cryptography** (Springer), 53(3):175-193, 2009.

7. C. Santos, L. Antunes, A. Souto, J. Bernardes. *Assessment of disagreement: a new information based approach*, **Annals of Epidemiology**, 20:555-561, 2010.

8. A. Ferreira, L. Antunes, D. Chadwick and R. Crz-Correia. *Grounding Information Security in Healthcare.* **International Journal of Medical Informatics**, 79(4):268-283. 2010.

9. L. Antunes, A. Souto. *Information measures for infinite sequences*, **Theoretical Computer Science**, 41(26-28): 2602-2611, 2010.

Papers in conference proceedings

1. L. Antunes, L. Fortnow and D. van Melkebeek. *Computational depth.* Proceedings of the 16th **IEEE** Conference on Computational Complexity, pages 266-273. IEEE, New York, 2001. ISBN 0-7695-1053-1. (Ratio $30/60 = 0.5$)

2. L. Antunes, L. Fortnow, and V. Vinodchandran. *Using depth to capture average-case complexity.* In 14th International Symposium on Fundamentals of Computation Theory, volume 2751 of Lecture Notes in Computer Science, pages 303-310. **Springer**, Berlin, 2003. ISBN 3-540-40543-7. (Ratio $39/81 = 0.48$)

3. L. Antunes and L. Fortnow. *Sophistication revisited.* In Proceedings of the 30th International Colloquium on Automata, Languages and Programming, volume 2719 of Lecture Notes in Computer Science, pages 267-277. **Springer**, 2003. ISBN 3-540-40493-7. (Ratio $52/146 = 0.35$)

4. A. Ferreira, R. Correia, L. Antunes, E. Palhares, P. Marques, P. Costa and A. Costa Pereira. *Integrity for Electronic Patient Record Reports.* In Proceedings of the 17th **IEEE** Symposium on Computer Based Medical Systems, (CBMS'2004), pages 4-9. ISBN 0-7695-2104-5.

5. Ferreira A, Cruz-Correia R, Antunes L, Farinha P, Oliveira-Palhares E, Chadwick D W, Costa-Pereira A. *How to break access control in a controlled manner?* Special Track on Security, Privacy and Confidentiality - Threats and Challenges to Health Systems. In Proceedings of the 19th **IEEE** International Symposium on Computer-Based Medical Systems 2006, pages 847-854. ISBN 0-7695-2517-1. (Ratio $150/267 = 0.56$)

6. Costa-Santos C , Bernardes J , Vitányi P and Antunes L. *Clustering Fetal Heart Rate Tracings by Compression.* Special Track on Data Mining. In Proceedings of the 19th **IEEE** International Symposium on Computer-Based Medical Systems 2006, pages 685-690. ISBN 0-7695-2517-1. (Ratio $150/267 = 0.56$)

7. L. Antunes, L. Fortnow, A. Pinto and A. Souto. *Low-depth witnesses are easy to find.* In Proceedings of the 22nd IEEE Conference on Computational Complexity, pages 46-51. **IEEE**, New York, 2007.

8. L. Antunes, S. Laplante, A. Pinto and L. Salvador. *Cryptographic Security of Individual Instances.* In Proceedings of the International Conference on Information Theoretic Security. Lecture Notes in Computer Science. **Springer**, 2007.

9. A. Pinto, A. Souto, Armando Matos and L. Antunes. Commitment and Authentication Systems. In Proceedings of the International Conference on Information Theoretic Security. Lecture Notes in Computer Science. **Springer**, 2007.

10. Ferreira A, Antunes L, Pinho C, Sá C, Mendes E, Santos E, Silva F, Sousa F, Gomes F, Abreu F, Mota F, Aguiar F, Faria F, Macedo F, Martins S, Cruz-Correia R. *Who Should Access Electronic Patient Records.* In Proceedings of HEALTHINF-International Conference on Health Informatics, Funchal,Madeira, vol.2, 28-31 January 2008, pp.182-185.

11. A. Cunha, P. Vieira-Marques, R. Cruz-Correia, L. Antunes, A. Costa-Pereira. *A First Approach for a Regional Wide VEPR.* In Proceedings of HEALTHINF-International Conference on Health Informatics, Funchal,Madeira, vol.2, 28-31 January 2008, pp.215-218.

12. R. Santos, M. E. Correia, L. Antunes. *Use of a Government Issued Digital Identification Card Securing a Health Information System.* Proceedings of the IEEE International Carnahan Conference on Security Technology, Czech Republic October 13 - 16, 2008.

13. A. Ferreira, R. Correia, D. Chadwick, L. Antunes. *Improving the Implementation of Access Control in EMR.* Proceedings of the IEEE International Carnahan Conference on Security Technology, Czech Republic October 13 - 16, 2008.

14. L. Antunes and L. Fortnow. Worst-Case Running Times for Average-Case Algorithms. 24th IEEE Conference on Computational Complexity, pages 298-303. 2009.

15. A. Ferreira, D. Chadwick, P. Farinha, G. Zhaoe, R. Chilro, R. Correia and L. Antunes. How to securely break into RBAC: the BTG-RBAC model. Proceedings of the Annual Computer Security Applications Conference 2009.

16. A. Ferreira, R Crz-Correia,D. Chadwick and L. Antunes. Access Control in Healthcare: the methodology from legislation to practice . 13th World Congress on Medical and Health Informatics Medinfo 2010.

17. Farinha P., Ferreira A., Cruz-Correia R, Almeida F. and Antunes L. From legislation to practice: a case study of break the glass in healthcare. HealthInf 2010. 2010. Valencia, Spain.

18. A. Teixeira, A. Souto, L. Antunes and A. Matos: Entropy Measures vs. Algorithmic Information. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2010), Austin, Texas, USA, June 2010.