SECRYPT 2006

Proceedings of the International Conference on Security and Cryptography

Setúbal, Portugal

August 7 – 10, 2006

Organized by
INSTICC – Institute for Systems and Technologies of Information, Control and Communication

Sponsored by
Polytechnic Institute of Setúbal

Technically Co-Sponsored by
IEEE Systems, Man and Cybernetics (SMC) Society

In Cooperation with
International Association for Cryptologic Research

Hosted by
Setúbal College of Business Administration

Edited by Manu Malek, Eduardo Fernández-Medina and Javier Hernando

Printed in Portugal

ISBN: 972-8865-63-5

ISBN (13 digits): 978-972-8865-63-4

Depósito Legal: 245453/06

http://www.secrypt.org

secretariat@secrypt.org

SECRYPT is part of ICETE - The International Joint Conference on

e-Business and Telecommunications

BRIEF CONTENTS

BRIEF CONTENTS III

KEYNOTE LECTURES IV

TUTORIAL IV

ORGANIZING AND STEERING COMMITTEES V

PROGRAM COMMITTEE IX

AUXILIARY REVIEWERS VIII

SELECTED PAPERS BOOK IX

FOREWORD............ XI

CONTENTS............ XIII

KEYNOTE LECTURES

David Marca

University of Phoenix

U.S.A.

Manu Malek

Stevens Institute of Technology

U.S.A.

Les Barclay

Barclay Associates Ltd

U.K.

Fernando Pereira

Instituto Superior Técnico – Instituto de Telecomunicações

Portugal

Jan Jürjens

Technische Universität München

Germany

Anisse Taleb

Ericsson AB

Sweden

Tom Greene

M.I.T.

U.S.A.

TUTORIAL

David Marca

University of Phoenix

U.S.A.

ORGANIZING AND STEERING COMMITTEES

Conference Chair

Joaquim Filipe, INSTICC / Polytechnic Institute of Setúbal, Portugal

Honorary Chair

Mohammad S. Obaidat, Monmouth University, U.S.A.

Program co-Chairs

Manu Malek, Stevens Institute of Technology, U.S.A.

Eduardo Fernández-Medina, UCLM, Spain

Javier Hernando, Polytechnic University of Catalonia, Spain

Proceedings Production

Paulo Brito, INSTICC, Portugal

Helder Cide, INSTICC, Portugal

Bruno Encarnação, INSTICC, Portugal

Vitor Pedrosa, INSTICC, Portugal

Graphics Production

Marina Carvalho, INSTICC, Portugal

Secretariat and Webdesigner

Mónica Saramago, INSTICC, Portugal

PROGRAM COMMITTEE

Kamel Adi, University of Quebec in Outaouais (UQO), Canada

Gail-Joon Ahn, University of North Carolina at Charlotte, U.S.A

Ali Akhavi, LIAFA - CNRS, France

Jörn Altmann, School of Information Technology, Germany

Farooq Anjum, Telcordia Technologies, U.S.A.

Giuseppe Ateniese, The Johns Hopkins University, U.S.A.

Dan Bailey, RSA Laboratories, U.S.A.

Anthony Bedford, RMIT University, Australia

John Black, University of Colorado at Boulder, U.S.A.

Carlo Blundo, Università di Salerno, Italy

Xavier Boyen, Voltage Inc., U.S.A

Emmanuel Bresson, CELAR, France

Rahmat Budiarto, National Advanced IPv6 (NAv6) Center, Malaysia

Roy Campbell, University of Illinois, U.S.A

Rui Costa Cardoso, University of Beira Interior, Portugal

Eurico Carrapatoso, FEUP/INESC Porto, Portugal

Pascale Charpin, INRIA - Rocquencourt, France

Mathieu Ciet, Gemplus, France

Miguel Correia, LASIGE, Faculdade de Ciencias da Universidade de Lisboa, Portugal

Véronique Cortier, Loria, CNRS, France

Paolo D'Arco, D.I.A - University of Salerno, Italy

Sabrina De Capitani di Vimercati, DTI, Universita' degli Studi di Milano, Italy

Falko Dressler, University of Erlangen, Germany

Robert Erbacher, Utah State University, U.S.A.

Serge Fehr, CWI Amsterdam, The Netherlands

Eduardo B. Fernandez, Florida Atlantic University, U.S.A.

Marc Fischlin, Darmstadt University of Technology, Germany

Mário Freire, University of Beira Interior, Portugal

Mariagrazia Fugini, Politecnico di Milano, Italy

Steven Furnell, University of Plymouth, U.K.

Luciano Gaspary, Universidade Federal do Rio Grande do Sul, Brazil

Paolo Giorgini, University of Trento, Italy

Dieter Gollmann, TU Hamburg-Harburg, Germany

Carlos Goulart, Federal University of Vicosa, Brazil

Lisandro Granville, Federal University of Rio Grande do Sul, Brazil

Stefanos Gritzalis, University of the Aegean, Greece

Vic Grout, University of Wales, U.K.

Cynthia Irvine, Naval Postgraduate School, U.S.A.

Hamid Jahankhani, University Of East London, U.K.

Nigel Jefferies, Vodafone Group R&D, U.K.

Willem Jonker, Philips Research / Twente University, The Netherlands

Elias P. Duarte Jr., Federal University of Parana, Brazil

Agggelos Kiayias, University of Connecticut, U.S.A

Seungjoo Kim, Sungkyunkwan Universit and Twente University, Korea

Paris Kitsos, Hellenic Open University (HOU), Greece

Lars Knudsen, Technical University of Denmark, Denmark

Cetin Koc, Istanbul Commerce University, Turkey

Christopher Kruegel, Technical University Vienna, Austria

Kaoru Kurosawa, Ibaraki University, Japan

Tanja Lange, Technical University of Denmark, Denmark

Victor Peral Lecha, France Telecom R&D, U.K.

Albert Levi, Sabanci University, Turkey

Chae Hoon Lim, Sejong University, Korea

Javier Lopez, University of Malaga, Spain

Olivier Markowitch, Université Libre de Bruxelles, Belgium

Alexander May, TU Darmstadt, Germany

Madjid Merabti, Liverpool John Moores University, U.K.

Ali Miri, University of Ottawa, Canada

PROGRAM COMMITTEE (CONT.)

Atsuko Miyaji, Japan Advaned Institute of Science and Technology, Japan

Edmundo Monteiro, University of Coimbra, Portugal

Haralambos Mouratidis, University of East London, U.K.

Yi Mu, University of Wollongong, Australia

Volker Müller, University of Luxembourg, Luxembourg

Juan Gonzalez Nieto, Queensland University of Technology, Australia

Kaisa Nyberg, Helsinki University of Technology and Nokia, Finland

Tatsuaki Okamoto, NTT, Japan

José Luis Oliveira, University of Aveiro, Portugal

Martin Olivier, University of Pretoria, South Africa

Rolf Oppliger, eSECURITY Technologies, Switzerland

Elisabeth Oswald, Graz University of Technology, Austria

Guenther Pernul, University of Regensburg, Germany

George Polyzos, AUEB, Greece

Atul Prakash, University of Michigan, Greece

Jean-Jacques Quisquater, UCL, Louvain, Belgium

Indrakshi Ray, Colorado State University, U.S.A

Indrajit Ray, Colorado State University, U.S.A

David Samyde, FemtoNano, France

Susana Sargento, Instituto de Telecomunicações - Universidade de Aveiro, Portugal

Damien Sauveron, University of Limoges, France

Erkay Savas, Sabanci University, Turkey

Berry Schoenmakers, Technical University of Eindhoven, The Netherlands

Bruno Schulze, LNCC, Brazil

Alice Silverberg, University of California, Irvine, U.S.A.

Nicolas Sklavos, University of Patras, Greece

Jose Neuman de Souza, Federal University of Ceará, Brazil

Mark Stamp, San Jose State University, U.S.A.

Lily Sun, The University of Reading, U.K.

Berk Sunar, Worcester Polytechnic Institute, U.S.A.

Willy Susilo, University of Wollongong, Australia

Tsuyoshi Takagi, Future University-Hakodate, Japan

Robert Tolksdorf, Freie Universität Berlin, Germany

Ambrosio Toval, University of Murcia, Spain

Wade Trappe, WINLAB, Rutgers University, U.S.A.

Wen-Guey Tzeng, National Chiao Tung University, Taiwan

Ulrich Ultes-Nitsche, University of Fribourg, Switzerland

Guillaume Urvoy-Keller, Institut Eurecom, France

Huaxiong Wang, Macquarie University, Australia

Yongge Wang, University of North Carolina, U.S.A.

Susanne Wetzel, Stevens Institute of Technology, U.S.A.

Duminda Wijesekera, George Mason University, U.S.A.

Chaoping Xing, National University of Singapore, Singapore

Shouhuai Xu, University of Texas at San Antonio, U.S.A.

Mariemma Yagüe, University of Malaga, Spain

Jeff Yan, University of Newcastle, U.K.

Alec Yasinsac, SAIT Laboratory, FSU, U.S.A.

Sung-Ming Yen, National Central University, Taiwan

Meng Yu, Monmouth University, U.S.A.

Moti Yung, RSA Labs and Columbia University, U.S.A.

Yuliang Zheng, UNC Charlotte, U.S.A.

André Zúquete, University of Aveiro, Portugal

AUXILIARY REVIEWERS

Jun Furukawa, NEC Corporation, Japan

Goichiro Hanaoka, Research Center for Information Security, AIST, Japan

Chien-Ning Chen, National Central University, Taiwan

Kuo-Zhe Chiou, National Central University, Taiwan

Chao-Chih Hsu, National Central University, Taiwan

Fu-Hau Hsu, National Central University, Taiwan

Hsi-Chung Lin, National Central University, Taiwan

Rachel Akimana, Universite Libre de Bruxelles, Belgium

Daniel J. Bernstein, University of Illinois at Chicago, U.S.A.

Marc Joye, Gemplus, Card Security Group, France

Claude Barral, Gemalto, France

Christophe Clavier, Gemalto, France

Damien Giry, UCL CryptoGroup, Belgium

Guerric Meurice de Dormale, UCL CryptoGroup, Belgium

Steve Kremer, LSV ENS Cachan, France

Ozgur Gurleyen, Vodafone, UK

Wolfgang Dobmeier, University of Regensburg, Germany

Rolf Schillinger, University of Regensburg, Germany

Christian Schläger, University of Regensburg, Germany

Francisco Javier Lucas Martínez, Universidad de Murcia, Spain

Fernando Molina Molina, Universidad de Murcia, Spain

Miguel Ángel Martínez Aguilar, Universidad de Murcia, Spain

Celalettin Emre Sayin, Sabanci University, Turkey

Abdulhakim Unlu, Sabanci University, Turkey

Fabien Laguillaumie, INRIA Futurs, France

Didier Alquie, CELAR, France

Johann Barbier, CELAR, France

Lutz Suhrbier, FU Berlin, Germany

Franck Landelle, CELAR, France

Xiaofeng Gong, University of Newcastle upon Tyne, U.K.

Toshihiro Tabata, Okayama University, Japan

Masakazu Soshi, JAIST, Japan

Takeshi Okamoto, Tsukuba University, Japan

Sotiris Ioannidis, Stevens Institute of Technology, U.S.A.

C. Lambrinoudakis, University of the Aegean, Greece

SELECTED PAPERS BOOK

A number of selected papers presented at SECRYPT 2006 will be published by Springer, in a book entitled e-Business and Telecommunication Networks. This selection will be done by the conference and program co-chairs, among the papers actually presented at the conference, based on a rigorous review by the SECRYPT 2006 program committee members.

FOREWORD

We warmly welcome you to SECRYPT 2006 - the *International Conference on Security and Cryptography*, which is held, this year, in Portugal. This conference reflects a continuing effort to increase the dissemination of recent research among professionals who work on the fields of security and cryptography, especially for telecommunications. SECRYPT is integrated as one of the modules of the ICETE joint conference.

The major goal of ICETE is to bring together researchers, engineers and practitioners interested in information and communication technologies, including e-business, wireless networks and information systems, security and cryptography, signal processing and multimedia applications. These are the main knowledge areas that define the four component conferences, namely: ICE-B, WINSYS, SECRYPT and SIGMAP, which together form the ICETE joint conference.

In the program for this joint conference, we have included keynote lectures, tutorials, papers, and posters to present the widest possible view on these technical areas. With these tracks, we expect to appeal to a global audience of engineers, scientists, business practitioners and policy experts, interested in the research topics of ICETE. All tracks focus on real world applications and rely on contributions from the industry, with different solutions for end-user applications and enabling technologies, in a diversity of communication environments. The proceedings demonstrate a number of new and innovative solutions for e-business and telecommunication, and demonstrate the vitality of these research areas.

We have received 326 papers in total, with contributions from 53 different countries, from all continents, which really shows the success and global dimension of ICETE 2006. To evaluate each submission, a double blind paper evaluation method was used: each paper was reviewed by at least two internationally known experts from our Program Committee, and more than 95% of the papers had 3 reviews or more. In the end, 98 papers were selected to be published and presented as full papers, 30' oral presentations, corresponding to a 30% full paper acceptance ratio; 105 additional papers were published and presented, including short papers and posters, corresponding to a 62% total acceptance ratio. Furthermore, a short list of about thirty top-quality papers will be selected to appear in a book that will be published by Springer.

We would like to emphasize the fact that ICETE 2006 includes one tutorial and seven outstanding keynote lectures in areas which are very relevant, nowadays. These talks are presented by distinguished researchers who are internationally recognized experts in all ICETE areas, and contribute to heighten the overall interest of the Conference.

ICETE 2006 is a joint conference that has achieved a high quality level, which we hope and strive not only to maintain but even increase in next year's conference, ICETE 2007, which is already planned to be held in Barcelona/Spain.

But life is more than technology, so a Conference Banquet was planned for the evening of August 9 (Wednesday) in order to facilitate social networking. We hope that you enjoy this exciting conference and we wish you an unforgettable stay in the beautiful city of Setúbal.

We would like to express our thanks, first of all, to the authors of the technical papers presented at the conference, whose work made possible to put together a high quality program. Next, we would like to thank all the members of the program committee and reviewers, who helped us with their expertise, dedication and time. We would also like to thank the invited speakers for their invaluable contribution, sharing their vision and knowledge. Naturally, a word of appreciation for the work of the secretariat and all other members of the organization, whose diligence in dealing with all organizational issues were essential and required a collaborative effort of a dedicated and highly capable team.

We hope that you will find these proceedings interesting and a helpful reference in the future for all those who need to address the areas of security and cryptography.

Manu Malek

Stevens Institute of Technology, U.S.A.

Eduardo Fernández-Medina

UCLM, Spain

Javier Hernando

Polytechnic University of Catalonia, Spain

Joaquim Filipe

Polytechnic Institute of Setúbal / INSTICC, Portugal

Mohammad Obaidat

Monmouth University, U.S.A.

CONTENTS

INVITED SPEAKERS

KEYNOTE LECTURES

E-BUSINESS STRATEGY - Charting a Way through Uncertain Waters of Electronic Commerce IS-5
David A. Marca

IT SECURITY FORENSICS: PROMISES AND SHORTCOMINGS IS-17
Manu Malek

WIRELESS COMMUNICATIONS, A NEW EMPHASIS FOR EFFECTIVE USE OF THE RADIO SPECTRUM IS-19
Les Barclay

MULTIMEDIA REPRESENTATION IN MPEG STANDARDS: ACHIEVEMENTS AND CHALLENGES IS-21
Fernando Pereira

MODEL-BASED SECURITY ENGINEERING IS-23
Jan Jürjens

ADVANCES IN SPEECH AND AUDIO CODING AND ITS APPLICATIONS FOR MOBILE MULTIMEDIA IS-31
Anisse Taleb

REDEFINING THE MARKET PLACE: ONLY THE NUMBERS ARE DIFFERENT? IS-33
Thomas Greene

TUTORIAL

PROJECT MANAGEMENT FOR E-BUSINESS INITIATIVES - Project Framework, Proven Practices, Coordinated Work, Focused Sub-Teams IS-37
David A. Marca

ACCESS CONTROL AND INTRUSION DETECTION

FULL PAPERS

SECURITY ENHANCEMENT FOR A LOW COMPUTATION COST USER AUTHENTICATION SCHEME
Behnam Sattarzadeh, Mahdi Asadpour and Rasool Jalili 5

THE "SECUREPHONE" - A Mobile Phone with Biometric Authentication and e-Signature Support for Dealing Secure Transactions on the Fly
R. Ricci, G. Chollet, M. V. Crispino, S. Jassim, J. Koreman, A. Morris, M. Olivar-Dimas, S. García-Salicetti and P. Soria-Rodríguez 9

PERSON VERIFICATION BY FUSION OF PROSODIC, VOICE SPECTRAL AND FACIAL PARAMETERS
Javier Hernando, Mireia Farrús, Pascual Ejarque, Ainara Garde and Jordi Luque 17

COMPARATIVE STUDY BETWEEN BAYESIAN NETWORK AND POSSIBILISTIC NETWORK IN INTRUSION DETECTION
Najla Arfaoui, Farah Jemili, Montaceur Zaghdoud and Mohamed Ben Ahmed 24

INTRUSION DETECTION FOR WEB APPLICATIONS (SHORT VERSION)
Nathalie Dagorn 32

SPOOFED ARP PACKETS DETECTION IN SWITCHED LAN NETWORKS
Zouheir Trabelsi and Khaled Shuaib 40

EVALUATION OF THE INTRUSION DETECTION CAPABILITIES AND PERFORMANCE OF A SECURITY OPERATION CENTER
Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou and Francois Spies 48

WORKLOAD HIDDEN MARKOV MODEL FOR ANOMALY DETECTION
Juan Manuel García, Tomás Navarrete and Carlos Orozco 56

SHORT PAPERS

USING ATTACK GRAPHS IN AD HOC NETWORKS - For Intrusion Prediction Correlation and Detection
Marianne Azer, Sherif El-Kassas and Magdy El-Soudani 63

QUANTITATIVE ANALYSIS AND ENFORCEMENT OF THE PRINCIPLE OF LEAST PRIVILEGE IN ROLE-BASED
Chunren Lai and Chang N. Zhang 69

ON THE SELF-SIMILARITY OF THE 1999 DARPA/LINCOLN LABORATORY EVALUATION DATA
Kun Huang and Dafang Zhang 75

POSTERS

ACCESS CONTROL AND JOINT MANAGEMENT FOR COLLABORATIVE PEER GROUPS
Wenhua Qi 83

PROTECTING ADAPTIVE MULTIMEDIA DELIVERY AND ADAPTATION USING PROXY BASED APPROACH
Ahmed Reda Kaced and Jean-Claude Moissinac 87

DIGITAL PSEUDONYM IDENTITY FOR E-COMMERCE
Rafael Martínez-Peláez, Francisco J. Rico-Novella and Luis A. Zarza-López 91

NETWORK SECURITY AND PROTOCOLS

FULL PAPERS

A CHALLENGING BUT FEASIBLE BLOCKWISE-ADAPTIVE CHOSEN-PLAINTEXT ATTACK ON SSL
Gregory V. Bard 99

INTERNET ROUTING SECURITY: AN APPROACH TO DETECT AND TO REACT TO INCORRECT ADVERTISEMENTS
Ines Feki, Xiaoli Zheng, Mohammed Achemlal and Ahmed Serhrouchni 110

LAYERED ARCHITECTURE FOR SECURE E-COMMERCE APPLICATIONS
Amir Herzberg and Igal Yoffe 118

TRUST MANAGEMENT WITHOUT REPUTATION IN P2P GAMES
Adam Wierzbicki 126

PROTECTING CIPHER BLOCK CHAINING AGAINST ADAPTIVE CHOSEN PLAINTEXT ATTACK
Chuan-Wen Loe and Khoongming Khoo 135

FORWARD-SECURE AUTHENTICATED-ENCRYPTION IN MULTI-RECEIVER SETTING
Kan Yasuda, Kazumaro Aoki, Eiichiro Fujisaki and Atsushi Fujioka 141

ON THE DESIGN OF A LOW-RATE DOS ATTACK AGAINST ITERATIVE SERVERS
Gabriel Maciá-Fernández, Jesús E. Díaz-Verdejo and Pedro García-Teodoro 149

SECURE ACCESS MODULES FOR IDENTITY PROTECTION OVER THE EAP-TLS - Smartcard Benefits for User Anonymity in Wireless Infrastructures
Pascal Urien and Mohamad Badra 157

SHORT PAPERS

A SERVICE DISCOVERY THREAT MODEL FOR AD HOC NETWORKS
Adrian Leung and Chris Mitchell 167

ACTION-TRIGGERED PUBLIC-KEY SYSTEM FOR GSM USING RSA WITH PHONE-DEPENDENT ENCRYPTION
Rehab K. El Nemr, Imane Aly Saroit Ismail and S. H. Ahmed 175

SECURITY CONSIDERATIONS IN CURRENT VOIP PROTOCOLS
Steffen Fries 183

A DOS ATTACK AGAINST THE INTEGRITY-LESS ESP (IPSEC)
Ventzislav Nikov 192

POSTERS

COMBINATION OF A SMARTCARD E-PURSE AND E-COIN TO MAKE ELECTRONIC PAYMENTS ON THE INTERNET
Antonio Ruiz-Martínez, Antonio F. Gómez-Skarmeta and Óscar Cánovas 203

ACHIEVING UNCONDITIONAL SECURITY IN EXISTING NETWORKS USING QUANTUM CRYPTOGRAPHY
Stefan Rass, Mohamed Ali Sfaxi and Solange Ghernaouti-Hélie 207

PROTOCOL INDEPENDENT LIGHTWEIGHT SECURE COMMUNICATION
M. Amaç Güvensan and A. Gökhan Yavuz 211

CRYPTOGRAPHIC TECHNIQUES AND KEY MANAGEMENT

FULL PAPERS

TRAITOR TRACING FOR SUBSCRIPTION-BASED SYSTEMS
Hongxia Jin, Jeffory Lotspiech and Mario Blaum 223

DIGITAL OBJECT RIGHTS MANAGEMENT - Interoperable Client-side DRM Middleware
Carlos Serrão, Miguel Dias and Jaime Delgado 229

EFFICIENT ALL-OR-NOTHING ENCRYPTION USING CTR MODE
Robert P. McEvoy and Colin C. Murphy 237

PROPOSALS FOR ITERATED HASH FUNCTIONS
Lars R. Knudsen and Søren S. Thomsen 246

PARALLEL MULTIPLICATION IN F2n USING CONDENSED MATRIX REPRESENTATION
Christophe Negre 254

CHOSEN-IV STATISTICAL ATTACKS ON eSTREAM CIPHERS
Markku-Juhani O. Saarinen 260

DIGITAL CONTRACT SIGNATURE SCHEME BASED ON MULTIPLE CRYPTOSYSTEM
Wang Lianhai and Manu Malek 267

SHORT PAPERS

PRIVATE BIDDING FOR MOBILE AGENTS
Bartek Gedrojc, Kathy Cartrysse and Jan C. A. van der Lubbe 277

AN INFINITE PHASE-SIZE BMAP/M/1 QUEUE AND ITS APPLICATION TO SECURE GROUP COMMUNICATION
Hiroshi Toyoizumi 283

ON USE OF IDENTITY-BASED ENCRYPTION FOR SECURE EMAILING
Christian Veigner and Chunming Rong 289

MORE ROBUST PRIVATE INFORMATION
Chun-Hua Chen and Gwoboa Horng 297

AN ALGORITHM FOR AUTHENTICATION OF DIGITAL IMAGES
Dan Dumitru Burdescu and Liana Stanescu 303

POSTERS

USING OMA DRM 2.0 PROTECTED CONTENT - Ogg Vorbis Protected Audio under Symbian OS
Francisco Pimenta and Carlos Serrão 311

DESIGN OF CRYPTOGRAPHIC PROTOCOLS BY MEANS OF GENETIC ALGORITHMS TECHNIQUES
Luis Zarza, Josep Pegueroles, Miguel Soriano and Rafael Martínez 316

FINITE FIELD MULTIPLICATION IN LAGRANGE REPRESENTATION USING FAST FOURRIER TRANSFORM
Christophe Negre 320

INFORMATION ASSURANCE

FULL PAPERS

JASTEG2000 - Steganography for JPEG2000 Coded Images
Domenico Introna and Francescomaria Marino 329

SHORT PAPERS

NETWORK SECURITY EVALUATION BASED ON SIMULATION OF MALFACTOR'S BEHAVIOR
Igor Kotenko and Mikhail Stepashkin 339

POSTERS

SMOOTH BLOCKS-BASED BLIND WATERMARKING ALGORITHM IN COMPRESSED DCT DOMAIN
Chun Qi, Haitao Zhou and Bin Long 347

SECURITY IN INFORMATION SYSTEMS

FULL PAPERS

LEAST PRIVILEGE IN SEPARATION KERNELS
Timothy E. Levin, Cynthia E. Irvine and Thuy D. Nguyen 355

COLLABORATION SECURITY FOR MODERN INFORMATION SYSTEMS
Richard Whittaker, Gonzalo Argote-Garcia, Peter J. Clarke and Raimund K. Ege 363

INTER-NODE RELATIONSHIP LABELING: A FINE-GRAINED XML ACCESS CONTROL IMPLEMENTATION USING GENERIC SECURITY LABELS
Zheng Zhang and Walid Rjaibi 371

USING MICROSOFT OFFICE INFOPATH TO GENERATE XACML POLICIES
Manuel Sánchez, Gabriel López, Antonio F. Gómez-Skarmeta and Óscar Cánovas 379

SECURE ONLINE ENGLISH AUCTIONS
Jarrod Trevathan and Wayne Read 387

FLEXIBLE LICENSE TRANSFER SYSTEM USING MOBILE TERMINAL
Masaki Inamura, Toshiaki Tanaka, Toshiyuki Fujisawa, Kazuto Ogawa and Takeshi Kimura 397

SHORT PAPERS

EXTENDING XML SIGNATURE AND APPLYING IT TO WEB PAGE SIGNING
Takahito Tsukuba and Kenichiro Noguchi 407

SECURING WEB SERVICES USING IDENTITY-BASED ENCRYPTION (IBE)
Kari Anne Haaland and Chunming Rong 413

DEFINING VIEWPOINTS FOR SECURITY ARCHITECTURAL PATTERNS
David G. Rosado, Carlos Gutiérrez, Eduardo Fernández-Medina and Mario Piattini 419

SECURITY RISK ANALYSIS IN WEB SERVICES SYSTEMS
Carlos Gutiérrez, Eduardo Fernández-Medina amd Mario Piattini 425

DESIGN AND IMPLEMENTATION OF A PRACTICAL SECURE DISTRIBUTED HEALTHCARE APPLICATION
Zaobin Gan and Vijay Varadharajan 431

IMPROVING SOFTWARE SECURITY THROUGH AN INTEGRATED APPROACH
Zaobin Gan, Dengwei Wei and Vijay Varadharajan 437

A NEW (t,n) MULTI-SECRET SHARING SCHEME BASED ON LINEAR ALGEBRA
Seyed Hamed Hassani and Mohammad Reza Aref 443

UNDESIRABLE AND FRAUDULENT BEHAVIOUR IN ONLINE AUCTIONS
Jarrod Trevathan and Wayne Read 450

MODELLING E-BUSINESS SECURITY USING BUSINESS PROCESSES
Sharon Nachtigal and Chris J. Mitchell 459

POSTERS

SECURE INFORMATION SYSTEMS DEVELOPMENT - Based on a Security Requirements Engineering Process
Daniel Mellado, Eduardo Fernández-Medina and Mario Piattini 467

AN EXTENDED ROLE-BASED ACCESS CONTROL FOR WEB SERVICES
Yi-qun Zhu, Jian-hua Li and Quan-hai Zhang 471

AUTHOR INDEX 475

DEFINING VIEWPOINTS FOR SECURITY ARCHITECTURAL PATTERNS

David G. Rosado, Carlos Gutiérrez, Eduardo Fernández-Medina, Mario Piattini
ALARCOS Research Group. Information Systems and Technologies Department UCLM-Soluziona Research and Development Institute. Escuela Superior de Informática. University of Castilla-La Mancha.
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{David.GRosado, Eduardo.Fdez-Medina, Mario.Piattini}@uclm.es, carlos.gutierrez@stl.es

Keywords: Security Architectures, Security Patterns, ViewPoints

Abstract: For decades, the security community has undertaken detailed research into specific areas of security, while largely ignoring the design process. Software architecture has emerged as an important sub-discipline of software engineering, particularly in the realm of large system development. This paper describes how security architectural patterns lack of a comprehensive and complete well-structured documentation that conveys essential information of their logical structure, deployment-time, run-time behaviour, monitoring configuration, and so on. Thus we will propose a viewpoints model for describing security architectural patterns. We will investigate security architectural patterns from several IEEE 1471-2000 compliant viewpoints and develop an example that demonstrates how to describe a security architectural pattern with viewpoints. We will make use of well-known language notations such as UML to maximize comprehensibility.

1 INTRODUCTION

In a typical application development environment, architects and developers share similar experiences. They deploy business applications in a highly compressed time frame, making applications work, testing functionality at all levels, ensuring that they meet expected system performance or service levels, and wrapping applications with an attractive client presentation and user documentation. Ensuring the security of the application at all levels has usually been considered at the last phase of the development process (Steel, Nagappan et al. 2005).

For decades, the security community has undertaken detailed research into specific areas of security, while largely ignoring the design process. Security aspects cannot be "blindly" inserted into an IT-system, but the overall system development must take security aspects into account. The result of a well-engineered security system must be an architecture that ensures specific security aspects such as secrecy, integrity and availability (Artelsmair and Wagner 2003).

As we have seen over and over, the software architecture for a system plays a central role in system development as well as in the organization that produces it. Architecture serves as the blueprint for both the system and the project developing it. It defines the work assignments that must be carried out by design and implementation teams and it is the primary carrier of system qualities such as performance, modifiability, and security; none of which can be achieved without a unifying architectural vision. Architecture is an artifact for early analysis to make sure that the design approach will yield an acceptable system. In short, architecture is the conceptual glue that holds every phase of the project together for all of its many stakeholders (Bass, Clements et al. 2003). The architecture must be documented to communicate how it achieves those properties (Bachmann, Bass et al. 2000).

Recently, there has been a growing interest in identifying security patterns in software-intensive systems since they provide techniques for considering, detecting and solving security issues from the beginning of their development life-cycle (Yoder and Barcalow 1997; Schumacher and Roedig 2001; Cheng, Konrad et al. 2003; Schumacher, Fernandez et al. 2005). Security patterns work together to form a collection of coordinated security countermeasures thereby addressing host, network and application security.

This paper describes how security architectural patterns lack of a comprehensive and complete well-structured documentation that conveys essential information of its logical structure, run-time behaviour, deployment-time and monitoring configuration, constraints, elements, and so on. In consequence, we will propose an alternative way for describing security architectural patterns from viewpoints and views, and therefore we can add more information about the pattern in the template used for defining patterns.

The remainder of this paper is organized as follows. Section 2 will discuss the importance of software architectures and the two most important concepts associated with software architecture documentation: view and viewpoint; In Section 3, we will define security patterns and what security architectural patterns are; In section 4, we will describe the viewpoint template defined by the IEEE 1471-2000 standard; In section 5, an overview of the IEEE 1471-2000 compliant Security Subsystem Design viewpoint's template definition will be shown and we will discuss an example of security architectural pattern. Finally, we will put forward our conclusions and future work.

2 SOFTWARE ARCHITECTURE

Software architecture has emerged as an important sub-discipline of software engineering, particularly in the realm of large system development. There are many definitions of software architecture (Garlan and Anthony 2002; Bass, Clements et al. 2003), but what these definitions have in common is their emphasis on architecture as a description of a system, as a sum of smaller parts, and how those parts relate to and cooperate with each other to perform the work of the system.

The architecture must be documented to communicate how it achieves properties such as performance, reliability, security, or modifiability. Fundamentally, architecture documentation can serve three different functions (Bachmann, Bass et al. 2000): a) A means of education. Typically, this means introducing people to the system. b) A vehicle for communication among stakeholders. A stakeholder is someone who has a vested interest in the architecture. c) A basis for system analysis. To support analysis, documentation must provide the appropriate information for the particular activity being performed.

3 SECURITY PATTERNS

Security patterns are proposed as a means of bridging the gap between developers and security experts. Security patterns are intended to capture security expertise in the form of worked solutions to recurring problems. The benefits of using patterns are: they can be revisited and implemented at anytime to improve the design of a system; less experienced practitioners can benefit from the experience of those more fluent in security patterns; they provide a common language for discussion, testing and development; they can be easily searched, categorized and refactored; they provide reuseable, repeatable and documented security practices; they do not define coding styles, programming languages or vendors (Berry, Carnell et al. 2002).

An architectural pattern expresses a fundamental structural organization schema for software systems. It provides a set of predefined subsystems, specifies their responsibilities, and includes rules and guidelines for organizing the relationships between them (Buschmann, Meunier et al. 1996).

We define security architectural patterns at several levels of detail depending on the different potential consumers who see different characteristics, functionalities, connections and behavior of a same pattern. If we define security patterns from different perspectives, we are adding more relevant information to the template used for describing security patterns.

4 VIEWPOINTS APPROACH

We attempt to extend the template by adding new information from the stakeholders' viewpoint following as a reference the "4+1" view model (Kruchten 1995).

Obviously, since the 4+1 views preceded IEEE 1471, they do not meet the definition of views as specified in the standard. The 4+1 views describe a collection of representations that provide guidance for software architects. The viewpoints we discuss are within the spirit of the 4+1 views.

ANSI/IEEE 1471-2000 (IEEE 2000) provides guidance for choosing the best set of views to document, by bringing stakeholder interests to bear. It prescribes defining a set of viewpoints to satisfy the stakeholder community. For describing viewpoints and views, IEEE 1471 standard defines a set of elements or sections (template) that are showed in (IEEE 2006) and that we will see later.

4.1 ViewPoints Catalogue

We are defining a library of viewpoints of security that allow us to document security architectural patterns according to IEEE 1471-2000. By definition, these viewpoints are reusable for any software system, thus we can document security patterns, security architecture, software architecture, etc., based on our viewpoint's library.

A number of viewpoint catalogues already exist, but we have found that all of them do not consider aspects of security, they are only applied to the development of architectures for large information systems and they are not applied in the context of security. In response, we have developed a set of viewpoints for the security architect and the security engineers, that build up and extend the "4+1" set, identified by Philippe Kruchten (Kruchten 1995) and Nick Rozanski and Woods (Rozanski and Woods 2005). Our catalogue contains seven core security viewpoints: Logical, Process, Development, Physical, Deployment, Operational and Misuse Cases viewpoints as we can see in Figure 1.

The security logical viewpoint describes the objects or object models within the security architecture that support security behavioral requirements. The security process viewpoint describes the security architecture as a logical network of secure communicating processes. This viewpoint assigns each method of the object model to a thread of execution and captures concurrency and synchronization aspects of the security design. The security physical viewpoint maps software onto hardware and network elements and reflects the distributed aspect of security architecture. The security development viewpoint focuses on the static organization of the software in the security development environment and deals with issues of configuration management, security development assignments, security responsibilities, and countermeasures. The security deployment viewpoint describes the security environment which the system will be deployed into, including the fact of capturing the dependencies the system has on its runtime environment. The aim of the Security Operational viewpoint is to identify security system-wide strategies for addressing the operational concerns of the system's stakeholders and to identify solutions that address them.

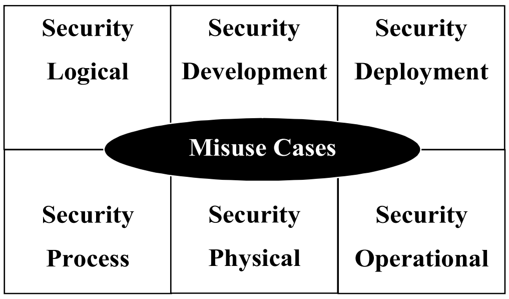

Figure 1: Our approach of Security Viewpoints.

Moreover, we are defining a new viewpoint's template extending the aforementioned template of IEEE 1471-2000 and we have added new sections in the context of security that are described as follows:

- Security properties to be addressed by the security policy on the basis of the security viewpoint's elements. We consider that the complete security policy of a security pattern is the aggregation of the security policies defined for each security viewpoint.
- Security metrics to be taken into account.
- Security procedures to be taken into consideration from this viewpoint; for instance, from the physical viewpoint, procedures to restore the physical node in which the security services defined by the pattern are running, or from the logical viewpoint, how to carry out the off-line exchange of key material between the involved parties.
- Best practices: for example, from the developer's viewpoint, techniques for secure programming, or from the physical viewpoint, topologies of secure networks.

5 SECURITY DESIGN SUBSYSTEM VIEWPOINT

Each aforementioned viewpoint can be divided into different viewpoints satisfying the interest of a particular stakeholder. A series of viewpoints is then used to elaborate the details of the general viewpoint. Selecting the security design subsystem viewpoint and considering the template IEEE 1471, we have defined this viewpoint as presented in Figure 2.

❶ **Abstract**. This viewpoint shows security module decomposition and the use between systems of software system. Each security module interprets itself as a subsystem to develop; therefore it is an entity in construction time, and can communicate with others security subsystems for completing its functionality. The decomposition continues until that each module or subsystem of security is allocated to a unique responsible of development or team.

❷ **Stakeholders and their concerns addressed.** Secure applications will be developed by (at least) three different roles: i) Application software developers that focus on the business logic; ii) Security providers that focus on the design and implementation of reusable frameworks of security logic; iii) Security engineers that implement the security policy for a particular application and focus on how the system is implemented from the perspective of security, and how security affects the system properties.

• Project managers, who must define work assignments, form teams, and formulate project plans and budgets and schedules; Maintainers, who are tasked with modifying the software elements; Testers and integrators who use the modules as their unit of work.

❸ **Elements, Relations, Properties, and Constraints.**

• Security modules are units of implementation, and their decomposition in shorter modules, just as use dependencies exist between them.

• Relations between security modules can have the semantic associated 'is-part-of' or 'utilize'.

• The last level of subsystems called security design subsystems, defined in the views according to this viewpoint: i) Must be set of products of work of design assigned to different develop teams; ii) Security subsystems will correlate with the construction directories that will be developed, tested and handed over respective teams of development; iii) Following modality origins, the security subsystems must exhibit high cohesion and low coupling; iv) These subsystems will be the lower level entities for which the software architects team will need to define the interface.

❹ **Language(s) to Model/Represent Conforming Views.**

• The representation language used will be the UML and extensions for security aspects such as UMLSec (Jürjens 2001; Jürjens 2002) and SecureUML (Lodderstedt, Basin et al. 2002).

• Each module or subsystem of security will represent itself as a stereotyped UML packet with the reserved word <<subsystem>>, the use relations will show with <<uses>> and decomposition relations with nesting of UML packets.

• The interfaces that implement each system are modeled as UML interfaces and the name of the service to be included in each interface corresponds with the names of the use cases defined at the abstraction level of "Goal Summarize" (CockBurn 2000) for each subsystem.

• The design subsystem included into views according to this viewpoint will declare a realization of one or more interfaces whose methods correspond with use cases at the abstraction level "User Goal" specified in the model of use cases of this design subsystem.

❺ **Applicable Evaluation/Analysis Techniques and Consistency/Completeness Criteria**. Revision checking of the fact that the different development groups of form understand the context of the subsystem that they are going to develop (where system comes from) so as the interfaces with other design subsystems. Some analysis and evaluation methods are described by Ronald Wassermann (Cheng, Konrad et al. 2003) and Jan Jürgens (Deubler, Grünbauer et al. 2004).

❻ **Viewpoint Source**. Viewpoint of Design Subsystem (Garlan and Anthony 2002)

Figure 2: Security Design Subsystem Viewpoint.

6 EXAMPLE: 'QoP' PATTERN

Due to space constraints and because actually we are working and researching in this issue, we will do a brief description of the 'QoP' pattern from security logical view that includes a views' packet with the information of decomposition in security design subsystem, attempting describe the main object from the security design subsystem viewpoint.

From this description of viewpoint, we will attempt to describe, following the viewpoint of design subsystem, the 'QoP' security pattern that offers Quality of Protection security service which address message confidentiality, message integrity and message authentication.

This view allows the security software architects to communicate security development team boundaries, communicate and negotiate interfaces between security development teams, and communicate with security project management.

Each subsystem must implement an interface that is used by the rest of elements that need the service that the owner subsystem of the interface offers. This subsystem implements the interface 'QoPSecurityService' with the methods protect and verifyProtection, as we can see in Figure 3.

These two methods are used by the elements for applying the service to outbound/inbound messages according to policy established for this service. This subsystem has relations with others subsystems or interfaces, as it can be the relation with the subsystem Security Token Manager, through its interface *SecurityTokenManager* that manages security tokens and they can be implemented using WS-Trust, XKMS with PKI infrastructure, etc., established in its security policy; it has relation with the subsystem Message Confidentiality Manager, through its interface *ConfidentialityManager* that cipher or decipher the message offering message confidentiality service using XML Encryption; and it has relation with the subsystem Message Integrity Manager, through its interface Integrity*Manager* that check and protect the message offering message integrity service using XML Digital Signature. Also it can have relation with the subsystem Security Policy Service, this is optional, where it would manage all policies associated to the services offered by the system. We have said that this is optional because policies can be managed and implemented into of the own subsystem (i.e. 'QoP' subsystem) without to be relation with this subsystem.

Other possible relation, non obligatory, is the relation between 'QoP' Security Service subsystem and an Alarm subsystem, using a common protocol of alarms (CAP, Common Alerting Protocol) establishing an alarms system in the application, communicating elements with others, indicating an event or an alarm generated and sent to others subsystems.

7 CONCLUSIONS

It is important to document a software architecture because first of all it serves to introduce people to the system; secondly, it serves as a vehicle for communication among stakeholders, and finally it is use as a basis for system analysis. Moreover, a documented architecture is crucial for understanding its main characteristics, its functionality, its components and connections, its behaviour, and so on. It will be important to describe and define the main characteristics of architectural patterns for stakeholders to be able to use and analyze the pattern at the time of integrating it into either the design of the application, or the design of the whole architecture.

In this paper, we have described an architectural pattern from viewpoints attempting to provide a wider vision of its main characteristics, its design, connections, elements, interfaces, implementation, classes and behavior, putting the description of the pattern conforming to the template as future work.

Our intention is not only to define security architectural patterns by means of a views template and a viewpoint template but also to recommend ANSI/IEEE 1471-2000 (IEEE 2000), that provides guidance for choosing the best set of views to document. We have defined a viewpoints' catalogue and we have added and we are adding new elements or sections to the viewpoint template of IEEE 1471-2000 standard. Our research concentrates in defining

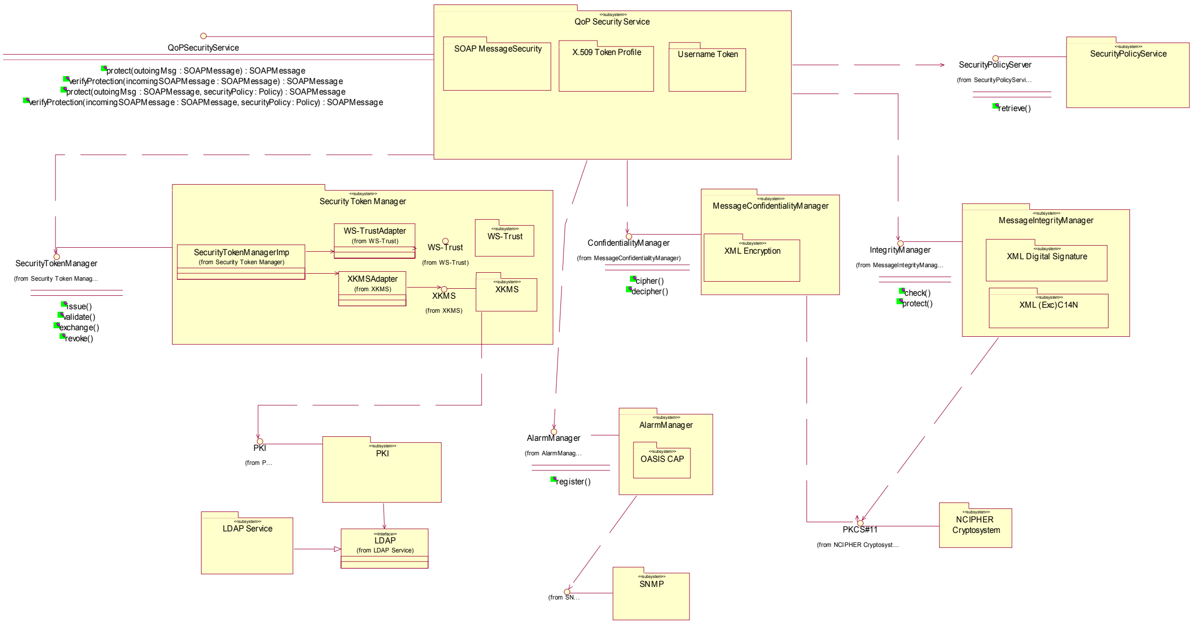

Figure 3: Relations between subsystems and interfaces of the 'QoP' Pattern.

a library of viewpoints adhered to IEEE 1471-2000 whose instances are the views that we can define following the documentation IEEE 1471-2000 (IEEE 2006). In this way, we could have a library of viewpoints to document security architectural patterns.

ACKNOWLEDGEMENTS

This research is part of the following projects: DIMENSIONS (PBC-05-012-2) and MISTICO (PBC06-0082) financed by FEDER and by the "Consejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain), and CALIPO (TIC2003-07804-C05-03) granted by the "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (Spain).

REFERENCES

Artelsmair, C. and Wagner, R. (2003). Towards a Security Engineering Process. The 7th World Multiconference on Systemics, Cybernetics and Informatics, Orlando, Florida, USA.

Bachmann, F., Bass, L., et al. (2000). Software Architecture Documentation in Practice: Documenting Architectural Layers**: Pgs.** 46.March 2000

Bass, L., Clements, P., et al., Eds. (2003). Software Architecture in Practice, Addison-Wesley.

Berry, C. A., Carnell, J., et al. (2002). Chapter 5: Patterns Applied to Manage Security. J2EE Design Patterns Applied.

Buschmann, F., Meunier, R., et al. (1996). Pattern-Oriented Software Architecture: A System of Patterns, John Wiley & Sons.

CockBurn, A. (2000). Writing Effective Use Cases, Addison-Wesley Professional.

Cheng, B. H. C., Konrad, S., et al. (2003). Using Security Patterns to Model and Analyze Security Requirements. High Assurance Systems Workshop (RHAS 03) as part of the IEEE Joint International Conference on Requirements Engineering (RE 03), Monterey Bay, CA, USA.

Deubler, M., Grünbauer, J., et al. (2004). Sound Development of Secure Service-based Systems. Second International Conference on Service Oriented Computing (ICSOC), New York City, USA, ACM Press.

Garlan, J. and Anthony, R. (2002). Large-Scale Software Architecture, John Wiley & Sons.

IEEE (2000). Recommended Practice for Architectural Description of Software-Intensive Systems (IEEE Std 1471-2000). New York, NY, Institute of Electrical and Electronics Engineers**: Pgs.** 29.01-May-2000

IEEE. (2006, last saved: March 21, 2006). "Software Architecture Document (SAD)." from www.sei.cmu.edu/architecture/SAD_template2.dot.

Jürjens, J. (2001). Towards Secure Systems Development with UMLsec. International Conference of Fundamental Approaches to Software Engineering (FASE/ETAPS), Genoa, Italy, Springer-Verlag.

Jürjens, J. (2002). UMLsec: Extending UML for Secure Systems Development. 5th International Conference on the Unified Modeling Language (UML), 2002, Dresden, Germany, Springer.

Kruchten, P. (1995). "Architectural Blueprints - The "4+1" View Model of Software Architecture." IEEE Software **12**(6): 42-50.

Lodderstedt, T., Basin, D., et al. (2002). SecureUML: A UML-Based Modeling Language for Model-Driven Security. 5th International Conference on the Unified Modeling Language (UML), 2002, Dresden, Germany, Springer.

Rozanski, N. and Woods, E. (2005). Software Systems Architecture: Working With Stakeholders Using Viewpoints and Perspectives, Addison Wesley Professional.

Schumacher, M., Fernandez, E. B., et al. (2005). Security Patterns, John Wiley & Sons.

Schumacher, M. and Roedig, U. (2001). Security Engineering with Patterns. 8th Conference on Patterns Lnaguages of Programs, PLoP 2001, Monticello, Illinois, USA.

Steel, C., Nagappan, R., et al. (2005). Core Security Patterns, Prentice Hall PTR.

Yoder, J. and Barcalow, J. (1997). Architectural Patterns for Enabling Application Security. 4th Conference on Patterns Language of Programming, PLop 1997, Monticello, Illinois, USA.