ARES Conference
International Conference on Availability, Reliability and Security

ARES 2017

Proceedings of the 12th International Conference on Availability, Reliability and Security

August 29 – September 1, 2017
Università degli Studi Mediterranea di Reggio Calabria, Italy

Organized by

SBA Research

Università degli Studi di Reggio Calabria
Mediterranea

The Association for Computing Machinery
2 Penn Plaza, Suite 701
New York New York 10121-0701

ACM ISBN: 978-1-4503-5257-4

ARES Full Papers

ARES Full I – Best Paper

A1: Security Proofs for Participation Privacy, Receipt-Freeness and Ballot Privacy for the Helios Voting Scheme Bulletin Board for the Helios Voting Scheme

David Bernhard (University of Bristol, UK), Oksana Kulyk and Melanie Volkamer (TU Darmstadt, Germany)

A2: VMAttack: Deobfuscating Virtualization-Based Packed Binaries

Anatoli Kalysch, Johannes Götzfried and Tilo Müller (Friedrich-Alexander University Erlangen-Nürnberg, Germany)

A3: A Non-Parametric Model for Accurate and Provably Private Synthetic Data Sets

Jordi Soria-Comas and Josep Domingo-Ferrer (Universitat Rovira i Virgili, Spain)

ARES Full II – Applications

A4: Continuous Biometric Verification for Non-Repudiation of Remote Services

Enrico Schiavone, Andrea Ceccarelli and Andrea Bondavalli (University of Florence, Italy)

A5: Artificial Ambient Environments for Proximity Critical Applications

IIakovos Gurulian, Konstantinos Markantonakis, Raja Naeem Akram and Keith Mayes (Royal Holloway, University of London, UK)

A6: Using Markov Chains to Model Sensor Network Reliability

Tom Arjannikov, Simon Diemert, Sudhakar Ganti, Chloe Lampman and Edward Wiebe (University of Victoria, Canada)

ARES Full III- Trust

A7: Establishing Mutually Trusted Channels for Remote Sensing Devices Using Trusted Execution Environments

Carlton Shepherd, Raja Naeem Akram and Konstantinos Markantonakis (Royal Holloway, University of London, UK)

A8: Enabling Trust Assessement In Clouds-of-Clouds: A Similarity-Based Approach

Reda Yaich, Nora Cuppens and Frédéric Cuppens (IMT Atlantique, France)

A9: Reliable Behavioural Factors in the Information Security Context

Peter Mayer, Alexandra Kunz and Melanie Volkamer (TU Darmstadt, Germany)

ARES Full IV – Cryptography

A10: Secure Enrollment of Certificates Using Short PINs

Michael Rossberg and Markus Theil (Technische Universitaet Ilmenau, Germany)

A11: Secure Matrix Multiplication with MapReduce

Xavier Bultel, Radu Ciucanu, Matthieu Giraud and Pascal Lafourcade (LIMOS, Université Clermont Auvergne, France)

ARES Full V - Security Models and Data Accountability

A12: Systemic Risk Modeling and Evaluation through Simulation and Bayesian Networks

Andrea Tundis (TU Darmstadt, Germany), Alfredo Garro, Teresa Gallo, Domenico Sacca (University of Calabria, Italy), Simona Citrigno, Sabrina Graziano (Centro di Competenza ICT-SUD, Italy) and Max Mühlhäuser (TU Darmstadt, Germany)

A13: Attack Scenario Modeling for Smart Grids Assessment through Simulation

Andrea Tundis, Rolf Egert, Max Mühlhäuser (Technische Universität Darmstadt)

A14: A Blockchain-based Approach for Data Accountability and Provenance Tracking

Ricardo Neisse, Gary Steri and Igor Nai-Fovino (European Commission Joint Research Centre (JRC), Italy)

ARES Full VI Privacy I

A15: Measuring privacy in high dimensional microdata collections

Spyros Boukoros and Stefan Katzenbeisser (TU Darmstadt, Germany)

A16: Constrained PET Composition for Measuring Enforced Privacy

Sebastian Funke, Alexander Wiesmaier (AGT International, Germany) and Jörg Daubert (TU Darmstadt, Germany)

A17: A Holistic Approach for Privacy Protection in E-Government

Konstantinos Angelopoulos, Vasiliki Diamantopoulou, Haralambos Mouratidis, Michalis Pavlidis (University of Brighton, UK), Mattia Salnitri, Paolo Giorgini (University of Trento, Italy) and José R. Ruiz (Atos, Spain)

ARES Full VII Privacy II

A18: Memory carving can finally unveil your embedded personal data

Thomas Gougeon, Morgan Barbier, Patrick Lacharme (ENSICAEN – GREYC, France), Gildas Avoine (INSA Rennes France, UCL Belgium) and Christophe Rosenberger (ENSICAEN – GREYC, France)

A19: PPAndroid-Benchmarker: Benchmarking Privacy Protection Systems on Android Devices

Saeed Ibrahim Saeed Alqahtani and Shujun Li (University of Surrey, UK)

Ares Full VIII - Network Security and Intrusion Detection

A20: Lightweight Address Hopping for Defending the IPv6 IoT

Aljosha Judmayer, Johanna Ullrich, Georg Merzdovnik, Artemios Voyiatzis and Edgar Weippl (SBA Research, Austria)

A21: Quantifying the Spectrum of Denial-of-Service Attacks through Internet Backscatter

Norbert Blenn, Vincent Ghiette and Christian Doerr (TU Delft, Netherlands)

A22: On the Sequential Pattern and Rule Mining in the Analysis of Cyber Security Alerts

Martin Husák, Jaroslav Kašpar (Masaryk University Czech Republic), Elias Bou-Harb (Florida Atlantic University, USA) and Pavel Čeleda (Masaryk University, Czech Republic)

A23: SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream

Quentin Le Sceller, Elmouatez Billah Karbab, Mourad Debbabi (Concordia University, Canada) and Farkhund Iqbalb (Zayed University, United Arab Emirates)

ARES Short Papers

ARES Short I – Cryptography

A24: Searchable Encryption with Access Control
Nils Löken (Paderborn University, Germany)

A25: One-Message Unilateral Entity Authentication Schemes
Alfredo De Santis, Manuela Flores and Barbara Masucci (University of Salerno, Italy)

A26: Overcoming Limits of Blockchain for IoT Applications
Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo and Antonino Nocera (Universita' Mediterranea di Reggio Calabria, Italy)

ARES Short II - IoT and Security Engineering

A27: A Trust-based Resilient Routing Mechanism for the Internet of Things
Zeeshan Ali Khan (IIK, NTNU, Norway), Johanna Ullrich, Artemios Voyiatzis (SBA Research, Austria) and Peter Herrmann (IIK, NTNU, Norway)

A28: M2M-REP: Reputation of Machines in the Internet of Things
Muhammad Azad, Samiran Bag and Feng Hao (Newcastle University, UK)

A29: Which Security Requirements Engineering Methodology Should I Choose? Towards a Requirements Engineering-based Evaluation Approach
Sravani Teja Bulusu, Romain Laborde, Ahmad Samer Wazan, Francois Barrere and Abdelmalek Benzekri

A30: A Low-Cost UAV-Based Secure Location Verification Method
Marco Rasori, Pericle Perazzo and Gianluca Dini (University of Pisa, Italy)

ARES Short III - Security Monitoring and Analysis

A31: Incremental Clustering for Semi-Supervised Anomaly Detection applied on Log Data
Markus Wurzenberger, Florian Skopik, Roman Fiedler, Max Landauer, Philipp Greitbauer (AIT Austrian Institute of Technology, Austria) and Wolfgang Kastner (TU Vienna, Austria)

A32: Attack Potential in Impact and Complexity
Luca Allodi (Eindhoven University of Technology, Netherlands) and Fabio Massacci (University of Trento, Italy)

A33: Timestamp hiccups: Detecting manipulated filesystem timestamps on NTFS
Sebastian Neuner, Artemios Voyiatzis, Martin Schmiedecker and Edgar Weippl (SBA Research, Austria)

A34: SensorBuster: On Identifying Sensor Nodes in P2P Botnets
Shankar Karuppayah (Universiti Sains Malaysia, Malaysia), Leon Böck, Tim Grube (TU Darmstadt, Germany), Selvakumar Manickam (Universiti Sains Malaysia, Malaysia), Max Mühlhäuser (TU Darmstadt, Germany) and Mathias Fischer (Universität Hamburg, Germany)

ARES Short IV - Applications

A35: Investigating User Comprehension and Risk Perception of Apple's Touch ID Technology
Yousra Javed, Mohamed Shehab and Emmanuel Bello Ogunu (University of North Carolina Charlotte, USA)

A36: C'MON : Monitoring the Compliance of Cloud Services to Contracted Properties
Soha Albaghdady, Stefan Winter, Ahmed Taha, Heng Zhang and Neeraj Suri (Tu Darmstadt, Germany)

A37: A Cloud-Based Compilation and Hardening Platform for Android Apps
Marcel Busch, Mykola Protsenko and Tilo Müller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

A38: Go with the -Bitcoin- Flow, with Visual Analytics
Soha Albaghdady, Stefan Winter, Ahmed Taha, Heng Zhang and Neeraj Suri (TU Darmstadt, Germany)

FARES 2017

FARES I -Critical Infrastructures and Cyber2Physical

A39: Integrating Reactive Cloud Applications in SERECA
Luigi Romano (Uniparthenope, Italy), Giovanni Mazzeo (Uniparthenope, Italy) and Martijn Verburg (jClarity, Italy)

A40: Anomaly-Based Detection and Classification of Attacks in Cyber-Physical Systems
Philipp Kreimel (Fachhochschule St. Pölten, Austria), Oliver Eigner (Fachhochschule St. Pölten, Austria), Paul Tavolato (Fachhochschule St. Pölten, Austria)

FARES II- Identity Management and Access Control

A41: Authentication Shutter: Alternative Countermeasure against Password Reuse Attack by Availability Control
Tetsuji Takada (The University of Electro-Communications, Japan)

A42: Insider Misuse Attribution using Biometrics
Abdulrahman Alruban (University of Plymouth, UK), Nathan Clarke (University of Plymouth, UK), Fudong Li (University of Plymouth, UK), Steven Furnell (University of Plymouth, UK)

A43: k-rAC – a Fine-Grained k-Resilient Access Control Scheme for Distributed Hash Tables
Olga Kieselmann (University of Kassel, Germany), Arno Wacker (University of Kassel, Germany), Gregor Schiele (University of Duisburg-Essen, Germany)

A44: Efficient ID-based Designated Verifier Signature
Olivier Blazy (Université de Limoges, France), Emmanuel Conchon (XLIM, France), Paul Germouty (Université de Limoges, France), Amandine Jambert (CNIL, France)

FARES III- Code Security and Privacy

A45: bin2llvm: Analysis of Binary Programs Using LLVM Intermediate Representation
Kevin Kirchner (University of Applied Sciences Upper Austria, Austria), Stefan Rosenthaler (University of Applied Sciences Upper Austria, Austria)

A46: Security Analysis of Cordova Applications in Google Play
Michiel Willocx (KU Leuven, TCG, Belgium), Jan Vossaert (KU Leuven, TCG, Belgium), Vincent Naessens (KU Leuven, TCG, Belgium)

A47: Security and Privacy Implications of NFC-enabled Contactless Payment Systems

Nicholas Akinyokun (The University of Melbourne, Melbourne, Australia), Vanessa Teague (The University of Melbourne, Melbourne, Australia)

A48: Microblogging in a Privacy-Preserving way

Nikolaos Karvelas (TU Darmstadt, Germany), Marius Senftleben (TU Darmstadt, Germany), Stefan Katzenbeisser (TU Darmstadt, Germany)

FARES IV - Security Models and Methods

A49: Provisioning Software with Hardware-Software Binding

Robert Lee (Royal Holloway, University of London, UK), Konstantinos Markantonakis (Royal Holloway, University of London, UK), Raja Naeem Akram (Royal Holloway, University of London, UK)

A50: Victim Communication Stack: A flexible model to select the Human Attack Vector

Enrico Frumento (Cefriel, Italy), Angelo Consoli (SUPSI, Italy), Federica Freschi (Cefriel, Italy), Davide Andreoletti (SUPSI, Italy)

A51: Fully threshold broadcast encryption

Sigurd Eskeland (Norwegian Computing Center, Norway)

A52: Adaptive Resource Management Enabling Deception (ARMED)

Partha Pal (Raytheon BBN Technologies, USA), Nate Soule, (Raytheon BBN Technologies, USA), Nate Lageman (Raytheon BBN Technologies, USA), Shane Clark (Raytheon BBN Technologies, USA), Marco Carvalho (Harris Institute for Assured Information, Florida Institute of Technology, USA), Adrian Granados (Harris Institute for Assured Information, Florida Institute of Technology, USA), Anthony Alves (Harris Institute for Assured Information, Florida Institute of Technology, USA)

WSDF 2017

WSDF I

A53: Forensic Image Inspection Assisted by Deep Learning

Felix Mayer (Fraunhofer Institute for Secure Information Technology SIT, Germany) and Martin Steinebach (Fraunhofer Institute for Secure Information Technology SIT, Germany)

WSDF II

A54: On the Usefulness of Compression-Models for Authorship Verification

Oren Halvani (Fraunhofer Institute for Secure Information Technology SIT, Germany), Christian Winter (Fraunhofer Institute for Secure Information Technology SIT, Germany) and Lukas Graner (Fraunhofer Institute for Secure Information Technology SIT, Germany)

A55: Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)

Tanveer Zia (Charles Sturt University, Australia), Peng Liu (Pennsylvania State University, USA) and Weili Han (Fudan University, China)

A56: Forensic State Acquisition from Internet of Things (FSIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition

Christopher Meffert (University of New Haven, USA), Devon Clark (University of New Haven, USA), Ibrahim Baggili (University of New Haven, USA) and Frank Breitinger (University of New Haven, USA)

IWSMA 2017

IWSMA I

A57: The Demon is in the Configuration: Revisiting Hybrid Mobile Apps Configuration Model

Abeer Aljarrah (University of North Carolina at Charlotte, USA) and Mohamed Shehab (University of North Carolina at Charlotte, USA)

A58: Quantitative Dynamic Taint Analysis of Privacy Leakage in Android Arabic Apps

Ayman Youssef (Nile University, Egypt) and Ahmed F. Shosha (Nile University, Egypt)

A59: Learning Android Malware

Khanh-Huu-The Dam (University Paris Diderot & LIPN, France) and Tayssir Touili (LIPN, CNRS & University Paris 13, France)

IWCC 2017

IWCC I

A60: Type Me the Truth! Detecting Deceitful Users via Keystroke Dynamics

Merylin Monaro (University of Padua, Italy), Riccardo Spolaor (University of Padua, Italy), Qianqian Li (University of Padua, Italy), Mauro Conti (University of Padua, Italy), Luciano Gamberini (University of Padua, Italy) and Giuseppe Sartori (University of Padua, Italy

A61: Resource Hints in HTML5: A New Pandora's Box of Security Nightmares

Natalija Vlajic (York University, Canada)

IWCC II

A62: A Comparative Study on the Scalability of Dynamic Group Key Agreement Protocols

Orhan Ermis (Bogazici University, Turkey), Serif Bahtiyar (Bogazici University, Turkey), Emin Anarım (Bogazici University, Turkey) and Mehmet Ufuk Caglayan (Bogazici University, Turkey)

A63: Secure and Efficient Data Sharing with Attribute-based Proxy Re-encryption Scheme

Alberto Trombetta (Insubria University, Italy) and Masoomeh Sepheri (Università degli Studi di Milano, Italy)

SAW 2017

SAW I

A64: Towards Semi-automated Detection of Trigger-based Behavior for Software Security Assurance

Dorottya Papp (CrySyS Lab, Dept. of Networked Systems and Services, BME, Hungary), Levente Buttyán (CrySyS Lab, Dept. of Networked Systems and Services, BME, Hungary) and Zhendong Ma (Center of Digital Safety and Security, Austrian Institute of Technology, Austria)

A65: Protection of personal data in security alert sharing platforms

Václav Stupka (Masaryk University, Czech Republic), Martin Horák (Masaryk University, Czech Republic) and Martin Husák (Masaryk University, Czech Republic)

A66: SAFE and Secure: Deeply Integrating Security in a New Hazard Analysis
Sam Procter (Software Engineering Institute, Carnegie Mellon University, USA), Eugene Vasserman (Kansas State University, USA) and John Hatcliff (Kansas State University, USA)

A67: On Using TLS to Secure In-Vehicle Networks
Daniel Zelle (Fraunhofer SIT, Germany), Christoph Krauß (Fraunhofer SIT, Germany), Hubert Strauß (Audi Electronics Venture GmbH, Germany) and Karsten Schmidt (Audi AG, Germany)

SSE 2017

SSE I - DevSecOps and cloud computing

A68: Identification of Dependency-based Attacks on Node.js
Brian Pfretzschner (TU Darmstadt, Germany) and Lotfi Ben Othmane (Iowa State University, USA)

A69: DevOps for Better Software Security in the Cloud
Martin Gilje Jaatun, Daniela Soares Cruzes, and Jesus Luna

A70: Implementing Secure DevOps assessment for highly regulated environments.
Hasan Yasar (CMU, USA)

SSE II - Agile secure software development

A71: DoS Attacks on Controller Area Networks by Fault Injections from the Software Layer
Pal-Stefan Murvay (Politehnica University of Timisoara, Romania), Bogdan Groza (Politehnica University of Timisoara, Romania)

A72: Source Code Patterns of SQL Injection Vulnerabilities
Felix Schuckert (HTWG Konstanz, Germany) Basel Katt (Norwegian Information Security laboratory, Norway), Hanno Langweg (HTWG Konstanz, Germany)

A73: Towards a Secure SCRUM Process for Agile Web Application Development
Patrik Maier (Graz University of Technology,Austria), Zhendong Ma (Austrian Institute of Technology, Austria), Roderick Bloem (Graz University of Technology, Austria)

A74: Busting a Myth: Review of Agile Security Engineering Methods
Kalle Rindell (University of Turku, Finland), Sami Hyrynsalmi (Tampere University of Technology, Finland), Ville Leppänen (University of Turku, Finland)

WMA 2017

WMA I - Malware detection

A75: An Approach to Botnet Malware Detection Using Nonparametric Bayesian Methods
Joseph Divita(US Department of Defence, SPAWAR Systems Center Pacific, USA) and Roger Hallman (US Department of Defense, SPAWAR Systems Center Pacific, Cybersecurity S&T Branch, USA)

A76: Malware and Formal Methods
Fabio Martinelli (Institute for Informatics and Telematics, CNR, Italy), Francesco Mercaldo (Institute for Infromatics and Telematics, CNR, Italy), Vittoria Nardone (University of Sannio, Italy) and Antonella Santone (University of Sannio, Italy)

A77: End-node Fingerprinting for Malware Detection on HTTPS Data

Tomáš Komárek (Czech Technical University in Prague, Czech Republic) and Petr Somol (Cisco Systems, Inc., Czech Republic)

WMA II - Defensive technologies

A78: How to Ensure Bad Quality in Metal Additive Manufacturing: In-Situ Infrared Thermography from the Security Perspective

Andrew Slaughter (University of South Alabama, USA), Mark Yampolskiy (University of South Alabama, USA), Manyalibo Matthews (Lawrence Livermore National Laboratory, USA), Wayne E. King (Lawrence Livermore National Laboratory, USA), Gabe Guss (Lawrence Livermore National Laboratory, USA) and Yuval Elovici (Ben-Gurion University, Israel)

A79: Popularity-based Detection of Domain Generation Algorithms

Jasper Abbink (TU Delft, Netherlands) and Christian Doerr (TU Delft, Netherlands)

A80: JSDES – An Automated De-Obfuscation System for Malicious JavaScript

Moataz Abdel Khalek (University Nile, Egypt) and Ahmed Shosha (University Nile, Egypt)

CUING 2017

CUING I

A81: Are Network Covert Timing Channels Statistical Anomalies?

Félix Iglesias Vázquez and Tanja Zseby (Institute of Telecommunication, TU Wien)

A82: FROST – Anti-Forensics Digital-Dead-DROp Information Hiding RobuST to Detection & Data Loss with Fault-tolerance

Avinash Srinivasan (Temple University, USA), Hunter Dong (Temple University, USA) and Angelos Stavrou (George Mason University, USA).

A83: A New Data-Hiding Approach for IP Telephony Applications with Silence Suppression

Sabine Schmidt (FernUniversitaet in Hagen, Germany), Wojciech Mazurczyk (Warsaw University of Technology, Poland), Joerg Keller (FernUniversitaet in Hagen, Germany) and Luca Caviglione (National Research Council of Italy, Italy)

CUING II

A84: REMI: A Reliable and Secure Multicast Routing Protocol for IoT Networks

Mauro Conti (University of Padova, Italy), Pallavi Kaliyar (University of Padova, Italy) and Chhagan Lal (University of Padova, Italy)

A85: Machine Learning Approach for Detection of nonTor Traffic

Elike Hodo (University of Strathclyde, UK), Xavier Bellekens (University of Abertay, Dundee, UK, Ephraim Iorkyase (University of Strathclyde, UK), Andrew Hamilton (University of Strathclyde, UK), Christos Tachtatzis (University of Strathclyde, UK) and Robert Atkinson (University of Strathclyde, UK)

A86: Investigating the darknet: Legal limitations in Slovenian legal system

Anze Mihelic (Faculty of Criminal Justice and Security, University of Maribor, Slovenia), Blaž Markelj (Faculty of Criminal Justice and Security, University of Maribor, Slovenia), Igor Bernik (Faculty of Criminal Justice and Security, University of Maribor, Slovenia) and Sabina Zgaga (Constitutional Court of the Republic of Slovenia, Slovenia)

SECPID 2017

SECPID I

A87: Position Paper: The Past, Present, and Future of Sanitizable and Redactable Signatures
Arne Bilzhause (Uni Passau, Germany), Henrich C. Pöhls (Uni Passau, Germany) and Kai Samelin (TU Darmstadt & IBM Research, Switzerland)

A88: The Archistar Secret-Sharing Backup Proxy
Andreas Happe (Austrian Institute of Technology, Austria), Florian Wohner (Austrian Institute of Technology, Austria) and Thomas Loruenser (Austrian Institute of Technology, Austria)

A89: Orchestrating Privacy Enhancing Technologies and Services with BPM Tools
Nicolás Notario, Alberto Crespo, Eduardo González Real, Eleonora Ciceri, Ilio Catallo, and Sauro Vicini

SECPID II

A90: Towards the Adoption of Secure Cloud Identity Services
Alexandros Kostopoulos (Hellenic Telecommunications Organization R&D, Greece), Evangelos Sfakianakis (Hellenic Telecommunications Organization R&D, Greece), Ioannis Chochliouros (Hellenic Telecommunications Organization R&D, Greece), John-Sören Pettersson (Karlstad University, Sweden), Stephan Krenn (Austrian Institute of Technology, Austria), Welderufael Tesfay (Goethe University Frankfurt, Germany), Andrea Migliavacca (Lombardia Informatica S.p.A., Italy) and Felix Hörandner (Graz University of Technology, Austria)

A91: Towards a Model of User-centered Privacy Preservation
Paul Grace (University of Southampton, UK) and Mike Surridge (University of Southampton, UK)

A92: NEXTLEAP: Decentralizing Identity with Privacy for Secure Messaging
Harry Halpin (World Wide Web Consortium, UK)

SECPID III

A93: Self-healing Multi-Cloud Application Modelling
Erkuden Rios (Tecnalia Research & Innovation, Spain), Maria Carmen Palacios (Tecnalia Research & Innovation, Spain) and Eider Iturbe (Tecnalia Research & Innovation, Spain)

A94: Application of the holistic Data Privacy and Security Framework PaaSword
Sebastian Thomas Schork (CAS Software AG, Germany), Antonia Schwichtenberg (CAS Software AG, Germany), Spiros Alexakis (CAS Software AG, Germany) and George Moldovan (Siemens, Romania)

S-CI 2017

S-CI I - CyberSecurity and Critical Infrastructures

A95: Rolling DICE – Lightweight Remote Attestation for COTS IoT Hardware
Lukas Jäger (Fraunhofer Institute for Secure Information Technology SIT, Germany), Richard Petri (Fraunhofer Institute for Secure Information Technology SIT, Germany), Andreas Fuchs (Fraunhofer Institute for Secure Information Technology SIT, Germany)

A96: ZONESEC: built-in cyber-security for wide area surveillance system
Aljosa Pasic (Atos, Spain), Jose-Ramon Martinez-Salio (Atos, Spain), Susana Gonzalez Zarzosa (Atos, Spain)

A97: Protecting Future Maritime Communication

Karin Bernsmed (SINTEF, Norway), Christian Frøystad (SINTEF, Norway), Per Håkon Meland (SINTEF, Norway)

S-CI II - Critical Infrastructure Systems CyberSecurity Tools

A98: Using Ciphers for Failure Recovery in ITS Systems

Mustafa Ayoob (TU-BS, Germany), Wael Adi (TU-BS, Germany), Vassilis Prevelakis (TU-BS, Germany)

A99: Towards DDoS Attack Resilient Wide Area Monitoring Systems

Kubilay Demir (TU Darmstadt, Germany), Neeraj Suri (TU Darmstadt, Germany)

A100: Anomaly Detection for Simulated IEC-60870-5-104 Traffic

Ersi Hodo (Fachhochschule St. Pölten, Austria), Stepan Grebeniuk (Fachhochschule St. Pölten, Austria), Henri Ruotsalainen (Fachhochschule St. Pölten, Austria), Paul Tavolato (Fachhochschule St. Pölten, Austria)

The 12th International Conference on Availability, Reliability and Security (ARES 2017)

Welcome Message from ARES Program Committee Co-Chairs and General Chair

It is our great pleasure to welcome you to the Twelfth International Conference on Availability, Reliability and Security (ARES 2017).

The Twelfth International Conference on Availability, Reliability and Security (ARES 2017) brings again together researchers and practitioners in the field of dependability and cybersecurity. ARES 2017 highlights the various aspects of this very important field, following the tradition of previous ARES conferences, again with a special focus on the crucial linkage between availability, reliability, security and privacy. This year we are very happy to welcome well-known keynote speakers: Andrea Servida (Head of Unit DG CONNECT – H4 "eGovernment and Trust", European Commission, Belgium), Neil D. Lawrence (University of Sheffield and Amazon, UK) and Marta Milo (University of Sheffield, UK).

From the many submissions, we have selected the 23 best ones as full paper. The quality of submissions has steadily improved over the last years and the conference officers sometimes faced a difficult decision when selecting which papers should be accepted. This year's acceptance rate for full papers is only 24, 21%. In addition, several workshops and short papers are included in the program and show intermediate results of ongoing research projects and offer interesting starting points for discussions. Putting together ARES 2017 was a team effort. We first thank the authors for providing the content of the program. We are grateful to the program committee, which worked very hard in reviewing papers and providing feedback for authors. Finally, we thank all workshop chairs for their efforts in organizing interesting workshop sessions.

The symbolic link between the acronym of the conference (ARES) and the Ancient Greeks is strengthened this year. The god of war and double-faced liar, according to what Zeus said to him after the battlefield at Troy, evokes indeed the intrinsic unreliability of computer systems in hostile environments, which is the underlying mainstream of the conference. The venue of the 2017 edition of ARES has a strong relationship with this ancient world. Indeed, Reggio Calabria is one of the oldest Greek colonies, and one of the most important *Polis* of Magna Graecia.

We would like to thank the University Mediterranea of Reggio Calabria for hosting ARES 2017!

Special thanks goes to the Sponsors of the conference: Palo Alto Networks and Poste Italiane, our Gold Sponsors, and our Silver Sponsors Lutech, Innovery, Progetti di Impresa and Naos Evolution.

Enjoy ARES 2017 and Reggio Calabria!

Mathias Fischer
Universität Hamburg, Germany

Max Mühlhauser
TU Darmstadt, Germany

Francesco Buccafurri
Università degli Studi Mediterranea di Reggio Calabria, Italy

Committee ARES 2017

Steering Committee Chairpersons
Edgar Weippl*, SBA Research, Austria*
A Min Tjoa, *TU Vienna, Austria*

General Chair 2017
Francesco Buccafurri*, Università degli Studi Mediterranea di Reggio Calabria, Italy*

Program Committee Chairs 2017
Mathias Fischer, *Universität Hamburg, Germany*
Max Mühlhäuser, *TU Darmstadt, Germany*

Workshop Chair 2017
Edgar Weippl, *SBA Research, Austria*

Program Committee 2017

- Isaac Agudo Ruiz, *University of Malaga, Spain*
- Todd R. Andel, *University of South Alabama, US*
- Abdelmalek Benzekri, *University of Toulouse, France*
- Francesco Buccafurri, *University of Reggio Calabria, Italy*
- Lasaro Camargos, *Federal University of Uberlândia ,Brazil*
- Jordi Castellà-Roca, *Rovira i Virgili University of Tarragona, Spain*
- David Chadwick, *University of Kent, UK*
- Nathan Clarke, *Plymouth University, UK*
- Marijke Coetzee, *University of Johannesburg, South Africa*
- Jörg Daubert, *TU Darmstadt, Germany*
- Luca De Cicco, *Politecnico di Bari, Italy*
- José Maria de Fuentes, *Carlos III University of Madrid, Spain*
- Pavlos Efraimidis, *Democritus University of Thrace, Greece*
- Dominik Engel, *Salzburg University of Applied Sciences, Austria*
- Christian Engelmann, *Oak Ridge National Laboratory, US*
- Hannes Federrath, *University of Hamburg, Germany*
- Christophe Feltus, *Luxembourg Institute of Science and Technology, Luxembourg*
- Steven Furnell, *Plymouth University, UK*
- Joaquin Garcia-Alfaro, *Télécom SudParis, France*
- Karl Goeschka, *Vienna University of Technology, Austria*
- Nico Golde, *Comsecuris UG, Germany*
- Lorena Gonzalez-Manzano, *Carlos III University of Madrid, Spain*
- Bogdan Groza, *Politehnica University of Timisoara, Romania*
- Sheikh Mahbub *Habib, TU Darmstadt, Germany*
- Dominik Herrmann, *University Hamburg, Germany*
- Martin Gilje Jaatun, *SINTEF, Norway*
- Jan Jürjens, *TU Dortmund and Fraunhofer ISST, Germany*
- Shankar Karuppayah, *National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Malaysia*

- Sokratis K. Katsikas, *NTNU: Norwegian University of Science and Technology, Norway*
- Peter Kieseberg, *SBA Research, Austria*
- Ezzat Kirmani, *St. Cloud State University, US*
- Ryan Ko*, University of Waikato, New Zealand*
- Ralf Kuesters, *University of Stuttgart, Germany*
- Romain Laborde, *University of Toulouse, France*
- Costas Lambrinoudakis, *University of Piraeus, Greece*
- Shujun Li, *University of Surrey, UK*
- Giovanni Livraga, *Universita' degli Studi di Milano, Italy*
- Javier Lopez, *University of Malaga, Spain*
- Konstantinos Markantonakis, *Royal Holloway, University of London, UK*
- Keith Martin, *Royal Holloway, University of London, UK*
- Barbara Masucci, *University of Salerno, Italy*
- Srdjan Matic, *Università degli studi di Milano, Italy*
- Ioannis Mavridis, *University of Macedonia, Greece*
- Mattia Monga, *Universita` degli Studi di Milano, Italy*
- Haralambos Mouratidis, *University of Brighton, UK*
- Thomas Moyer, *MIT Lincoln Laboratory, US*
- Sebastian Neuner*, SBA Research, Austria*
- Thomas Nowey, *Krones AG, Germany*
- Christoforos Ntantogian*, University of Piraeus, Greece*
- Jaehong Park, *University of Alabama in Huntsville, US*
- Günther Pernul, *University of Regensburg, Germany*
- Andreas Peter, *University of Twente, Netherlands*
- Sriram Raghavan, *University of Melbourne, Australia*
- Stefanie Rinderle-Ma, *Vienna University, Austria*
- Stefanie Roos, *University of Waterloo, Canada*
- Michael Roßberg, *TU Ilmenau, Germany*
- Volker Roth, *Freie Universität Berlin, Germany*
- Giovanni Russello, *University of Auckland, New Zealand*
- Luis Enrique Sánchez Crespo, *University of Castilla-la Mancha, Spain*
- Mark Scanlon, *University College Dublin, Ireland*
- Sebastian Schinzel, FH Münster, *Germany*
- Jörn-Marc Schmidt, *secunet, Germany*
- Martin Schmiedecker, *SBA Research, Austria*
- Max Schuchard, *University of Minnesota, US*
- Stefan Schulte, *Vienna University of Technology, Austria*
- Daniele Sgandurra, *Royal Holloway, University of London, UK*
- Jon A. Solworth, *University of Illinois at Chicago, US*
- Mark Strembeck, *WU Vienna, Austria*
- Jakub Szefer, *Yale University, US*
- Oliver Theel, *Carl von Ossietzky Universität Oldenburg, Germany*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*

- Steven Van Acker, *Chalmers University, Sweden*
- Emmanouil Vasilomanolakis, *TU Darmstadt, Germany*
- Umberto Villano, *Universita' del Sannio, Italy*
- Corrado Aaron Visaggio, *Univeristà del Sannio, Italy*
- Artemios Voyiatzis, *SBA* Research, Austria
- Xiao Wang, Carnegie *Mellon University, US*
- Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
- Christos Xenakis, *University of Piraeus, Greece*
- Alec Yasinsac, *University of South Alabama, US*
- Nicola Zannone, *Eindhoven University of Technology, Netherlands*

ARES 2017 Program: Full Papers

ARES Full I – Best Paper

Security Proofs for Participation Privacy, Receipt-Freeness and Ballot Privacy for the Helios Voting Scheme Bulletin Board for the Helios Voting Scheme
David Bernhard (University of Bristol, UK), Oksana Kulyk and Melanie Volkamer (TU Darmstadt, Germany)

VMAttack: Deobfuscating Virtualization-Based Packed Binaries
Anatoli Kalysch, Johannes Götzfried and Tilo Müller (Friedrich-Alexander University Erlangen-Nürnberg, Germany)

A Non-Parametric Model for Accurate and Provably Private Synthetic Data Sets
Jordi Soria-Comas and Josep Domingo-Ferrer (Universitat Rovira i Virgili, Spain)

ARES Full II – Applications

Continuous Biometric Verification for Non-Repudiation of Remote Services
Enrico Schiavone, Andrea Ceccarelli and Andrea Bondavalli (University of Florence, Italy)

Artificial Ambient Environments for Proximity Critical Applications
IIakovos Gurulian, Konstantinos Markantonakis, Raja Naeem Akram and Keith Mayes (Royal Holloway, University of London, UK)

Using Markov Chains to Model Sensor Network Reliability
Tom Arjannikov, Simon Diemert, Sudhakar Ganti, Chloe Lampman and Edward Wiebe (University of Victoria, Canada)

ARES Full III- Trust

Establishing Mutually Trusted Channels for Remote Sensing Devices Using Trusted Execution Environments
Carlton Shepherd, Raja Naeem Akram and Konstantinos Markantonakis (Royal Holloway, University of London, UK)

Enabling Trust Assessement In Clouds-of-Clouds: A Similarity-Based Approach
Reda Yaich, Nora Cuppens and Frédéric Cuppens (IMT Atlantique, France)

Reliable Behavioural Factors in the Information Security Context
Peter Mayer, Alexandra Kunz and Melanie Volkamer (TU Darmstadt, Germany)

ARES Full IV – Cryptography

Secure Enrollment of Certificates Using Short PINs
Michael Rossberg and Markus Theil (Technische Universitaet Ilmenau, Germany)

Secure Matrix Multiplication with MapReduce
Xavier Bultel, Radu Ciucanu, Matthieu Giraud and Pascal Lafourcade (LIMOS, Université Clermont Auvergne, France)

ARES Full V - Security Models and Data Accountability

Systemic Risk Modeling and Evaluation through Simulation and Bayesian Networks
Andrea Tundis (TU Darmstadt, Germany), Alfredo Garro, Teresa Gallo, Domenico Sacca (University of Calabria, Italy), Simona Citrigno, Sabrina Graziano (Centro di Competenza ICT-SUD, Italy) and Max Mühlhäuser (TU Darmstadt, Germany)

Attack Scenario Modeling for Smart Grids Assessment through Simulation
Andrea Tundis, Rolf Egert, Max Mühlhäuser (Technische Universität Darmstadt)

A Blockchain-based Approach for Data Accountability and Provenance Tracking
Ricardo Neisse, Gary Steri and Igor Nai-Fovino (European Commission Joint Research Centre (JRC), Italy)

ARES Full VI Privacy I

Measuring privacy in high dimensional microdata collections
Spyros Boukoros and Stefan Katzenbeisser (TU Darmstadt, Germany)

Constrained PET Composition for Measuring Enforced Privacy
Sebastian Funke, Alexander Wiesmaier (AGT International, Germany) and Jörg Daubert (TU Darmstadt, Germany)

A Holistic Approach for Privacy Protection in E-Government
Konstantinos Angelopoulos, Vasiliki Diamantopoulou, Haralambos Mouratidis, Michalis Pavlidis (University of Brighton, UK), Mattia Salnitri, Paolo Giorgini (University of Trento, Italy) and José R. Ruiz (Atos, Spain)

ARES Full VII Privacy II

Memory carving can finally unveil your embedded personal data
Thomas Gougeon, Morgan Barbier, Patrick Lacharme (ENSICAEN – GREYC, France), Gildas Avoine (INSA Rennes France, UCL Belgium) and Christophe Rosenberger (ENSICAEN – GREYC, France)

PPAndroid-Benchmarker: Benchmarking Privacy Protection Systems on Android Devices
Saeed Ibrahim Saeed Alqahtani and Shujun Li (University of Surrey, UK)

Ares Full VIII - Network Security and Intrusion Detection

Lightweight Address Hopping for Defending the IPv6 IoT
Aljosha Judmayer, Johanna Ullrich, Georg Merzdovnik, Artemios Voyiatzis and Edgar Weippl (SBA Research, Austria)

Quantifying the Spectrum of Denial-of-Service Attacks through Internet Backscatter
Norbert Blenn, Vincent Ghiette and Christian Doerr (TU Delft, Netherlands)

On the Sequential Pattern and Rule Mining in the Analysis of Cyber Security Alerts
Martin Husák, Jaroslav Kašpar (Masaryk University Czech Republic), Elias Bou-Harb (Florida Atlantic University, USA) and Pavel Čeleda (Masaryk University, Czech Republic)

SONAR: Automatic Detection of Cyber Security Events over the Twitter Stream
Quentin Le Sceller, Elmouatez Billah Karbab, Mourad Debbabi (Concordia University, Canada) and Farkhund Iqbalb (Zayed University, United Arab Emirates)

ARES 2017 Program: Short Papers

ARES Short I – Cryptography

Searchable Encryption with Access Control
Nils Löken (Paderborn University, Germany)

One-Message Unilateral Entity Authentication Schemes
Alfredo De Santis, Manuela Flores and Barbara Masucci (University of Salerno, Italy)

Overcoming Limits of Blockchain for IoT Applications
Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo and Antonino Nocera (Universita' Mediterranea di Reggio Calabria, Italy)

ARES Short II - IoT and Security Engineering

A Trust-based Resilient Routing Mechanism for the Internet of Things
Zeeshan Ali Khan (IIK, NTNU, Norway), Johanna Ullrich, Artemios Voyiatzis (SBA Research, Austria) and Peter Herrmann (IIK, NTNU, Norway)

M2M-REP: Reputation of Machines in the Internet of Things
Muhammad Azad, Samiran Bag and Feng Hao (Newcastle University, UK)

Which Security Requirements Engineering Methodology Should I Choose? Towards a Requirements Engineering-based Evaluation Approach
Sravani Teja Bulusu, Romain Laborde, Ahmad Samer Wazan, Francois Barrere and Abdelmalek Benzekri

A Low-Cost UAV-Based Secure Location Verification Method
Marco Rasori, Pericle Perazzo and Gianluca Dini (University of Pisa, Italy)

ARES Short III - Security Monitoring and Analysis

Incremental Clustering for Semi-Supervised Anomaly Detection applied on Log Data
Markus Wurzenberger, Florian Skopik, Roman Fiedler, Max Landauer, Philipp Greitbauer (AIT Austrian Institute of Technology, Austria) and Wolfgang Kastner (TU Vienna, Austria)

Attack Potential in Impact and Complexity
Luca Allodi (Eindhoven University of Technology, Netherlands) and Fabio Massacci (University of Trento, Italy)

Timestamp hiccups: Detecting manipulated filesystem timestamps on NTFS
Sebastian Neuner, Artemios Voyiatzis, Martin Schmiedecker and Edgar Weippl (SBA Research, Austria)

SensorBuster: On Identifying Sensor Nodes in P2P Botnets
Shankar Karuppayah (Universiti Sains Malaysia, Malaysia), Leon Böck, Tim Grube (TU Darmstadt, Germany), Selvakumar Manickam (Universiti Sains Malaysia, Malaysia), Max Mühlhäuser (TU Darmstadt, Germany) and Mathias Fischer (Universität Hamburg, Germany)

ARES Short IV - Applications

Investigating User Comprehension and Risk Perception of Apple's Touch ID Technology
Yousra Javed, Mohamed Shehab and Emmanuel Bello Ogunu (University of North Carolina Charlotte, USA)

C'MON : Monitoring the Compliance of Cloud Services to Contracted Properties
Soha Albaghdady, Stefan Winter, Ahmed Taha, Heng Zhang and Neeraj Suri (Tu Darmstadt, Germany)

A Cloud-Based Compilation and Hardening Platform for Android Apps
Marcel Busch, Mykola Protsenko and Tilo Müller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

Go with the -Bitcoin- Flow, with Visual Analytics
Soha Albaghdady, Stefan Winter, Ahmed Taha, Heng Zhang and Neeraj Suri (TU Darmstadt, Germany)

The Workshops of the 12th International Conference on Availability, Reliability and Security (ARES 2017)

Welcome Message from ARES Workshop Chair

Welcome to the Workshops of the Twelfth International Conference on Availability, Reliability and Security (ARES 2017).

The workshops are central events for ARES as they provide an essential platform for researchers of various domains to present and discuss their current work and discuss work in progress. This year we can offer the conference attendees 8 workshops which range from “start-ups” to well-established ones supporting ARES the ninth year.

The succeeding listing comprises the workshops of ARES 2017:

- 12th International Workshop on Frontiers in Availability, Reliability and Security (FARES 2017)
- 10th International Workshop on Digital Forensics (WSDF 2017)
- 6th International Workshop on Security of Mobile Applications (IWSMA 2017)
- 6th International Workshop on Cyber Crime (IWCC 2017)
- 4th International Workshop on Software Assurance Workshop (SAW 2017)
- 3rd International Workshop on Agile Secure Software Development (SSE 2017)
- 2nd International Workshop on Malware Analysis (WMA 2017)
- 1st International Workshop on Criminal Use of Information Hiding (CUING 2017)

These workshops are organized each on specific topics and thus offer researchers the opportunity to learn from a rich multi-disciplinary experience. The Workshop Chair would like to thank the workshop organizers for their great efforts and hard work in proposing the workshop, selecting the papers, the interesting programs and for the arrangements of the workshops during the conference days.

We hope you enjoy the workshops programs and proceedings.

Edgar Weippl
ARES 2017 Workshop Chair
SBA Research, Austria

The 12th Workshop on Frontiers of Availability, Reliability and Security (FARES 2017)

Welcome Message from FARES Workshop Organizers

The 12th Workshop on Frontiers of Availability, Reliability and Security (FARES 2017) establishes an in-depth academic platform to exchange novel theories, designs, applications and on-going research results among researchers and practitioners in different Computing Dependability aspects, which emphasize the Practical Issues in Availability, Reliability and Security.

From the received submissions, we have selected the 14 best for presentation. These presentations have been grouped into 4 sessions. The first session deals with problems related to critical infrastructures and cyber-physical systems. The second session collects papers focusing on the topics of identity management and access control. The third session merges two important topics, which are code security and privacy. The last session presents models and methods for improving security.

We are very grateful to Prof. Andrea Bondavalli (University of Florence – Italy) for his Keynote talk.

Finally, our special thanks are due to Yvonne Poul and Bettina Bauer for their kind assistance and help.

Francesco Buccafurri
FARES 2017 Program Co-Chair
University of Reggio Calabria, Italy

Gianluca Lax
FARES 2017 Program Co-Chair
University of Reggio Calabria, Italy

The Workshop organizing committee

Antonio Azzarà, *University of Reggio Calabria, Italy*
Sofia Giuffrè, *University of Reggio Calabria, Italy*
Francesco Mazzacuva, *University of Reggio Calabria, Italy*
Serena Nicolazzo, *University of Reggio Calabria, Italy*
Antonino Nocera, *University of Reggio Calabria, Italy*

FARES 2017 Program

FARES I -Critical Infrastructures and Cyber2Physical

Integrating Reactive Cloud Applications in SERECA
Luigi Romano (Uniparthenope, Italy), Giovanni Mazzeo (Uniparthenope, Italy) and Martijn Verburg (jClarity, Italy)

Anomaly-Based Detection and Classification of Attacks in Cyber-Physical Systems
Philipp Kreimel (Fachhochschule St. Pölten, Austria), Oliver Eigner (Fachhochschule St. Pölten, Austria), Paul Tavolato (Fachhochschule St. Pölten, Austria)

FARES II- Identity Management and Access Control

Authentication Shutter: Alternative Countermeasure against Password Reuse Attack by Availability Control
Tetsuji Takada (The University of Electro-Communications, Japan)

Insider Misuse Attribution using Biometrics
Abdulrahman Alruban (University of Plymouth, UK), Nathan Clarke (University of Plymouth, UK), Fudong Li (University of Plymouth, UK), Steven Furnell (University of Plymouth, UK)

k-rAC – a Fine-Grained k-Resilient Access Control Scheme for Distributed Hash Tables
Olga Kieselmann (University of Kassel, Germany), Arno Wacker (University of Kassel, Germany), Gregor Schiele (University of Duisburg-Essen, Germany)

Efficient ID-based Designated Verifier Signature
Olivier Blazy (Université de Limoges, France), Emmanuel Conchon (XLIM, France), Paul Germouty (Université de Limoges, France), Amandine Jambert (CNIL, France)

FARES III- Code Security and Privacy

bin2llvm: Analysis of Binary Programs Using LLVM Intermediate Representation
Kevin Kirchner (University of Applied Sciences Upper Austria, Austria), Stefan Rosenthaler (University of Applied Sciences Upper Austria, Austria)

Security Analysis of Cordova Applications in Google Play
Michiel Willocx (KU Leuven, TCG, Belgium), Jan Vossaert (KU Leuven, TCG, Belgium), Vincent Naessens (KU Leuven, TCG, Belgium)

Security and Privacy Implications of NFC-enabled Contactless Payment Systems
Nicholas Akinyokun (The University of Melbourne, Melbourne, Australia), Vanessa Teague (The University of Melbourne, Melbourne, Australia)

Microblogging in a Privacy-Preserving way
Nikolaos Karvelas (TU Darmstadt, Germany), Marius Senftleben (TU Darmstadt, Germany), Stefan Katzenbeisser (TU Darmstadt, Germany)

FARES IV - Security Models and Methods

Provisioning Software with Hardware-Software Binding

Robert Lee (Royal Holloway, University of London, UK), Konstantinos Markantonakis (Royal Holloway, University of London, UK), Raja Naeem Akram (Royal Holloway, University of London, UK)

Victim Communication Stack: A flexible model to select the Human Attack Vector

Enrico Frumento (Cefriel, Italy), Angelo Consoli (SUPSI, Italy), Federica Freschi (Cefriel, Italy), Davide Andreoletti (SUPSI, Italy)

Fully threshold broadcast encryption

Sigurd Eskeland (Norwegian Computing Center, Norway)

Adaptive Resource Management Enabling Deception (ARMED)

Partha Pal (Raytheon BBN Technologies, USA), Nate Soule, (Raytheon BBN Technologies, USA), Nate Lageman (Raytheon BBN Technologies, USA), Shane Clark (Raytheon BBN Technologies, USA), Marco Carvalho (Harris Institute for Assured Information, Florida Institute of Technology, USA), Adrian Granados (Harris Institute for Assured Information, Florida Institute of Technology, USA), Anthony Alves (Harris Institute for Assured Information, Florida Institute of Technology, USA)

The 10th International Workshop on Digital Forensics (WSDF 2017)

Message from WSDF 2017 Workshop Organizers

It is our great pleasure to welcome you to the 10th Annual International Workshop on Digital Forensics (WSDF), which takes place at the Università degli Studi Mediterranea di Reggio Calabria (Reggio Calabria, Italy) from 29 August - 1 September 2017.

Digital forensics is a rapidly evolving field primarily focused on the extraction, preservation and analysis of digital evidence obtained from electronic devices in a manner that is legally acceptable. Research into new methodologies tools and techniques within this domain is necessitated by an ever-increasing dependency on tightly interconnected, complex and pervasive computer systems and networks. The ubiquitous nature of our digital lifestyle presents many avenues for the potential misuse of electronic devices in crimes that directly involve, or are facilitated by, these technologies. The aim of digital forensics is to produce outputs that can help investigators ascertain the overall state of a system. This includes any events that have occurred within the system and entities that have interacted with that system. Due care has to be taken in the identification, collection, archiving, maintenance, handling and analysis of digital evidence in order to prevent damage to data integrity. Such issues combined with the constant evolution of technology provide a large scope of digital forensic research. WSDF aims to bring together experts from academia, industry, government and law enforcement who are interested in advancing the state of the art in digital forensics by exchanging their knowledge, results, ideas and experiences.

The aim of the workshop is to provide a relaxed atmosphere that promotes discussion and free exchange of ideas while providing a sound academic backing. The focus of this workshop is not only restricted to digital forensics in the investigation of crime. It also addresses security applications such as automated log analysis, forensic aspects of fraud prevention and investigation, policy and governance.

The acceptance rate of this edition of the workshop was 50%.

The Workshop organizing committee

Richard E. Overill, *King's College London, UK*
Virginia N. L. Franqueira**,** *University of Derby, UK*
Andrew Marrington, *Zayed University, UAE*
Andrew Jones, *University of Hertfordshire, UK*

Workshop Program Committee WSDF 2017

- Olga Angelopoulou, *University of Hertfordshire, UK*
- Ibrahim Baggili, *University of New Haven, USA*
- Frank Breitinger, *University of New Haven, USA*
- Joanne Bryce, *University of Central Lancashire, UK*
- Aniello Costiglione, *Università di Salerno, Italy*
- Kim-Kwang Raymond Choo, *University of South Australia, Australia*
- George Grispos, *The Irish Software Research Centre (LERO), Ireland*
- Joshua James, *Soon Chun Hyang University, Korea*
- Vassil Roussev, *University of New Orleans, USA*
- Mark Scanlon, *University College Dublin, Ireland*
- Timothy Storer, *University of Glasgow, UK*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
- Pedro R. M. Inacio, *University of Beira Interior, Portugal*
- Katharina Krombholz, *SBA Research, Austria*
- Aswami Ariffin, *CyberSecurity Malaysia, Malaysia*
- Stefano Zanero, *Politecnico di Milano, Italy*
- Kam-Pui Chow, *Hong Kong University, China*
- Chris Hargreaves, *HARGS, UK*
- Antonio Colella, *Italian Army, Italy*
- Yijun Yu, *The Open University, UK*
- Thein Tun, *The Open University, UK*

WSDF 2017 Program

WSDF I

Forensic Image Inspection Assisted by Deep Learning
Felix Mayer (Fraunhofer Institute for Secure Information Technology SIT, Germany) and Martin Steinebach (Fraunhofer Institute for Secure Information Technology SIT, Germany)

WSDF II

On the Usefulness of Compression-Models for Authorship Verification
Oren Halvani (Fraunhofer Institute for Secure Information Technology SIT, Germany), Christian Winter (Fraunhofer Institute for Secure Information Technology SIT, Germany) and Lukas Graner (Fraunhofer Institute for Secure Information Technology SIT, Germany)

Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)
Tanveer Zia (Charles Sturt University, Australia), Peng Liu (Pennsylvania State University, USA) and Weili Han (Fudan University, China)

Forensic State Acquisition from Internet of Things (FSIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition
Christopher Meffert (University of New Haven, USA), Devon Clark (University of New Haven, USA), Ibrahim Baggili (University of New Haven, USA) and Frank Breitinger (University of New Haven, USA)

The 6th International Workshop on Security of Mobile Applications (IWSMA 2017)

Welcome Message from IWSMA 2017 Workshop Organizers

Since the advent of Smartphones, mobile applications have been one of the most thriving areas in the last few years. Thus, securing mobile applications as well as protecting private user data has to be considered as key research topics in the realm of security research. The International Workshop on Security of Mobile Applications (co-located with the ARES-conference) focuses on bringing together researchers from all over the world to share their experience and present recent research, as well as strives to initiate discussions regarding future research topics. The main focus of this year's installment of IWSMA lies in the area of Android-Security and Privacy protection.

The papers that were selected for this workshop cover several interesting topics in this big area, thus they should give an ideal starting point for further discussion, which we are looking forward to participate in, together with the authors and an active audience.

The Workshop organizing committee

Peter Kieseberg, *SBA Research, Austria*
Sebastian Schrittwieser, *Josef Ressel Center for Unified Threat Intelligence on Targeted Attacks, Austria*

Workshop Program Committee IWSMA 2017

- Jakub Breier, *Nanyang Technological University, Singapore*
- Isao Echizen, *National Institute of Informatics (NII), Japan*
- Peter Frühwirt, *Vienna University of Technology, Austria*
- Uschi Gonschor, *EntServ Enterprise Services, Austria*
- Johannes Heurix, *Vienna University of Technology, Austria*
- Andreas Hula, *University College London (UCL), UK*
- Martin Husák, *Masaryk University, Czech Republic*
- Francesco Mercaldo, *Institute for Informatics and Telematics (CNR), Italy*
- Raydel Montesino Perurena*, Universidad de las Ciencias Informáticas, Cuba*
- Lukasz Olejnik, *University College London (UCL), UK*
- Mayank Sinha, *Shell, The Netherlands*
- Ronald Tögl, *Infineon Technologies, Austria*
- Johanna Ullrich, *SBA Research, Austria*

IWSMA 2017 Program

IWSMA I

The Demon is in the Configuration: Revisiting Hybrid Mobile Apps Configuration Model
Abeer Aljarrah (University of North Carolina at Charlotte, USA) and Mohamed Shehab (University of North Carolina at Charlotte, USA)

Quantitative Dynamic Taint Analysis of Privacy Leakage in Android Arabic Apps
Ayman Youssef (Nile University, Egypt) and Ahmed F. Shosha (Nile University, Egypt)

Learning Android Malware
Khanh-Huu-The Dam (University Paris Diderot & LIPN, France) and Tayssir Touili (LIPN, CNRS & University Paris 13, France)

The 6th International Workshop on Cyber Crime (IWCC 2017)

Welcome Message from IWCC 2017 Workshop Organizers

Today's societies are becoming more and more dependent on open networks such as the Internet – where commercial activities, business transactions and government services are realized. This has led to the fast development of new cyber threats and numerous information security issues, which are exploited by cyber criminals. The inability to provide trusted secure services in contemporary computer network technologies has a tremendous socio-economic impact on global enterprises as well as individuals.

Moreover, the frequently occurring international frauds impose the necessity to conduct the investigation of facts spanning across multiple international borders. Such examination is often subject to different jurisdictions and legal systems. A good illustration of the above being the Internet, which has made it easier to perpetrate traditional crimes. It has acted as an alternate avenue for the criminals to conduct their activities, and launch attacks with relative anonymity. The increased complexity of the communications and the networking infrastructure is making investigation of the crimes difficult. Traces of illegal digital activities are often buried in large volumes of data, which are hard to inspect with the aim of detecting offences and collecting evidence. Nowadays, the digital crime scene functions like any other network, with dedicated administrators functioning as the first responders.

This poses new challenges for law enforcement policies and forces the computer societies to utilize digital forensics to combat the increasing number of cybercrimes. Forensic professionals must be fully prepared in order to be able to provide court admissible evidence. To make these goals achievable, forensic techniques should keep pace with new technologies.

The aim of the IWCC workshop is to bring together the research accomplishments provided by the researchers from academia and the industry. The other goal is to show the latest research results in the field of digital forensics and to present the development of tools and techniques, which assist the investigation process of potentially illegal cyber activity.

The Workshop organizing committee

Artur Janicki, *Warsaw University of Technology, Poland*
Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
Krzysztof Szczypiorski, *Warsaw University of Technology, Poland*

Workshop Program Committee IWCC 2017

- Marc Chaumont, *LIRMM, France*
- Michal Choras, *ITTI Ltd., Poland*
- Xiaofeng Chen, *Xidian University, China*
- Guangjie Liu, *NJUST, China*
- Jozef Wozniak, *Gdansk University of Technology, Poland*
- Frédéric Cuppens, *TELECOM Bretagne, France*
- Prof. Dr. Jana Dittmann, *Otto-von-Guericke University Magdeburg, Germany*
- Steffen Wendzel, *Worms University of Applied Sciences and Fraunhofer FKIE, Germany*
- Stefan Katzenbeisser, *TU Darmstadt, Germany*
- Joanna Śliwa, *Military Communication Institute, Poland*
- Maciej Korczyñski, *Delft University of Technology, The Netherlands*
- Alessandro Checco, *University of Sheffield, UK*
- Nabil Schear, *MIT Lincoln Laboratory, USA*
- Bela Genge, *University of Tg Mures, Romania*
- Igor Kotenko, *Russian Academy of Sciences (SPIIRAS), Russia*
- Johnson Thomas, *Oklahoma State University, USA*
- Ewa Syta, *Trinity College, Ireland*
- Jean-Francois Lalande, *INSA Centre Val de Loire, France*
- Christian Kraetzer, *Otto-von-Guericke University Magdeburg, Germany*
- Pedro Luis Prospero Sanchez, *University of Sao Paulo, Brazil*
- Zbigniew Kotulski, *Warsaw University of Technology, Poland*
- Eric Chan-Tin, *Oklahoma State University, USA*
- Josef Pieprzyk, *Queensland University of Technology, Australia*
- Luca Caviglione, *ISSIA, CNR, Italy*
- Hui Tian, *National Huaqiao University, China*

IWCC 2017 Program

IWCC I

Type Me the Truth! Detecting Deceitful Users via Keystroke Dynamics
Merylin Monaro (University of Padua, Italy), Riccardo Spolaor (University of Padua, Italy), Qianqian Li (University of Padua, Italy), Mauro Conti (University of Padua, Italy), Luciano Gamberini (University of Padua, Italy) and Giuseppe Sartori (University of Padua, Italy

Resource Hints in HTML5: A New Pandora's Box of Security Nightmares
Natalija Vlajic (York University, Canada)

IWCC II

Group Key Agreement Protocols, Dynamic Groups, Scalability Analysis, Performance Analysis
Orhan Ermis (Bogazici University, Turkey), Serif Bahtiyar (Bogazici University, Turkey), Emin Anarım (Bogazici University, Turkey) and Mehmet Ufuk Caglayan (Bogazici University, Turkey)

Secure and Efficient Data Sharing with Attribute-based Proxy Re-encryption Scheme
Alberto Trombetta (Insubria University, Italy) and Masoomeh Sepheri (Università degli Studi di Milano, Italy)

The 4th Workshop on Software Assurance (SAW 2017)

Welcome Message from SAW 2017 Workshop Organizers

We would like to offer our warm welcome to our fourth Software Assurance Workshop (SAW) co-located with ARES 2017!

Software security is drawing more attention from the software engineering community, in part due to the many highly publicized attacks exploiting software vulnerabilities. Software increasingly affects our daily lives: our social networks, our automobiles, our smart home systems, our smart phones, and our financial well-being.

Although many attempts have been made to improve software security over the years, the focus of these efforts has traditionally been limited to tools and techniques focusing on implementation and testing, such as static analysis, penetration testing, and secure coding.

We believe that the scope of software security is much wider than those heavily studied research areas and would like to invite researchers to explore other facets of software security, which have not been as thoroughly studied.

The vision of our workshop is to provide the state-of-the-art in Software Assurance as well as opportunities to network with academicians and professionals working in the software community. We look forward to getting to know you at the workshop and sincerely thank you for your participation.

The Workshop organizing committee

Jungwoo Ryoo, *Penn State Altoona, USA*
Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
Rick Kazman, *University of Hawaii/SEI, USA*

Workshop Program Committee SAW 2017

- Robert Ellison, *Software Engineering Institute (SEI)/Computer Emergency Response Team (CERT), USA*
- Rick Kazman*, University of Hawaii/SEI, USA*
- Dae-kyoo Kim, *Oakland University, USA*
- Suntae Kim, *Chonbuk National University, Republic of Korea*
- Phillip Laplante, *Pennsylvania State University, USA*
- Jungwoo Ryoo, *Pennsylvania State University, USA*
- Sebastian Schrittwieser, *St. Pölten University of Applied Sciences, Austria*
- Eunjee Song*, Baylor University, USA*
- Paul Tavolato*, St. Pölten University of Applied Sciences, Austria*
- A Min Tjoa, *Vienna University of Technology, Austria*
- Simon Tjoa, *St. Pölten University of Applied Sciences, Austria*
- Edgar Weippl, *Secure Business Austria (SBA) Research, Austria*
- Carol Woody, *SEI/CERT, USA*

SAW 2017 Program

SAW I

Towards Semi-automated Detection of Trigger-based Behavior for Software Security Assurance
Dorottya Papp (CrySyS Lab, Dept. of Networked Systems and Services, BME, Hungary), Levente Buttyán (CrySyS Lab, Dept. of Networked Systems and Services, BME, Hungary) and Zhendong Ma (Center of Digital Safety and Security, Austrian Institute of Technology, Austria)

Protection of personal data in security alert sharing platforms
Václav Stupka (Masaryk University, Czech Republic), Martin Horák (Masaryk University, Czech Republic) and Martin Husák (Masaryk University, Czech Republic)

SAFE and Secure: Deeply Integrating Security in a New Hazard Analysis
Sam Procter (Software Engineering Institute, Carnegie Mellon University, USA), Eugene Vasserman (Kansas State University, USA) and John Hatcliff (Kansas State University, USA)

On Using TLS to Secure In-Vehicle Networks
Daniel Zelle (Fraunhofer SIT, Germany), Christoph Krauß (Fraunhofer SIT, Germany), Hubert Strauß (Audi Electronics Venture GmbH, Germany) and Karsten Schmidt (Audi AG, Germany)

The 3rd International Workshop on Secure Software Engineering (SSE 2017)

Welcome Message from SSE 2017 Workshop Organizers

We are pleased to welcome you to the third International Workshop on Secure Software Engineering (SSE 2017), organized in conjunction with the International Conference on Availability, Reliability and Security (ARES 2017) in Reggio Calabria, Italy.

The goal of the workshop is to bring together security and software development researchers to share their finding, experiences, and positions about developing secure software. The goal of the workshop is to bring together security and software development researchers and practitioners to share their finding, experiences, and positions about developing secure software. The workshop aims to encourage the use of scientific methods to investigate the challenges related to developing secure software. It aims also to increase the communication between security researchers and software development researchers to enable the development of techniques and best practices for developing secure software. The workshop was renamed from Agile Secure Software Development to Secure Software Engineering to avoid the long discussions about the relation of submitted papers to agile, while current practices of engineering secure software use the agile approach.

We have assembled this year a nice program to challenge the participants and stimulate the discussion. We selected 6 papers and one extended abstract. We thank the members of the Program Committee for their support, and all the authors for their contribution to the workshop. Each paper has been reviewed by minimum 3 members of the Program Committee. The program includes also two invited speakers and a panel on Secure DevOps.

We hope you will enjoy it!

The Workshop organizing committee

Lotfi ben Othmane, *Iowa State University, USA*
Juha Röning, *University of Oulu, Finland*

Workshop Program Committee SSE 2017

- Benjamin Aziz, *University of Portsmouth, UK*
- Achim Brucker, *University of Sheffield, UK*
- Bengt Carlsson, *Uppsala University, Sweden*
- Martin Jaatun, *SINTEF ICT, Norway*
- Joern Eichler, *Fraunhofer AISEC, Germany*
- Khaled Khan, *Qatar University, Qatar*
- Lotfi ben Othmane, *Iowa State University, USA*
- Juha Röning, *University of Oulu, Finland*
- Gerald Quirchmayr, *University of Vienna, Austria*
- Antti Vähä-Sipilä, *F-Secure, Finland*
- Edgar Weippl, *SBA Research, Austria*

SSE 2017 Program

SSE I - DevSecOps and cloud computing

Identification of Dependency-based Attacks on Node.js
Brian Pfretzschner (TU Darmstadt, Germany) and Lotfi Ben Othmane (Iowa State University, USA)

DevOps for Better Software Security in the Cloud
Martin Gilje Jaatun, Daniela Soares Cruzes, and Jesus Luna

Implementing Secure DevOps assessment for highly regulated environments.
Hasan Yasar (CMU, USA)

SSE II - Agile secure software development

DoS Attacks on Controller Area Networks by Fault Injections from the Software Layer
Pal-Stefan Murvay (Politehnica University of Timisoara, Romania), Bogdan Groza (Politehnica University of Timisoara, Romania)

Source Code Patterns of SQL Injection Vulnerabilities
Felix Schuckert (HTWG Konstanz, Germany) Basel Katt (Norwegian Information Security laboratory, Norway), Hanno Langweg (HTWG Konstanz, Germany)

Towards a Secure SCRUM Process for Agile Web Application Development
Patrik Maier (Graz University of Technology, Austria), Zhendong Ma (Austrian Institute of Technology, Austria), Roderick Bloem (Graz University of Technology, Austria)

Busting a Myth: Review of Agile Security Engineering Methods
Kalle Rindell (University of Turku, Finland), Sami Hyrynsalmi (Tampere University of Technology, Finland), Ville Leppänen (University of Turku, Finland)

The 2nd International Workshop on Malware Analysis (WMA 2017)

Welcome Message from WMA 2017 Workshop Organizers

This is the second edition of the International Workshop on Malware Analysis, held in conjunction with the 12th International Conference on Availability, Reliability and Security.

The volume and technical sophistication of malware are constantly increasing. Malware writers have recently developed advanced techniques to evade detection and attack strategies that increase the potential harm caused by malware. The large number and types of devices that can be affected by malware makes the malware detection problem of vital interest to a wide spectrum of computer users. Moreover, recent studies demonstrate that the evolutionary pace of evasion techniques has been much faster than that of anti-malware. This scenario makes urgent the development of a new generation of effective solutions for detecting and removing malware. For these reasons, WMA aims to bring together experts from academia, industry, government, and law enforcement who are interested in advancing the state of the art in malware analysis by exchanging their knowledge, results, ideas, and experiences. The goal of the workshop is to provide a relaxed atmosphere that promotes discussion and free exchange of ideas, with a sound academic backing. The focus of this workshop is not restricted to techniques for malware detection, but also includes discussion of new models of malware and guidelines for limiting malware diffusion that can be utilized by governments, industries, and other organizations to defend against cyber-attacks.

We would like to thank the authors for their valuable contributions to this workshop and the program committee members for their help.

The Workshop organizing committee

Mark Stamp, *State University of San Josè, USA*
Corrado Aaron Visaggio, *Università degli Studi del Sannio, Italy*

Workshop Program Committee WMA 2017

- Shahid Alam, *Gebze Technical University*, *Turkey*
- Thomas Austin, *San Jose State University*, *USA*
- Lorenzo Cavallaro, *Royal Holloway, University of London, UK*
- Giorgio Giacinto, *Università di Cagliari, Italy*
- Sotiris Ioannidis, *Foundation for Research and Technology, Greece*
- Francesco Mercaldo, *Università del Sannio, Italy*
- Vinod P Nair, *SCMS School of Engineering & Technology, India*
- Charles Nicholas, *University of Maryland, Baltimore County, USA*
- Yulei Pang, *Southern Connecticut State University, USA*
- Antonella Santone, *Università del Sannio, Italy*

WMA 2017 Program

WMA I - Malware detection

An Approach to Botnet Malware Detection Using Nonparametric Bayesian Methods
Joseph Divita(US Department of Defence, SPAWAR Systems Center Pacific, USA) and Roger Hallman (US Department of Defense, SPAWAR Systems Center Pacific, Cybersecurity S&T Branch, USA)

Malware and Formal Methods
Fabio Martinelli (Institute for Informatics and Telematics, CNR, Italy), Francesco Mercaldo (Institute for Infromatics and Telematics, CNR, Italy), Vittoria Nardone (University of Sannio, Italy) and Antonella Santone (University of Sannio, Italy)

End-node Fingerprinting for Malware Detection on HTTPS Data
Tomáš Komárek (Czech Technical University in Prague, Czech Republic) and Petr Somol (Cisco Systems, Inc., Czech Republic)

WMA II - Defensive technologies

How to Ensure Bad Quality in Metal Additive Manufacturing: In-Situ Infrared Thermography from the Security Perspective
Andrew Slaughter (University of South Alabama, USA), Mark Yampolskiy (University of South Alabama, USA), Manyalibo Matthews (Lawrence Livermore National Laboratory, USA), Wayne E. King (Lawrence Livermore National Laboratory, USA), Gabe Guss (Lawrence Livermore National Laboratory, USA) and Yuval Elovici (Ben-Gurion University, Israel)

Popularity-based Detection of Domain Generation Algorithms
Jasper Abbink (TU Delft, Netherlands) and Christian Doerr (TU Delft, Netherlands)

JSDES – An Automated De-Obfuscation System for Malicious JavaScript
Moataz Abdel Khalek (University Nile, Egypt) and Ahmed Shosha (University Nile, Egypt)

The 1st International Workshop on Criminal Use of Information Hiding (CUING 2017)

Welcome Message from CUING 2017 Workshop Organizers

With the constant rise of the number of Internet users, available bandwidth and an increasing number of services shifting into the connected world, criminals are increasingly active in the virtual world. With improving defensive methods, cybercriminals have to utilize increasingly sophisticated ways to perform their malicious activities. While protecting the privacy of users, many technologies used in current malware and network attacks have been abused in order to allow criminals to carry out their activities undetected.

The aim of the First International Workshop, on Criminal Use of Information Hiding (CUING), is to bring together researchers, practitioners, law enforcement representatives, and security professionals in the area of analysis of information hiding (e.g. steganography, covert channels), obfuscation techniques and underground networks (darknets) in order to present novel research regarding the use of data and communication hiding methods in criminal environments and to discuss ideas for fighting misuse of privacy enhancing technologies.

The Workshop organizing committee

Philipp Amann, *Europol, European Cybercrime Centre, The Netherlands*
Jart Armin, *CyberDefcon, The Netherlands*
Wojciech Mazurczyk, *Warsaw University of Technology, Poland*
Angelo Consoli, *Scuola universitaria professionale della Svizzera italiana (SUPSI), Switzerland*
Peter Kieseberg, *SBA Research, Austria*
Joerg Keller, *FernUniversitaet in Hagen, Germany*

Workshop Program Committee CUING 2017

- Francesca Bosco, *UNICRI, Italy*
- Brent Carrara, *University of Ottawa, Canada*
- Luca Caviglione, *CNR, Italy*
- Marc Chaumont, *LIRMM Montpellier – University of Nimes, France*
- Marco Cremonini, *University of Milan, Italy*
- Jana Dittmann, *Otto-von-Guericke University Magdeburg, Germany*
- Mattia Epifani, *CNR, Italy*
- Zeno Geradts, *Netherlands Forensic Institute, Netherland*
- Dipak Ghosal, *University of California, Davis, USA*
- Julio Hernandez-Castro, *University of Kent, UK*
- David-Olivier Jaquet-Chiffelle, *University of Lausanne, Switzerland*
- Stefan Katzenbeisser, *Technische Universität Darmstadt, Germany*
- Piotr Kijewski, *Shadowserver, Poland*
- Pawel Korus, *AGH University of Science and Technology, Poland*
- Christian Kraetzer, *Otto-von-Guericke University Magdeburg, Germany*
- Jean-Francois Lalande, *INSA Centre Val de Loire, France*
- Shujun Li, *University of Surrey, UK*
- Foy Shiver, *APWG, USA*
- Edgar Weippl, *SBA Research, Austria*
- Steffen Wendzel, *Worms University of Applied Sciences, Germany*
- Alan Woodward, *University of Surrey, UK*
- Sebastian Zander, *Murdoch University, Australia*
- Hui Tian, *National Huaqiao University, China*
- and several LEA representatives (however they do not want to be listed openly)

CUING 2017 Program

CUING I

Are Covert Timing Channels Statistical Anomalies?

Félix Iglesias Vázquez (TU Wien, Austria) and Tanja Zseby (TU Wien, Austria)

FROST – Anti-Forensics Digital-Dead-DROp Information Hiding RobuST to Detection & Data Loss with Fault-tolerance

Avinash Srinivasan (Temple University, USA), Hunter Dong (Temple University, USA) and Angelos Stavrou (George Mason University, USA)

A New Data-Hiding Approach for IP Telephony Applications with Silence Suppression

Sabine Schmidt (FernUniversitaet in Hagen, Germany), Wojciech Mazurczyk (Warsaw University of Technology, Poland), Joerg Keller (FernUniversitaet in Hagen, Germany) and Luca Caviglione (National Research Council of Italy, Italy)

CUING II

REMI: A Reliable and Secure Multicast Routing Protocol for IoT Networks

Mauro Conti (University of Padova, Italy), Pallavi Kaliyar (University of Padova, Italy) and Chhagan Lal (University of Padova, Italy)

Machine Learning Approach for Detection of nonTor Traffic

Elike Hodo (University of Strathclyde, UK), Xavier Bellekens (University of Abertay, Dundee, UK, Ephraim Iorkyase (University of Strathclyde, UK), Andrew Hamilton (University of Strathclyde, UK), Christos Tachtatzis (University of Strathclyde, UK) and Robert Atkinson (University of Strathclyde, UK)

Investigating the darknet: Legal limitations in Slovenian legal system

Anze Mihelic (Faculty of Criminal Justice and Security, University of Maribor, Slovenia), Blaž Markelj (Faculty of Criminal Justice and Security, University of Maribor, Slovenia), Igor Bernik (Faculty of Criminal Justice and Security, University of Maribor, Slovenia) and Sabina Zgaga (Constitutional Court of the Republic of Slovenia, Slovenia)

The 3rd ARES 2017 EU Projects Symposium

Welcome to the ARES EU Projects Symposium!

The ARES EU Projects Symposium is held for the third time in conjunction with the ARES Conference.

The goal is to disseminate the results of EU research projects, meet potential project partners and exchange ideas within the scientific community.

This year, four workshops will be held within the ARES EU Projects Symposium:

- 2nd Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID 2017)
- 1st International Workshop on Securing Critical Infrastructures (S-CI 2017)
- 1st International Workshop on Supply Chain Security, Resilience and Accountability (SC-SRA 2017)
- 1st International Workshop on Creating Identity – Trustworthy Ecosystems (CITE 2017)

We would like to thank the workshop organizers for their great efforts and hard work in proposing the workshop, selecting the papers, the interesting programs and for the arrangements of the workshops during the conference days.

We hope you enjoy the ARES EU Projects Symposium!

Edgar Weippl
SBA Research, Austria

The 2nd International Workshop on Security, Privacy, and Identity Management in the Cloud (SECPID 2017)

Welcome Message from SECPID 2017 Workshop Organizers

Over the last years, the computing paradigm has experienced a massive shift from local to cloud-based applications. As a result, users and organizations do no longer have full control over their data and services, but they rely on third-party cloud providers.

This development poses various challenges concerning the integrity and confidentiality of data as well as the privacy of users of such systems. Currently, no satisfactory solutions to these challenges exist, which is a roadblock for the large-scale deployment of cloud-based applications handling sensitive data such as electronic health records.

As last year, the purpose of SECPID is therefore to provide a platform to present and discuss innovative ideas related to security, cryptography, trust, and identity management in and for the cloud.

SECPID was jointly organized by the EU-H2020 projects CREDENTIAL and PRISMACLOUD, together with the DPSP cluster on data protection, security, and privacy, which was in particular supported by the EU-H2020 projects SecureCloud, PaaSword, SERECA, WITDOM, and MUSA.

We are looking forward to fruitful and interesting discussions in Italy!

The Workshop organizing committee

Stephan Krenn, *AIT Austrian Institute of Technology GmbH, Austria*
Thomas Lorünser, *AIT Austrian Institute of Technology GmbH, Austria*
Erkuden Rios Velasco, *Fundación Tecnalia Research & Innovation, Spain*

Workshop Program Committee SECPID 2017

- Jan Camenisch, *IBM Research – Zurich, Switzerland*
- Manuel Barbosa, *University of Porto, Portugal*
- Denise Demirel, *Technical University of Darmstadt, Germany*
- Simone Fischer-Hübner, *Karlstad University, Sweden*
- Thomas Gross, *Newcastle University, UK*
- Lucjan Hanzlik, *Wroclaw University of Science and Technology, Poland*
- Henrich Pöhls, *University of Passau, Germany*
- Jetzabel Serna, *Goethe University Frankfurt, Germany*
- Daniel Slamanig, *Graz University of Technology, Austria*

In addition, the program committee was supported by the following sub reviewers:

- David Derler
- Matthias Geihs
- Hans Hedbom
- Felix Hörandner
- Sebastian Ramacher
- Simon Roth
- Kai Samelin
- Florian Thiemer
- Giulia Traverso

SECPID 2017 Program

SECPID I

Position Paper: The Past, Present, and Future of Sanitizable and Redactable Signatures
Arne Bilzhause (Uni Passau, Germany), Henrich C. Pöhls (Uni Passau, Germany) and Kai Samelin (TU Darmstadt & IBM Research, Switzerland)

The Archistar Secret-Sharing Backup Proxy
Andreas Happe (Austrian Institute of Technology, Austria), Florian Wohner (Austrian Institute of Technology, Austria) and Thomas Loruenser (Austrian Institute of Technology, Austria)

Orchestrating Privacy Enhancing Technologies and Services with BPM Tools
Nicolás Notario, Alberto Crespo, Eduardo González Real, Eleonora Ciceri, Ilio Catallo, and Sauro Vicini

SECPID II

Towards the Adoption of Secure Cloud Identity Services
Alexandros Kostopoulos (Hellenic Telecommunications Organization R&D, Greece), Evangelos Sfakianakis (Hellenic Telecommunications Organization R&D, Greece), Ioannis Chochliouros (Hellenic Telecommunications Organization R&D, Greece), John-Sören Pettersson (Karlstad University, Sweden), Stephan Krenn (Austrian Institute of Technology, Austria), Welderufael Tesfay (Goethe University Frankfurt, Germany), Andrea Migliavacca (Lombardia Informatica S.p.A., Italy) and Felix Hörandner (Graz University of Technology, Austria)

Towards a Model of User-centered Privacy Preservation
Paul Grace (University of Southampton, UK) and Mike Surridge (University of Southampton, UK)

NEXTLEAP: Decentralizing Identity with Privacy for Secure Messaging
Harry Halpin (World Wide Web Consortium, UK)

SECPID III

Self-healing Multi-Cloud Application Modelling
Erkuden Rios (Tecnalia Research & Innovation, Spain), Maria Carmen Palacios (Tecnalia Research & Innovation, Spain) and Eider Iturbe (Tecnalia Research & Innovation, Spain)

Application of the holistic Data Privacy and Security Framework PaaSword
Sebastian Thomas Schork (CAS Software AG, Germany), Antonia Schwichtenberg (CAS Software AG, Germany), Spiros Alexakis (CAS Software AG, Germany) and George Moldovan (Siemens, Romania)

The 1st International Workshop on Securing Critical Infrastructures (S-CI 2017)

Welcome Message from S-CI 2017 Workshop Organizers

Critical Infrastructures (Communication, Transportation, Banking, e-Commerce, Utilities etc.) increasingly and inextricably depend on IT-technologies to provide for both functionality and efficiency. However, the cost of the IT-reliance is the consequent exposure of the Critical Infrastructure (CI) to IT-based security vulnerabilities. The state of the practice often has different CI's developing customized security solutions to meet their specific needs. While this is judicious, the CI's can benefit from sharing approaches to intrusion detection, threat classification, diagnostics, mitigation schema, security architectures and many others. The workshop aims to bring together viewpoints from diverse CI's to explore the commonalities of security problems and solutions for advancing the collective science and practice of CI security protection.

This workshop is organized by the CIPSEC project consortium. The overall goal of CIPSEC is to offer a complete security ecosystem that supports the secure operation of critical infrastructures. Security services include vulnerability tests and recommendations, key personnel training courses, public-private partnerships (PPPs) forensics analysis, standardization and protection against cascading effects. All solutions and services will be validated in three pilots performed in three different CI environments (transportation, health, and environment). CIPSEC will also develop a marketing strategy for optimal positioning of its solutions in the CI security market.

The workshop consists of two invited talks by CIPSEC members as well as six contributed papers, which show the versatility of security solutions required in the domain of critical infrastructures. We hope that the workshop will inspire the exchange of information between CI domains.

The Workshop organizing committee

Stefan Katzenbeisser, *TU Darmstadt, Germany*
Apostolos P. Fournaris, *University of Patras, Greece*

Workshop Program Committee S-CI 2017

- Jorge Cuellar, *Siemens, Germany*
- Daniel Germanus, *DB Systel, Germany*
- Klaus Kursawe, *The Netherlands*
- Kostas Lampropoulos, *University of Patras, Greece*
- Eva Marín, *Universitat Politècnica de Catalunya, Spain*
- Xavi Masip, *Universitat Politècnica de Catalunya, Spain*
- Michael Paulitsch, *Thales, Austria*
- Andreas Peter, *University of Twente, The Netherlands*
- Luigi Romano, *University of Naples, Italy*
- Wilfried Steiner, *TTTech, Austria*
- Neeraj Suri, *TU Darmstadt, Germany*

S-CI 2017 Program

S-CI I - CyberSecurity and Critical Infrastructures

Rolling DICE – Lightweight Remote Attestation for COTS IoT Hardware
Lukas Jäger (Fraunhofer Institute for Secure Information Technology SIT, Germany), Richard Petri (Fraunhofer Institute for Secure Information Technology SIT, Germany), Andreas Fuchs (Fraunhofer Institute for Secure Information Technology SIT, Germany)

ZONESEC: built-in cyber-security for wide area surveillance system
Aljosa Pasic (Atos, Spain), Jose-Ramon Martinez-Salio (Atos, Spain), Susana Gonzalez Zarzosa (Atos, Spain)

Protecting Future Maritime Communication
Karin Bernsmed (SINTEF, Norway), Christian Frøystad (SINTEF, Norway), Per Håkon Meland (SINTEF, Norway)

S-CI II - Critical Infrastructure Systems CyberSecurity Tools

Using Ciphers for Failure Recovery in ITS Systems
Mustafa Ayoob (TU-BS, Germany), Wael Adi (TU-BS, Germany), Vassilis Prevelakis (TU-BS, Germany)

Towards DDoS Attack Resilient Wide Area Monitoring Systems
Kubilay Demir (TU Darmstadt, Germany), Neeraj Suri (TU Darmstadt, Germany)

Anomaly Detection for Simulated IEC-60870-5-104 Traffic
Ersi Hodo (Fachhochschule St. Pölten, Austria), Stepan Grebeniuk (Fachhochschule St. Pölten, Austria), Henri Ruotsalainen (Fachhochschule St. Pölten, Austria), Paul Tavolato (Fachhochschule St. Pölten, Austria)

Supporters and Sponsors

Supported by

Municipality of Reggio Calabria

Province of Reggio Calabria

CINI Cybersecurity Lab

Associazione Italiana per l'infromatica ed il Calcolo Automatico

Information Systems Security Association

Associazione Italiana Professionisti della Sicurezza Sicurezza

Sponsored by

Gold Sponsor

Gold Sponsor

Silver Sponsor

Silver Sponsor

Silver Sponsor

Silver Sponsor

A Holistic Approach for Privacy Protection in E-Government

Konstantinos Angelopoulos
University of Brighton
Brighton, UK
K.Angelopoulos@brighton.ac.uk

Vasiliki Diamantopoulou
University of Brighton
Brighton, UK
V.Diamantopoulou@brighton.ac.uk

Haralambos Mouratidis
University of Brighton
Brighton, UK
H.Mouratidis@brighton.ac.uk

Michalis Pavlidis
University of Brighton
Brighton, UK
M.Pavlidis@brighton.ac.uk

Mattia Salnitri
University of Trento
Trento, Italy
mattia.salnitri@unitn.it

Paolo Giorgini
University of Trento
Trento, Italy
paolo.giorgini@unitn.it

José F. Ruiz
Atos
Madrid, Spain
jose.ruizr@atos.net

ABSTRACT

Improving e-government services by using data more effectively is a major focus globally. It requires Public Administrations to be transparent, accountable and provide trustworthy services that improve citizen confidence. However, despite all the technological advantages on developing such services and analysing security and privacy concerns, the literature does not provide evidence of frameworks and platforms that enable privacy analysis, from multiple perspectives, and take into account citizens' needs with regards to transparency and usage of citizens information. This paper presents the VisiOn (Visual Privacy Management in User Centric Open Requirements) platform, an outcome of a H2020 European Project. Our objective is to enable Public Administrations to analyse privacy and security from different perspectives, including requirements, threats, trust and law compliance. Finally, our platform-supported approach introduces the concept of Privacy Level Agreement (PLA) which allows Public Administrations to customise their privacy policies based on the privacy preferences of each citizen.

CCS CONCEPTS

•**Security and privacy** →*Domain-specific security and privacy architectures;*

KEYWORDS

Privacy by Design, Privacy Level Agreement, Privacy Requirements, Privacy Enforcement

ARES'17, Reggio Calabria, Italy

DOI: 10.475/123_4

1 INTRODUCTION

An increasing number of government operations take advantage of new technological advances [17, 26] (e.g., Cloud and Big Data), moving toward e-government. This direction has provided new challenges for software engineers associated with information and data privacy management, technological complexity and restrictive laws and regulations [1]. From a societal perspective, citizens' lack trust for such services and their perception on how Public Administrations (PAs) store and deal with their data along with the lack of transparency, are a bottleneck to the wide adoption of e-government [10]. On the other hand, from a technical perspective, in e-government multiple organizations might require to process citizens' private data differently. This rises a major concern about the accountability of the PAs involved.

Existing privacy engineering frameworks, platforms and models [15, 16, 18, 28] do not support analysis of privacy issues from different perspectives (e.g., organisational, business-process, threat and mitigation), nor they allow public administration authorities to take into account citizens' needs in order to make their services transparent. Moreover, they fail to combine such analyses with trust analysis in order to better understand how trust influences the citizen needs and how it impacts potential privacy threats and mitigation strategies. A higher level of trust is very likely to increase the adoption of e-government by the society [3, 5].

This paper proposes a holistic, platform-supported approach for privacy protection in e-government that provides solutions to both the societal and the technical challenges discussed above. In particular, it contributes to improving privacy in e-government services through: a) the enhancement of user trust and confidence in e-government services, by combining existing software engineering approaches and modelling languages, in order to analyse trust relationships between citizens and PAs and identify ways of strengthening such relationships, which could result in decreasing the number of users that are reluctant to use such services; b) the improvement of transparency, by imposing accountability to service providers (e.g., public authorities) with regard to privacy of citizen information; c) the empowerment of users (i.e. citizens and

Public Administrators), by providing a new type of Privacy Management system that allows them to take control over their data; d) the construction of personalised privacy agreements between governments and citizens, based on the individual preferences of the latter (e.g., choose what third party organisations will have access to their personal data) and through the provision of a privacy policy enforcement mechanism to guarantee that these agreements are respected.

The paper is structured as follows; Section 2 overviews the baseline of our work. Next, Section 3 presents the VisiOn Privacy Platform. Section 4 evaluates our platform with a real case scenario. Section 5 discusses related work while Section 6 concludes the paper.

2 BASELINE

In this section we present a set of research tools that constitute the baseline of our proposal. These tools support privacy analysis of socio-technical systems [7]. These tools allow capturing requirements for PA systems, systematically creating privacy policies and enforcing them.

2.1 Privacy by Design

Privacy by Design (PbD) is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures. PbD is currently included in the revised draft regulation for data protection in the EU [21], referred to as 'Data Protection by Design' in order to increase incentives to implement PbD for both suppliers of systems that process personal data and for government organisations that procure such systems. The following modelling tools adopt the concept of PbD by providing the means to systematically elicit and document privacy, security and trust requirements.

STS-Tool This tool supports the Socio-Technical Security Modelling Language (STS-ml) [8]. STS-ml allows modelling privacy and security aspects from social and organisational perspectives of PA systems. STS-ml enables its users to perform the following activities: a) capture the source and destination entities in a transmission of citizens' information and thus enhancing the transparency of the e-government services; b) identify privacy requirements and potential conflicts with social and organisational aspects of the system; c) specify who is authorised to access information of citizens. For example, STS-ml can be used to specify confidentiality requirements on medical record of patient's hospital, to specify how such information is transmitted and check whether the confidentiality is preserved or there are security leaks in the systems.

SecBPMN2 This tool uses an extension of BPMN 2.0 [20], the standard modelling notation for business processes, with security and privacy concepts. SecBPMN2 [24] allows to: a) specify secure business processes, i.e. business processes with annotated security aspects; b) define privacy policies, i.e. procedural constraints with privacy properties; c) verify privacy policies against secure business processes; d) verify if business processes are compliant with citizen requirements; e) generate a report that describes the secure business processes and the privacy policies specified by PAs. For example, SecBPMN2 allows PA administrators to specify business processes, implemented within a hospital, and capture how to store and distribute medical records of patients. Therefore, SecBPMN2 allows to verify that such processes do not violate security constraints, such as the restriction of distribution of medical record only to authorised doctors.

SecTro This tool supports the Secure Tropos [19], a security-aware software systems development methodology that shares several concepts with STS-ml on modelling socio-technical systems. SecTro allows the detection of security and privacy threats that could prevent the modelled system from fulfilling its goals or compromise the privacy of the data that handles. Moreover, SecTro allows the detection of vulnerabilities and the selection of security and privacy mechanisms, through a pattern library, to protect them. This library also guides the user on which pattern is most suitable, based on the threat that is addressed. The main purpose of this tool is to explicitly capture the security requirements of the analysed system and facilitate the selection of a suitable security mechanism in order to mitigate potential attacks.

JTrust This tool supports a methodology for modelling and reasoning about trust relationships and for assessing the trustworthiness of a system under development. JTrust [22] enables PAs to model the privacy related trust relationships that affect the trustworthiness of their systems in terms of ensuring privacy. The tool also allows reasoning about these trust relationships in a structured way, facilitating the identification of technical or organisational controls in cases where there are gaps of trust, in order to ensure that data privacy is preserved. In the context of e-government services, capturing the level of trustworthiness between citizens and other organisations, contributes to eliciting questions about permitting of refusing access of their data to the latter.

CARiSMA The CompliAnce, Risk, and Security Model Analyzer (CARiSMA) tool allows modelling system architectures using UMLsec [13] diagrams. UMLsec is an extension of UML [4] in form of a UML profile that provides model driven development for secure information systems. The tool supports and implements UMLsec checks on compliance, risk or security. Tags and stereotypes are used to express security requirements and assumptions on system environments. CARiSMA is used for analysing the enforcement of security constraints at architectural level, as well as the enforcement of security requirements of citizens in the PA system. In particular, the latter will increase the security level of the system and therefore, in the long term, the trust of the citizens in the application.

2.2 Privacy Policies

Every PA, when dealing with data collected from the citizens, is required to apply certain privacy policies that must be compliant with the existing laws and guarantee that they will be respected. These policies are usually a result of explicitly stated preferences of the citizens provided through questionnaires. Hereby, we present two tools that facilitate the composition of questionnaires for eliciting privacy preferences and provide guidance to the citizens in answering them.

DAE The Dynamic Audit Engine (DAE) supports the elicitation of citizens' privacy needs. DAE allows PAs to easily create questionnaires that are used by the citizens in order to provide their preferences about privacy of their data (e.g., who can access, for which service, for how long, if the data can be shared, etc.). PAs use

this tool for either creating a single questionnaire for their system or multiple ones that refer only to specific services they provide. This way they can link them to citizens according to the services they wish to use. The questionnaires can also be updated with new or additional information so citizens are always up to date with the new requirements of the PAs or express their preferences if new laws or policies are applied in the PA (e.g., new European law about data protection that mandates definition of a specific confirmation or definition by the user). The answered questionnaires form the privacy policies must be followed by the PAs.

DVT The Data Value Tool (DVT) uses simple questionnaires to capture the importance of citizens data and it compares this with both the PAs' expectations and citizens' perspective. This tool calculates metrics, based on the answers of the questionnaires, and visualises the results to the users. This tool promotes the citizens' awareness about privacy since it communicates to the citizens the relative value of their data and, consequently, increases the trust of the citizens to the PA.

2.3 Privacy Enforcement and Law Compliance

In this section we present a set of tools that support run time and monitoring.

LIONoso The machine Learning and Intelligent OptimizatioN (LIONoso) tool [2] performs data analytics that focus on history based assessment and law compliance. The former consists of an analysis of the authorisations request to access citizen's data and the generation of a prediction of the possible outcomes of subsequent requests. The latter part consists of a web-based component which permits: a) specification of how PAs use/manage citizen data; b) specification of constraints imposed by regulations and laws; c) verification of the conformance of the data management specified by the PAs with the constraints specified in laws and regulations. The main purpose of this tool is to guarantee to the citizens that a PA is compliant with the law.

PAE The Privacy Agreement Enforcer (PAE) tool [11] focuses on the protection of privacy of data by providing a policy and attribute-based access control functionality that is able to evaluate permissions for accessing confidential and private data. The protection of the privacy of the citizens' data is conducted according to privacy policies, which are created automatically by PAE, using as basis the privacy preferences defined by the citizens. Furthermore, this tool allows to automatically update and modify privacy preferences from computer-medium level (formatted) to computer-low level (policies). Additionally, the tool is able to evaluate requests for accessing private data against these policies, checking the different policies that apply to that specific data and enforce the result. The purpose of this tool in the context of e-government services is to secure and protect the access to the citizens' data by using as input the information of their privacy preferences and translating it to low level policies. Finally, PAE promotes accountability in e-government by processing and recording every access to the citizens' data and, if necessary, provides information on rejected data requests.

MANE The Media Aware Network Element (MANE) tool is responsible for monitoring and filtering the network traffic. It acts as an extra layer of data protection by applying access rules according to the data received from PAE. MANE provides additional protection of the privacy of citizens' data in the system as it monitors data exchange between a system storing sensitive data and a system that requests these data. MANE monitors exchanged packages by analysing, among other information, the data and the requester and then checks if the requester is in the white list of allowed accesses. If not then it prevents the host system from sending any data and registers and attempt of unauthorised access. The purpose of this tool is not only to control data requests to a system but also to monitor all data traffic in order to detect unauthorised transmissions. The control of the accesses is obtained from PAE, which, as we described previously, generates the privacy policies of the protected data. The automatic and continuous communication between these two tools guarantees that the data protection mechanism is always up to date.

3 THE VISION PRIVACY PLATFORM

In this section, we present the VisiOn Privacy Platform (VPP) which is designed to enable PAs, legal advisors, software and privacy engineers and domain experts to elicit privacy preferences from the citizens, identify privacy risks in the system-to-be and eventually propose countermeasures. Furthermore, our platform guides citizens to specify their privacy preferences and to increase their awareness about their personal data value. VPP also includes automated privacy protection mechanisms to guarantee that no personal information will leak by human error or malicious intention and therefore strengthening citizens' trust in e-government services.

3.1 VisiOn Architecture

The architecture of VPP, as shown in Figure 1, is composed of four major components namely, the Desktop Framework, the Web Framework, the VisiOn Database (VDB) and the Visualisation tool (Vito).

The Desktop Framework is composed of the STS-Tool, SecBPMN2 SecTro, JTrust and CARiSMA. These tools, as described in the previous section, allow PAs to capture the privacy and security requirements for their systems in the diagrams of their respective modelling languages. These diagrams are stored in the VDB as well as additional information that is used to guide the privacy preferences elicitation from the citizens and the privacy policies that PAs will apply.

The Web Framework consists of LIONoso, PAE, MANE, DAE and DVT and offers four main functionalities: i) assists PAs to create privacy policies; ii) ensures that these policies conform to existing laws; iii) allows citizens to state and update their privacy preferences; iv) ensure that the privacy policies are respected. The main output of this framework is the Privacy Level Agreement (PLA), a bilateral contract between a citizen and a PA which states how the latter shall handle the data of the first one, based on the provided privacy preferences and the guarantees offered by the system on security aspects. The PLA, an example of it is depicted in Figure 2, embodies the privacy policy that must be applied for each citizen.

For creating a PLA, the PA administrators provide an initial set of questions as input to the Web Framework which later on is enriched with metadata that support the automatic processing of

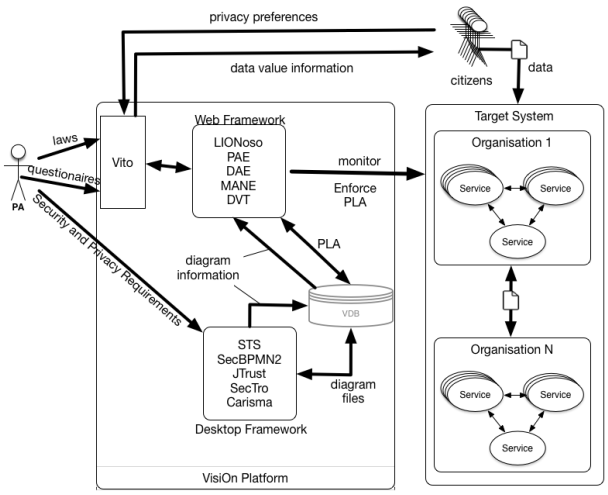


Figure 1: The VisiOn Privacy Platform Architecture

questions and their answers. These metadata provide information for the origin and the value of the data related to a question, who is responsible for handling, what operations is allowed to perform with these data, etc. The metadata generation is operated by the diagram information coming from the tools of the Desktop Framework and the DVT tool. Next, the citizens are requested to answer this questionnaire to state their privacy preferences. The answers are exported along with the questions and their metadata to the VDB in two different formats. One format contains questions, answers and metadata in a machine-readable document, the other format is a typeset textual representation of the filled questionnaire excluding the metadata and intended to be displayed in the PLA document.

The PLA is populated with security and privacy reports in order to demonstrate the compliance level of the PA privacy policies with privacy laws and increase citizens' awareness on data valuation. Towards this direction, CARiSMA performs security and privacy checks on the PA systems and generates reports with the results, which will be contained in the PLA of each citizen. Then, LIONoso is responsible to check the compliance of the information treatment declaration of the PA system with EU and the PAs' country's privacy laws in order to assess citizens' privacy requirements coverage, based on both historical values and monitoring results. Finally, DVT provides an indication to citizens regarding their perception of the value of their data using enhanced visualisation elements.

At runtime, the purpose of the Web Framework and in particular PAE, MANE and LIONoso, is twofold. First, it allows to monitor events and traffic within the PA's system in order to provide to the citizens and the PAs the means of controlling who is requesting the data and ensure that the privacy preferences set by the citizen are being fulfilled. Second, it enables the evaluation of requests, based on citizens' privacy preferences. The main goal is to ensure that the privacy preferences of the citizens control the accesses to their data. Therefore, these preferences will be taken into account by the platform for evaluating every received request of their data.

The Visualisation Tool (ViTo) was created specifically for VPP. The purpose of this tool is to provide a web interface for the tools of the Web Framework and, in the back-end, to generate the PLA documents for each citizen, which are stored in and retrieved from the VDB. The interface provided by ViTo allows PAs to submit and refine their questionnaire. Moreover, it allows citizens to answer the questionnaire and display information about the value of the data the questions refer to. ViTo is also responsible to download on demand the PLA when requested by a citizen. Such software is essential for the VPP since it eases the access of citizens to their data, increasing the transparency of a PA system. The generation of the PLA is central for increasing the trust the citizens have in the PAs.

3.2 The VisiOn Privacy Platform Process

The VPP, when applied in a PA system, is operated in three phases. The first two phases, namely Requirements Specification and PLA Generation are executed at design time, whereas the third, named PLA enforcement is executed at runtime. Below we describe the steps of each phase.

Requirements Specification Phase. In the first of the three phases the PA administrator along with the IT experts of the organisation use the Desktop Framework tools in order to capture the requirements and the structure of the system-to-be, by performing the following steps:

Step 1: The PA administrator uses the STS-tool to perform a privacy analysis of their system. More specifically, the PA graphically represents the organisational structure of the modelled system, i.e. which entities participate, what are their goals and how they interact with each other. The model includes privacy requirements (e.g., if a document is confidential or not) that are associated with the transmission of citizens' information among various entities within the system.

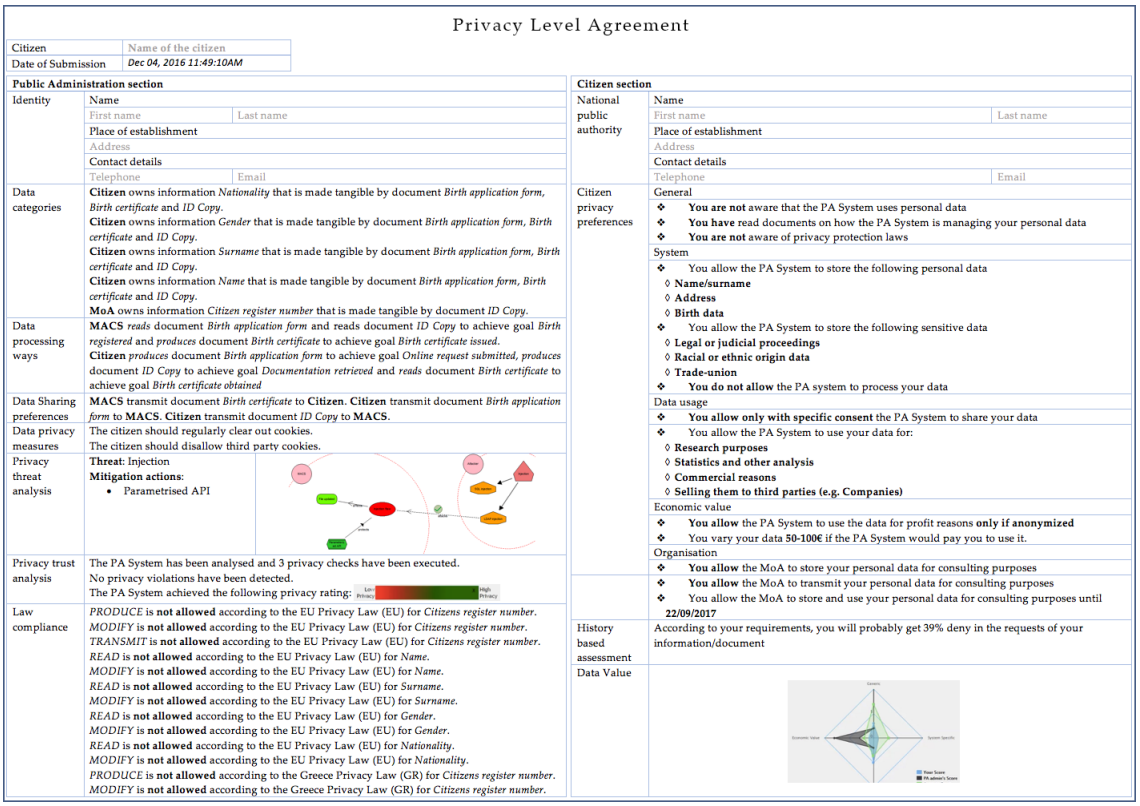
Step 2: With SecBPMN2 tool, the PA administrator models the business processes that are executed at the PA system and checks if security policies, derived from privacy requirements from Step 1, are satisfied by the business processes.

Step 3: The PA administrator uses the SecTro tool which imports the organisational structure and the privacy requirements, that are modelled in the STS-tool. The import is done through XSLT transformations [1] in order to convert the diagram from one modelling language to the other. In the converted model, the PA associates threats to the fulfilment of the privacy and security requirements and vulnerabilities of the PA system and uses a pattern library to propose mechanisms that will mitigate them.

Step 4: The PA administrator uses JTrust which imports the same model as in Step 3. In this step, the PA models and analyses the trust relationships among the entities that participate in the PA system. When an entity is not considered sufficiently trustworthy in order to fulfil the goals that are assigned with, control mechanisms are introduced to enhance the trust to the system. For example, if a system user cannot be trusted to change their password often, the PA administrator introduces a control mechanism that monitors the last time the password was changed and deactivates the account of the user, unless they update their password.

Step 5 The PA administrator uses CARiSMA to model the architecture of the PA system by using UMLsec. Then, the former performs

[1] https://www.w3.org/TR/xslt



Privacy Level Agreement

Citizen	Name of the citizen
Date of Submission	Dec 04, 2016 11:49:10AM

Public Administration section

Identity	Name First name — Last name Place of establishment Address Contact details Telephone — Email
Data categories	**Citizen** owns information *Nationality* that is made tangible by document *Birth application form, Birth certificate* and *ID Copy*. **Citizen** owns information *Gender* that is made tangible by document *Birth application form, Birth certificate* and *ID Copy*. **Citizen** owns information *Surname* that is made tangible by document *Birth application form, Birth certificate* and *ID Copy*. **Citizen** owns information *Name* that is made tangible by document *Birth application form, Birth certificate* and *ID Copy*. **MoA** owns information *Citizen register number* that is made tangible by document *ID Copy*.
Data processing ways	**MACS** *reads* document *Birth application form* and reads document *ID Copy* to achieve goal *Birth registered* and *produces* document *Birth certificate* to achieve goal *Birth certificate issued*. **Citizen** *produces* document *Birth application form* to achieve goal *Online request submitted*, *produces* document *ID Copy* to achieve goal *Documentation retrieved* and *reads* document *Birth certificate* to achieve goal *Birth certificate obtained*
Data Sharing preferences	**MACS** transmit document *Birth certificate* to **Citizen**. **Citizen** transmit document *Birth application form* to **MACS**. **Citizen** transmit document *ID Copy* to **MACS**.
Data privacy measures	The citizen should regularly clear out cookies. The citizen should disallow third party cookies.
Privacy threat analysis	**Threat**: Injection **Mitigation actions**: • Parametrised API
Privacy trust analysis	The PA System has been analysed and 3 privacy checks have been executed. No privacy violations have been detected. The PA System achieved the following privacy rating:
Law compliance	*PRODUCE* is **not allowed** according to the EU Privacy Law (EU) for *Citizens register number*. *MODIFY* is **not allowed** according to the EU Privacy Law (EU) for *Citizens register number*. *TRANSMIT* is **not allowed** according to the EU Privacy Law (EU) for *Citizens register number*. *READ* is **not allowed** according to the EU Privacy Law (EU) for *Name*. *MODIFY* is **not allowed** according to the EU Privacy Law (EU) for *Name*. *READ* is **not allowed** according to the EU Privacy Law (EU) for *Surname*. *MODIFY* is **not allowed** according to the EU Privacy Law (EU) for *Surname*. *READ* is **not allowed** according to the EU Privacy Law (EU) for *Gender*. *MODIFY* is **not allowed** according to the EU Privacy Law (EU) for *Gender*. *READ* is **not allowed** according to the EU Privacy Law (EU) for *Nationality*. *MODIFY* is **not allowed** according to the EU Privacy Law (EU) for *Nationality*. *PRODUCE* is **not allowed** according to the Greece Privacy Law (GR) for *Citizens register number*. *MODIFY* is **not allowed** according to the Greece Privacy Law (GR) for *Citizens register number*.

Citizen section

National public authority	Name First name — Last name Place of establishment Address Contact details Telephone — Email
Citizen privacy preferences	General ❖ **You are not** aware that the PA System uses personal data ❖ **You have** read documents on how the PA System is managing your personal data ❖ **You are not** aware of privacy protection laws System ❖ You allow the PA System to store the following personal data ◊ **Name/surname** ◊ **Address** ◊ **Birth data** ❖ You allow the PA System to store the following sensitive data ◊ **Legal or judicial proceedings** ◊ **Racial or ethnic origin data** ◊ **Trade-union** ❖ **You do not allow** the PA system to process your data Data usage ❖ **You allow only with specific consent** the PA System to share your data ❖ You allow the PA System to use your data for: ◊ **Research purposes** ◊ **Statistics and other analysis** ◊ **Commercial reasons** ◊ **Selling them to third parties (e.g. Companies)** Economic value ❖ **You allow** the PA System to use the data for profit reasons **only if anonymized** ❖ You vary your data **50-100€** if the PA System would pay you to use it. Organisation ❖ **You allow** the MoA to store your personal data for consulting purposes ❖ **You allow** the MoA to transmit your personal data for consulting purposes ❖ You allow the MoA to store and use your personal data for consulting purposes until **22/09/2017**
History based assessment	According to your requirements, you will probably get 39% deny in the requests of your information/document
Data Value	

Figure 2: Example of a PLA

a security analysis in order to verify if the architecture satisfies the requirements imported from STS. The verification process includes checks on the security level of the communication among the components of the architecture.

Step 6: The PA administrator uses LIONoso to perform compliance check of the PA system against laws and regulations. More specifically, LIONoso permits to define the constraints specified by laws and regulation, and the operation executed by the PA system on citizens data. Then, the tool controls if the constraints are violated. If the model is found compliant, i.e. the laws are not violated, then the phase terminates, otherwise the PA must modify the system, starting from Step 1.

PLA Generation Phase. In the next phase, the PLA is generated by using the questionnaires provided by the PA and the answers given by the citizens.

Step 1: The PA administrator accesses DAE through ViTo, which guides the citizen to create questions to the citizens about the PA system and how they wish their data to be treated. DAE also collects the diagram information from the STS models and in particular what access rights are documented for each piece of data transmitted within the PA system. Then, the PA administrator forms questions accordingly to ask the citizens if they agree with these access rights.

Step 2: The PA administrator assigns scores to evaluate the sensitivity of the data mentioned in the questions. These values are inserted to DVT which presents in web diagram the value of the data mentioned in the PLA from a) the PA's perspective; b) the citizen's perspective; and c) an average of both.

Step 3: The PA administrator publishes the questionnaire.

Step 4: The citizens answer the questionnaire and provide their values for the sensitivity of their data.

Step 5: PAE collects the citizens' answers and creates privacy policies that will be continuously monitored in the next phase.

Step 6: For each citizen that answers a questionnaire, ViTo gathers the responses from the citizens, the related laws, the diagram information, including the security and trust analysis results and the data value of the citizen's data. This information composes the PLA for this citizen.

PLA Enforcement Phase. Every time there is a request for accessing data of a citizen, then the policies, dictated by the PLA, should be respected. This phase takes place at runtime and is implemented in the following steps:

Step 1: PAE receives a new request from an external entity to access data provided by a citizen and controls, based on the privacy policies created by the answers of the citizens to the questionnaires, if the access should be permitted or denied. Moreover, PAE sends notifications through ViTo to the citizen when someone attempts to access their data.

Step 2: MANE updates the network traffic rules based on PAE's feedback. Therefore, if the access by the entity is permitted or denied by PAE, MANE will form a rule to permit or deny respectively future requests from the same entity for the same data.

Step 3: The logs created by PAE and MANE that contain information about the amount of requests which were denied or permitted, are inserted in LIONoso. The latter, performs a history based assessment and provides in the PLA page of the citizen a value about how the percentage of the requests to their data will be denied.

4 CASE STUDY

To better illustrate the functionalities and the benefits of VPP we present how it is applied in a real-world system which is part of the pilot stage of our project. The system belongs to DAEM S.A., a government organisation that develops e-government services for the Municipality of Athens (MoA) and other local government organisations in Greece. More specifically, DAEM S.A. is responsible for the development and maintenance of the Municipality of Athens Computer Services (MACS), an information system of MoA that stores and manages personal data of Athenian residents.

4.1 Motivating Scenario

MACS is integrated with information systems of other organisations such as hospitals, banks, the fiscal office, sports facilities and many others. The main purpose of MACS is to interconnect such organisations, store and transmit information that belongs to a citizen upon request (e.g., birth certificates) without requiring the citizen's physical presence. In our scenario, the citizen wishes to buy a subscription at a local Swimming Pool facility. Athenian residents, i.e. greek citizens whose permanent residence is registered in the city of Athens, have the right of a 10% discount. As proof of their residence, they are required to provide the facility with a birth certificate.

This certificate is provided directly by MACS to the information system of the swimming pool as part of the e-government services in the MoA. The request will be triggered when the citizen visits the swimming pool for the first time to buy their subscription. It is also required that the citizen provides a medical certificate to prove that they do not have any skin condition. This certificate can be provided by the citizen, who needs first to visit their physician. In case the citizen has recently received a medical certificate which is stored in the clinic's database, MACS is able to retrieve it and forward it to the information system of the swimming pool facility.

The citizen, in order to access the area of the swimming pool in the facility, uses a badge. Each entrance is stored in the database of the information system and can be used to make personalised offers to the citizen. For example, such offers include higher discount for less popular hours or when the swimming pool is most busy.

In this scenario, there are three types of data of the system that will be handled by the PA system; a birth certificate, a medical certificate and the swimming pool access logs. Given that MACS is interconnected with numerous swimming pool facilities around Athens and other services, the citizen must provide their privacy preferences about which information wishes to be shared and how. Furthermore, the citizen, without knowing who is accessing their data might be reluctant to share it and eventually use MACS. This means that the PA administrators of MoA must guarantee the transparency of the data sharing process with other organisations. Finally, to avoid citizens blindly denying or permitting access to all their data, it is crucial to a) increase the awareness of the value of the shared data and b) inform the citizens about the mechanisms applied to protect their privacy.

4.2 Applying the VisiOn Privacy Platform

Hereby, we describe how VPP is integrated with MACS and illustrate execution instances of the three phases that we described in Section 3. Note that both MACS and VPP are installed in the premises of the MoA. Additionally, the data requested by each external service is always provided from or through MACS.

During the Requirements Specification phase, the administrators of MoA use the tools of the Desktop Framework to capture the organisational settings of the system and perform security and trust analysis. Given that multiple administrators might be working on the same models, and, therefore the Desktop Framework has more than one instances, a locking mechanism has been implemented in the VDB to avoid synchronisation issues.

First, the administrators of MoA design the STS-ml model of their system which describes the goals of each entity that participate in their system. In Figure 3, a partial STS-ml model is depicted which illustrates four actors, the Citizen, the Clinic, MoA which hosts the MACS system and the Swimming Pool (SP) Information System. The exchange of information that is captured in this model is annotated with privacy requirements. More specifically, the transmission of the medical certificate is associated with three requirements, i) confidentiality, i.e. the information is not disclosed to any unauthorised entity, ii) integrity, i.e. the information is not modified by any unauthorised entity and iii) undetectability, i.e. the inability for a third party to distinguish who is the user (among a set of potential users) using a service.

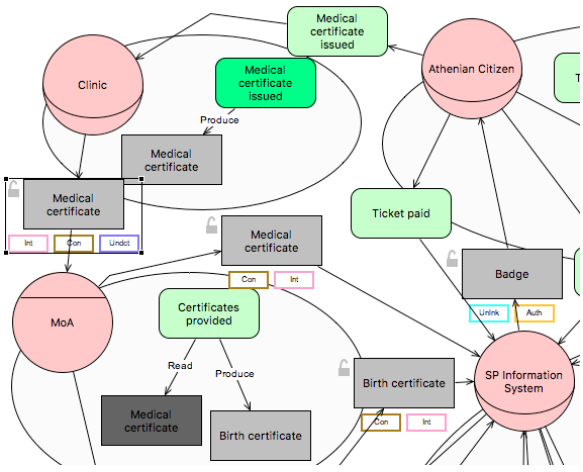


Figure 3: Example of a partial STS-ml diagram

Next, the MoA administrators design the business processes that are implemented by MACS and the interaction with other systems, by using SecBPMN2. Figure 4 shows portion of a SecBPMN2 diagram for our scenario. In particular, the tool specifies two activities executed by the SP information system. The first activity, Arrange ticket price, changes the price of the entrance ticket, by using the Visiting Time Record which is created by the Citizen. The activity Allow access reads the Medical certificate and stores it in the

Date	Resource	Subject	Role	Purpose	Action	Response
10 March 2017	MoACitizenXTA348065	SP_UserLT45675	SP_Administrative	read access log	Read	Deny

Table 1: Privacy policy from PAE

local database, allowing the citizens to access the SP information system. SecBPMN2 extends BPMN 2.0 with security and privacy annotations, which are represented with orange solid circles. In this case, the medical certificate is associated to an integrity annotation, which means that only authorised users can modify the document. The non-repudiation annotation is linked to the second activity, and it specifies that the SP information system must store a proof of the execution of that activity.

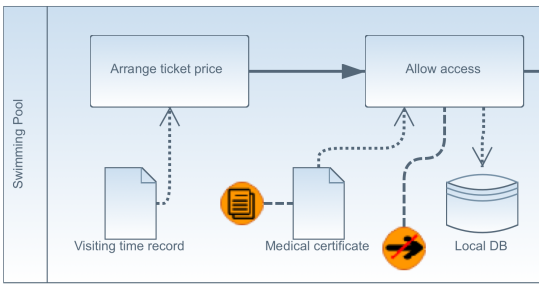


Figure 4: Example of a partial SecBPMN2 diagram

Then, the MoA administrators use the SecTro tool in order to enrich the STS-ml model with security requirements. Figure 5 depicts the privacy requirement Prevent unauthorised detection, identified previously with STS, which is modelled as a privacy constraint that restricts the use of the resource Medical certificate. The privacy objective therefore that satisfies the privacy constraint is to achieve undetectability with regards to the Medical certificate of the citizen. Privacy mechanisms are stored in a library of tools and specific ones can be selected according to the needs of each case. In this case, a set of administrative tools was selected, such as smart cards and permission management, along with a set of anonymizer mechanisms, such as Hordes, GAP, and Tor. This analysis enables the justification of why specific privacy and security mechanisms need to be placed and added to the PLA to assure the citizen about the level of their privacy protection and increase their trust in the service provided by MoA.

For the next step of this phase, the MoA administrators construct with the use of JTrust tool a trust model, as shown in Figure 6, where the citizen depends on the SP information system to have their visiting time kept confidential. This dependency implies a trust relationship between the Citizen and the SP information system. The trust relationship is justified with reported trust, i.e. MoA reports that the SP information system can be trusted to keep the visiting time confidential. Such information is elicited as part of the domain investigation and analysis. As a result, there is an underlying assumption that MoA can be trusted, represented with an ellipse symbol. Consequently, a new dependency is introduced on MoA for the validity of what is reported. The newly introduced dependency, and therefore trust relationship, is justified with normative trust,

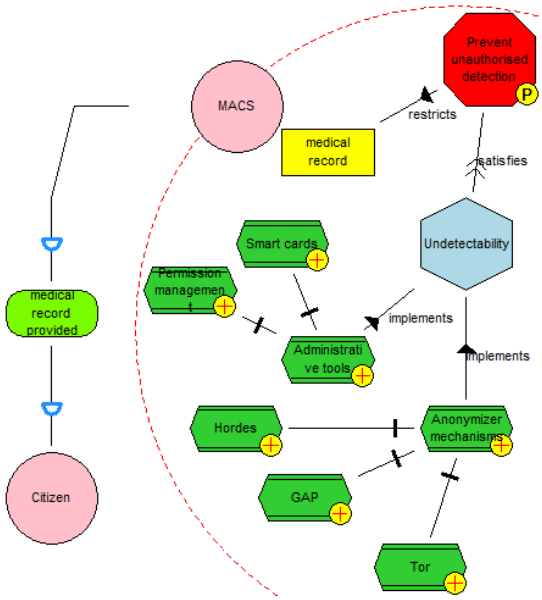


Figure 5: Example of a partial SecTro diagram

which is trust that is based on the norms of the system's environment. This information was elicited during the domain analysis. Likewise, there is an underlying assumption that the domain norm can be trusted. These two identified assumptions were further investigated and found to be valid. The developed model enabled the identification and justification of trust assumptions that underlie the analysis in order to be sound. In case there was lack of trust then control mechanisms would have to be added in order to enforce the fulfilment of goals such as visiting times to be kept confidential.

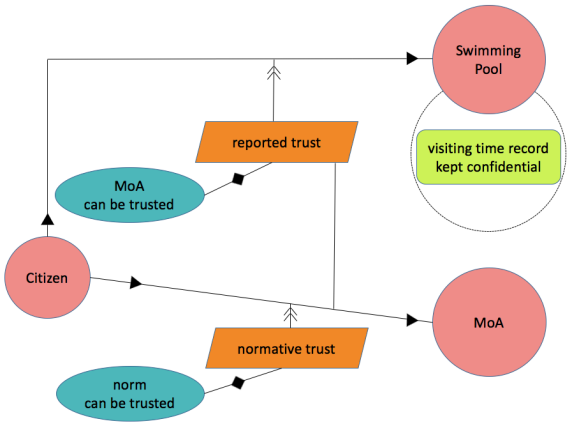


Figure 6: Example of a partial JTrust diagram

Date	Resource	Subject	Requested URL	Requesting IP	Response
10 March 2017	MoACitizenXTA348065	SP_UserLT45675	1.2.3.4:9999/log/179	5.6.7.8	Deny

Table 2: Network traffic rule from MANE

The use of the Desktop Framework is completed with CARiSMA, where the MoA administrators design the system's architecture by using UMLsec. The security annotations over the elements of the UML diagram are inserted from the STS-ml model. Then, the tool performs checks to validate if the architecture satisfies the security requirements. For instance, in our design the component that represents the information system of the a citizen's clinic is connected with the component that represents MACS. Given that this transmission is annotated with a confidentiality requirement in STS-ml model on the side of the sender and the receiver, a security annotation must be added to both components, otherwise the checks performed by the tools will fail. This guarantees that the engineers of the system will implement all the necessary security measures to guarantee the protection of the citizen's data.

The Requirements Specification process concludes with the compliance check of LIONoso which receives the three types of data transmitted through the system from the STS-tool. The MoA administrators must insert through ViTo the Greek and EU privacy laws related to these types of data. Then, they specify through the same interface the operations that are applied over this data, e.g., MoA produces birth certificate. When all operations and the subjects who perform them are defined, LIONoso checks if the prescribed operations are compliant with the existing laws.

When the system is verified by LIONoso to be compliant with the existing privacy laws, the MoA administrators proceed with the creation of the questionnaires with the use of DAE through ViTo. The website guides the administrators on the creation of the questions by demonstrating information derived from the STS model. In particular, DAE suggests to the administrators to create questions related to the storage and the transmission of the data that are modelled in STS. For example, a few questions submitted are: i) 'Do you allow third parties to store your medical certificate?', ii) 'Do you allow sharing your birth certificate with third party organisations?', iii) 'Do you allow your access log to sport facilities to be used for commercial purposes?'.

When registering to MACS, the citizen has to answer a set of answers about which organisations that are integrated with MACS authorises to access their personal data and to handle them. For instance, they are asked if they wish the sport facilities that they are visiting to store and use for commercial use their visiting time record. DVT also provides them the information that this type of data is useful for the sport facilities organisations in order to schedule their opening times and pricing policies. By sharing this information in the future, they could also receive personalised offers. Moreover, DVT informs that most citizens do not share this information, probably due to privacy concerns. After the questionnaire is published, every citizen when registering to MACS has to answer it. These answers formulate the privacy policies in PAE and ViTo generates and displays the PLA to each citizen.

After a few visits in the swimming pool, the SP information system will attempt to read the visiting time record of the citizen. PAE will receive this request and will check if this action is allowed, based on the PLA of the citizen. If the citizen forbids sport facilities to use their visiting time record for commercial purposes, then PAE has a policy, as the one shown in Table 1. The outcome of both PAE and MANE is forwarded as input to LIONoso which updates the number of requests to documents are being denied and display it in the PLA.

After the request arrives at PAE, the result of the request, in this case is 'Deny', is forwarded to MANE, which creates network traffic rules, as the one shown in Table 2. This will cut automatically future requests to this piece of information. Moreover, a notification will be sent to the citizen about who tried to access their data and the result of the attempt.

If a malicious user or unauthorised entity attempts to access the citizen's data, VPP will reject the request and inform the citizen about who requested access to their data. Hence, the citizen is continuously updated about who is accessing their data. This increases the trust of citizens in the PA as they will see system protects and informs of all accesses, being this valid or not. For example, if an administrator who works for the Swimming pool tries to access their Visiting Time record or their Medical certificate, the citizen receives a notification (e.g., via SMS) about who accessed their data, when and for what purpose.

The process that takes place at system level is the following. First, the information system of the Swimming pool which is integrated with MACS and VPP, sends the request of data to the latter. Then, PAE processes this request and, using the privacy policies defined by the citizen's answers, detects the request is unauthorised. PAE registers this denied access and sends the information to LIONoso, which will process and display this information in the VPP as a new notification so the citizen, when accessing the system next time, can check it. Additionally, PAE will send the response of the request to the system informing about the denial of the request because of unauthorised permission. Additionally, VPP has a second line of protection of privacy of the data which is MANE. Therefore, if a malicious user would be able to retrieve the data from the database, using a third-party application that access directly to the data storage, MANE would check continuously the exchange of data in order to detect unauthorised accesses. If detected, it compiles the information and sends to LIONoso for notification to the citizen and the PA, as this illegal access could be a potential security weakness in the system. Consequently, the PA could use this information for revision of the security architecture of its system.

4.3 Discussion

Our platform with the use of the Desktop Framework of the tools allowed PA administrators to identify and model with the STS and SecBPMN2 tools all the nodes (organizations, physical persons etc.) that the citizens' data pass through and define the access rights of each one of them based on their goals. These modes offer better understanding of how e-government systems operate and what are

the risks related to private data. Additionally, by using SecTro and CARiSMA the PA administrators are able to systematically identify the potential threats and vulnerabilities of their systems, propose defence mechanism and assess through various types of analyses the security level of the modelled system. The defence mechanisms and how they mitigate the identified threats are also presented in the PLA in order to increase the citizens' trust to the PA system. The analyses performed by JTrust also contributes towards this direction, by justifying why each node of the system can be trusted or not and provide this information through the PLA.

Despite the high level of maturity of the modelling languages of the Desktop Framework tools, training the pilot partners of the VisiOn project to use them has been a cumbersome task. The main reason was the reduced capacity of the pilots to provide multiple experts in the areas of software and security engineering along with domain experts in order to collaboratively produce the required diagrams,. To overcome this difficulty we organized workshops, tutorials and webinars which permitted our pilots to successfully use our tools and minimise the risk of human error. The user satisfaction has been confirmed during the evaluation process of our platform, where each pilot demonstrated the use of the platform, as it is integrated in their systems, and provided questionnaires[2].

Another contribution of our platform is the facilitation of the questionnaire creation for gathering privacy preferences from the citizens by DAE and ViTo. More specifically, the diagram information provided by the tools of the Desktop Framework guides the PA administrators to ask question about every data that is circulated within their system, ensuring the completeness of the privacy policies that will be composed from the answers. Moreover, by taking into account the opinion of the citizens on how they wish their data to be treated and customizing the privacy policies based on their preferences, VPP increases citizens' trust in e-government services. This can also be confirmed by the results of the aforementioned pilot evaluation. VPP also increases the awareness of the citizens about the value of their data and enables them to choose more carefully how they want their data to be managed in order to prevent future dissatisfaction.

Finally, The automated privacy enforcement provided by PAE and MANE relieves the PAs from the burden of performing manually regular audits on their systems to evaluate the level of privacy protection. These tools also promote transparency and accountability in e-government by capturing who requests what data, for what purpose and notify the citizen about these requests.

5 RELATED WORK

Various approaches have been proposed in the literature for systematically capturing privacy requirements. The Privacy Safeguard (PriS) [14] methodology enables the elicitation of privacy requirements in the software design phase, where privacy requirements are modelled as organisational goals. Next, in [25] the authors adopt the concepts of privacy-by-policy and privacy-by-architecture, and propose a three-sphere model of user privacy concerns, relating it to system operations (i.e. data transfer, storage and processing). Additionally, the Modelling and Analysis of Privacy-aware Systems (MAPaS) framework [6] is a framework for modelling requirements for privacy-aware systems. The ABC4Trust project [23] protects privacy in identity management systems. Differently than these works, VPP provides a start-to-end implementation of a privacy management approach that takes into account the PbD principles, since it starts with the elicitation of the user privacy needs and it ends with the provision of PA online services.

Trust analysis is yet another contributor to effective privacy management. A trust analysis method is proposed in [27] where the authors address the issues of trust at a requirements level and treat trustworthiness as an objective of the stakeholders. Next, in [12] the system analysis and design considers different domains in mobile communications. Additionally, in [9] the authors propose a method for discovering trade-offs that trust relationships bring between trust and control. Compared to these approaches our work is applicable to PA organisations and the described platform facilitates the identification of organisational controls that will ensure privacy of citizens' data.

Recently, quite a few commercial products have been developed that highlight the importance of the individuals' data protection. The TRUSTe[3] platform focuses on Data Privacy Management (DPM), enabling users to take control of a set of technology-driven solutions for managing privacy challenges. Disconnect[4] is a software that facilitates users to easily understand the websites' privacy policies and realise how websites are handling their data. The common characteristic of these products is that they focus on the better analysis and comprehension of each privacy policy, protecting user from actions that will put their personal data in danger. Contrary to these products, VPP elicits from both sides (service providers and service consumers) their privacy preferences, developing personalised PLAs, according to them.

The Information Shield[5] provides a repository containing all the necessary material that can assist companies and organisations to formalise or update their privacy policies, maintaining them compliant with the relevant laws and regulations, at national and international level. Nymity[6] enables organisations to use an accountability approach to demonstrate data privacy compliance. 2B Advice[7] is a group of companies offering consulting services concerning data privacy advice, software solutions and certifications. Otris privacy[8] is a software for data protection management, focusing on the planning, setting-up, operation and decommissioning of data processing methods. OneTrust[9] platform ensures the data privacy compliance, helping service providers to guarantee to their service consumers that they are compliant with the laws and the privacy policies. As opposed to these works, VPP follows a holistic approach in order to create each PLA, conducting security and privacy analysis of the information systems of each service provider, and ensuring that their processes are law compliant and based on these results, it retrieves the privacy preferences of a service consumer.

[2]The statistical results of the answers to the questionnaire of one of the VisiOn pilots https://sense-cloud.brighton.ac.uk:5001/sharing/Fdkk9aCNl

[3]https://www.truste.com
[4]https://disconnect.me/icons
[5]https://informationshield.com/
[6]https://www.nymity.com
[7]https://www.2b-advice.com
[8]https://www.otris.com/products/data-protection-management/
[9]https://onetrust.com

6 CONCLUSIONS

In this paper we presented a novel platform that improves privacy in Public Administration. In particular, VPP provides PAs with the ability to create citizen's PLAs using citizen privacy preferences, which are elicited through clear and non-technical questionnaires. Also, VPP enables citizens to understand the value of their data, using enhanced visualisation elements, and use that value to determine their privacy preferences. Moreover, VPP brings together a set of software engineering methodologies and tools across different levels, from privacy requirements to run-time, and different perspectives, from data evaluation to privacy assurance. Such integration provides a clear advantage over existing software engineering approaches and tools, since it enables a holistic analysis of privacy needs that includes both PAs and citizens. Moreover, VPP is the only platform in the literature, which we are aware of, that identifies and analyses privacy threats for PAs and it enables them to allow citizens to indicate their preference for the potential privacy mechanisms that can be used to countermeasure the identified threats.

The project is strongly linked to citizens and PA authorities, and therefore provides socially important impacts. In particular, VPP increases user trust and confidence in PA online services, therefore decreasing the number of users that are reluctant to use such services. VPP enables, on one hand, PAs to manage private data in an accountable and transparent way, and on the other hand, it provides citizens with the ability to control their privacy when they must share their personal data with PAs. Moreover, VPP makes transparency and accountability inherent characteristics of all activities related to citizens' data within PAs. Monitoring how this data is used after it has been given to PAs is one of the main functionalities of VPP provided by the Web Framework. This, along with the enforcement of PLA, plays a critical role in the maximisation of transparency and accountability.

ACKNOWLEDGMENT

The authors would like to thank DAEM S.A. for providing us with information about the e-government services of the MoA and the consortium of the VisiOn Project for their effort in the realisation of this work. This paper is supported by European Union Horizon 2020 research and innovation programme under grant agreement No 653642, project VisiOn (Visual Privacy Management in User Centric Open environments).

REFERENCES

[1] Data Protection Act. 2014. Conducting privacy impact assessments code of practice. (2014).
[2] Roberto Battiti and Mauro Brunato. 2014. *The LION way. Machine Learning* plus *Intelligent Optimization*. LIONlab, University of Trento, Italy.
[3] France Bélanger and Lemuria Carter. 2008. Trust and risk in e-government adoption. *The Journal of Strategic Information Systems* 17, 2 (2008), 165–176.
[4] Grady Booch, James Rumbaugh, and Ivar Jacobson. 2005. *Unified Modeling Language User Guide, The (2nd Edition)*. Addison-Wesley Professional.
[5] Sofia Elena Colesca. 2009. Increasing e-trust: A solution to minimize risk in e-government adoption. *Journal of applied quantitative methods* 4, 1 (2009), 31–44.
[6] Pietro Colombo and Elena Ferrari. 2012. Towards a modeling and analysis framework for privacy-aware systems. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*. IEEE, 81–90.
[7] Fabiano Dalpiaz, Paolo Giorgini, and John Mylopoulos. 2013. Adaptive Socio-Technical Systems: a Requirements-driven Approach. *Requirements Engineering* 18, 1 (2013), 1–24. Issue 4.
[8] F. Dalpiaz, E. Paja, and P. Giorgini. 2011. Security Requirements Engineering via Commitments. In *Proceedings of workshop on Socio-Technical Aspects in Security and Trust*. 1–8.
[9] Golnaz Elahi and Eric Yu. 2009. Trust trade-off analysis for security requirements engineering. In *2009 17th IEEE International Requirements Engineering Conference*. IEEE, 243–248.
[10] Rebecca Eynon. 2007. Breaking Barriers to eGovernment: Overcoming obstacles to improving European public services. *DG Information Society and Media. European Commission* 90 (2007).
[11] Mohamad Gharib, Mattia Salnitri, Elda Paja, Paolo Giorgini, Haralambos Mouratidis, Michalis Pavlidis, José F Ruiz, Sandra Fernandez, and Andrea Della Siria. 2016. Privacy Requirements: Findings and Lessons Learned in Developing a Privacy Platform. In *Proceedings of Requirement Engineering (RE) conference*.
[12] Janusz Górski, A Jarzebowicz, Rafal Leszczyna, Jakub Miler, and Marcin Olszewski. 2005. Trust case: Justifying trust in an IT solution. *Reliability Engineering and System Safety* 89, 1 (2005), 33–47.
[13] J. Jurjens. 2002. UMLsec: Extending UML for Secure Systems Development. In *Proc. of UML*. 412–425.
[14] Christos Kalloniatis, Evangelia Kavakli, and Stefanos Gritzalis. 2008. Addressing privacy requirements in system design: the PriS method. *Requirements Engineering* 13, 3 (2008), 241–255.
[15] Günter Karjoth and Matthias Schunter. 2002. A privacy policy model for enterprises. In *Computer Security Foundations Workshop, 2002. Proceedings. 15th IEEE*. IEEE, 271–281.
[16] Günter Karjoth, Matthias Schunter, and Michael Waidner. 2002. Platform for enterprise privacy practices: Privacy-enabled management of customer data. In *International Workshop on Privacy Enhancing Technologies*. Springer, 69–84.
[17] Gang-Hoon Kim, Silvana Trimi, and Ji-Hyong Chung. 2014. Big-data applications in the government sector. *Commun. ACM* 57, 3 (2014), 78–85.
[18] Marco Casassa Mont and Robert Thyne. 2006. A systemic approach to automate privacy policy enforcement in enterprises. In *International Workshop on Privacy Enhancing Technologies*. Springer, 118–134.
[19] Haralambos Mouratidis, Nikolaos Argyropoulos, and Shaun Shei. 2016. *Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach*. Springer International Publishing.
[20] OMG. 2011. *BPMN 2.0*. Technical Report. OMG. http://www.omg.org/spec/BPMN/2.0
[21] European Parliament. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Coucil of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). http://eur-lex.europa.eu/legal-content/EN/TXT/
[22] Michalis Pavlidis, Shareeful Islam, Haralambos Mouratidis, and Paul Kearney. 2014. Modeling trust relationships for developing trustworthy information systems. *International Journal of Information System Modeling and Design (IJISMD)* 5, 1 (2014), 25–48.
[23] Ahmad Sabouri and Kai Rannenberg. 2015. *ABC4Trust: Protecting Privacy in Identity Management by Bringing Privacy-ABCs into Real-Life*. Springer International Publishing, Cham, 3–16. DOI: http://dx.doi.org/10.1007/978-3-319-18621-4_1
[24] Mattia Salnitri, Elda Paja, and Paolo Giorgini. 2016. Maintaining secure business processes in light of socio-technical systems' evolution. In *Proceedings of Model Driven Requirement Engineering Workshop*.
[25] Sarah Spiekermann and Lorrie Faith Cranor. 2009. Engineering privacy. *IEEE Transactions on software engineering* 35, 1 (2009), 67–82.
[26] Aprna Tripathi and Bhawana Parihar. 2011. E-governance challenges and cloud benefits. In *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on*, Vol. 1. IEEE, 351–354.
[27] Eric Yu and Lin Liu. 2001. Modelling trust for system design using the i* strategic actors framework. In *Trust in Cyber-societies*. Springer, 175–194.
[28] Peng Yu, Jakub Sendor, Gabriel Serme, and Anderson Santana de Oliveira. 2013. Automating privacy enforcement in cloud platforms. In *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 160–173.