

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7411>

Daphne Tuncer · Robert Koch
Rémi Badonnel · Burkhard Stiller (Eds.)

Security of Networks and Services in an All-Connected World

11th IFIP WG 6.6 International Conference
on Autonomous Infrastructure, Management, and Security, AIMS 2017
Zurich, Switzerland, July 10–13, 2017
Proceedings

Editors

Daphne Tuncer
University College London
London
UK

Robert Koch
Universität der Bundeswehr München
Neubiberg
Germany

Rémi Badonnel
LORIA - Inria
Villers-lès-Nancy
France

Burkhard Stiller
University of Zurich
Zurich
Switzerland



ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-60773-3

ISBN 978-3-319-60774-0 (eBook)

DOI 10.1007/978-3-319-60774-0

Library of Congress Control Number: 2017943842

LNCS Sublibrary: SL5 – Computer Communication Networks and Telecommunications

© The Editor(s) (if applicable) and The Author(s) 2017. This book is an open access publication.

Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2017) is a single-track event targeted at junior researchers and PhD students in network and service management and security. It features a range of sessions including conference paper presentations, hands-on lab courses, and educational keynotes. One of the key goals of AIMS is to offer junior researchers and PhD students a dedicated place where they can discuss their research work and experience, receive constructive feedback from senior scientists, and benefit from practical hands-on sessions on emerging technologies. By putting the focus on junior researchers and PhD students, AIMS acts as a complementary piece in the set of international conferences in the network and service management community, providing an optimal environment for in-depth discussions and networking.

AIMS 2017 — which took place during July 10-13, 2017, in Zürich, Switzerland, and was hosted by the University of Zürich — was the 11th edition of a conference series on management and security aspects of distributed and autonomous systems. It followed the already established tradition of an unusually vivid and interactive conference series, after successful events in Munich, Germany, in 2016, Ghent, Belgium, in 2015, Brno, Czech Republic, in 2014, Barcelona, Spain, in 2013, Luxembourg, Luxembourg, in 2012, Nancy, France, in 2011, Zürich, Switzerland, in 2010, Enschede, The Netherlands, in 2009, Bremen, Germany, in 2008, and Oslo, Norway, in 2007.

AIMS 2017 focused on security of networks and services in an all-connected world. To address these challenges, solutions for the design, monitoring, configuration, and protection of the next generation of networked systems in an efficient, secure, and smart manner are investigated. The theme is reflected in the technical program with papers presenting novel approaches and evaluation studies for the security management of rich network services and environments. AIMS 2017 was organized as a 4-day program to encourage the active participation of and interaction with the audience. The program consisted of technical sessions for the main track and PhD sessions, interleaved with three lab sessions and two keynotes.

The lab sessions offered hands-on experience in the topics of security and advanced network management techniques, and were organized in on-site labs preceded by short tutorial-style teaching sessions. The first lab session was run by Martin Drašar (Masaryk University, Czech Republic) and focused on an introduction to security games. The second lab session was supervised by Thomas Bocek and Moritz Schneider (University of Zürich, Switzerland) and presented how to program smart contracts. Finally, the last session was held by Salvatore Signorello (University of Luxembourg, Luxembourg) and Jérôme François (Inria, France) and explored P4, the emerging high-level data plane programming language and its applicability to packet processors.

The keynotes were presented by two experts in their domain: Marcel Waldvogel (University of Konstanz, Germany), who discussed “Getting Rid of IoT Insecurity,” and Matthias Bossardt (KPMG, Switzerland), who shared his view with the audience on “Cyber Security Challenges – A Business Perspective.”

The technical program consisted of six sessions, divided into three full-paper sessions and three short-paper sessions. The three full-paper sessions covered technical presentations on the themes of: (1) Security Management, (2) Management of Cloud Environments and Services, and (3) Evaluation and Experimental Study of Rich Network Services. They included a total of eight full papers, which were selected after a thorough reviewing process out of 24 submissions. Each paper received at least three independent reviews. The three short-paper sessions included 11 short papers. These covered PhD research papers on the themes of “Methods for the Protection of Infrastructure and Services,” and “Autonomic and Self-Management Solutions” as well as six short presentations on the topic of “Security, Intrusion Detection, and Configuration.”

During all the PhD research presentations, doctoral students had the opportunity to present and discuss their research ideas, and more importantly to obtain valuable feedback from the AIMS audience about their PhD research work. All PhD research proposals included in this volume describe the current state of these investigations, including well-defined research problem statements, proposed approaches, and an outline of emerging and promising results achieved to date.

The present volume of the *Lecture Notes in Computer Science* series includes all papers presented at AIMS 2017 as defined within the overall final program. It demonstrates again the European scope of this conference series, since most of the accepted papers originate from European research groups. In addition, by hosting two tracks specifically dedicated to research proposals, AIMS 2017 stayed true to its defined DNA of a conference with a strong educational goal, focusing especially on issues and challenges associated with the security of networks and services.

The editors would like to thank the many people who helped to make AIMS 2017 such a high-quality and successful event. Firstly, many thanks are extended to all authors who submitted their contributions to AIMS 2017, and to the lab session speakers as well as the keynote speakers. The great review work performed by the members of the AIMS Technical Program Committee as well as additional reviewers is greatly acknowledged. Thanks also to Thomas Bocek and Martin Drašar for organizing the lab sessions. Additionally, many thanks are extended to the local organizers for handling logistics and hosting the AIMS 2017 event.

Finally, the editors would like to express their thanks to Springer, especially Anna Kramer, for the smooth cooperation in finalizing these proceedings. Additionally, special thanks go to the AIMS 2017 supporters, University of Zürich UZH, Communication Systems Group CSG, Research Institute for Cyber Defense and Smart Data CODE, München, Germany, and the European FP7 NoE FLAMINGO under Grant No. 318488.

May 2017

Daphne Tuncer
Robert Koch
Rémi Badonnel
Burkhard Stiller



Research Institute
Cyber Defence
Universität der Bundeswehr München



NoE
FLAMINGO

Organization

General Chair AIMS 2017

Burkhard Stiller University of Zürich, Switzerland

Technical Program Committee Co-chairs

Daphne Tuncer University College London, UK
Robert Koch Universität der Bundeswehr München, Germany

Labs Co-chairs

Martin Drašar Masaryk University, Czech Republic
Thomas Bocek University of Zürich, Switzerland

Publications Co-chairs

Rémi Badonnel LORIA, Inria, France
Burkhard Stiller University of Zürich, Switzerland

Local Chair

Barbara Jost University of Zürich, Switzerland

Publicity Chair and Web Master

Corinna Schmitt University of Zürich, Switzerland

AIMS Steering Committee

Anna Sperotto University of Twente, The Netherlands
Pavel Čeleda Masaryk University, Czech Republic
Filip De Turck Ghent University - iMinds, Belgium
Rémi Badonnel LORIA, Inria, France
Aiko Pras University of Twente, The Netherlands
Burkhard Stiller University of Zürich, Switzerland
Robert Koch Universität der Bundeswehr München, Germany

Technical Program Committee

Alexander Clemm Huawei, USA
Alexander Keller IBM Global Technology Services, USA

Alva L. Couch	Tufts University, USA
Anandha Gopalan	Imperial College London, UK
Anna Sperotto	University of Twente, The Netherlands
Bertrand Mathieu	Orange Labs, France
Bruno Quoitin	Université de Mons, Belgium
Burkhard Stiller	University of Zürich, Switzerland
Daniele Sgandurra	Imperial College London, UK
David Hausheer	Otto-von-Guericke Universität Magdeburg, Germany
Filip De Turck	Ghent University - iMinds, Belgium
Gabi Dreo Rodosek	Universität der Bundeswehr München, Germany
Guillaume Doyen	Troyes University of Technology, France
Isabelle Chrisment	TELECOM Nancy, Université de Lorraine, France
Jan Kořenek	Brno University of Technology, Czech Republic
Jérôme François	Inria Nancy Grand Est, France
Joan Serrat	Universitat Politècnica de Catalunya, Spain
Jürgen Schönwälder	Jacobs University Bremen, Germany
Kurt Tutschku	Blekinge Institute of Technology, Sweden
Lisandro Zambenedetti Granville	UFRGS, Brazil
Mario Golling	Universität der Bundeswehr München, Germany
Martin Barrère	Imperial College London, UK
Mauro Tortonesi	University of Ferrara, Italy
Michelle Sibilla	Paul Sabatier University, France
Olivier Festor	INRIA Nancy Grand Est, France
Pavel Čeleda	Masaryk University, Czech Republic
Philippe Owezarski	LAAS-CNRS, France
Rashid Mijumbi	Waterford Institute of Technology, Ireland
Rémi Badonnel	Telecom Nancy, Université de Lorraine, France
Ricardo Schmidt	University of Twente, The Netherlands
Roberto Riggio	CREATE-NET, Italy
Steven Latré	University of Antwerp, iMinds, Belgium
Thomas Bocek	University of Zürich, Switzerland

Additional Reviewers

Detailed reviews for papers submitted to AIMS 2017 were undertaken by the Technical Program Committee as listed above and additionally by the following reviewers:

Messaoud Aouadj, Jeremias Blendin, Remi Cogranne, Ariel Dalla-Costa, Muriel Franco, Borislava Gajic, Christian Jacquenet, Christian Koch, Radek Krejci, Genaro Longoria, Christian Mannweiler, Hassnaa Moustafa, Tan Nguyen, Leonhard Nobach, Vinicius Schaurich, and Eder John Scheid.

Keynotes

Getting Rid of IoT Insecurity

Marcel Waldvogel

University of Konstanz, Distributed Systems Group, Universitätsstr. 10/229,
78457 Konstanz, Germany
`Marcel.Waldvogel@uni-konstanz.de`

Abstract. The Internet-of-Things (IoT) is already everywhere, but even then, there is still much more to come. Right now, IoT security is a mess, chaotic, unsustainable, and unmanageable. To prevent this is going to remain like this, and that these devices will continue to risk or endanger increasing amounts of our and everybody's lives, we need coordinated actions by manufacturers, vendors, integrators, ISPs, and customers.

But it is the researchers, you, who need to make a long-term difference: how to create blueprints, on which new products may be based, which may include design for privacy, security, manageability, while not overwhelming the users is probably the biggest challenge of them all.

This talk will present three examples, which clearly outlines the challenges, describes open problems, and proposes a coherent framework, into which your next solutions hopefully will fit.

Cyber Security Challenges – A Business Perspective

Matthias Bossardt

Lead Partner for Cyber Security, KPMG Switzerland, Zürich, Switzerland
mbossardt@kpmg.com

Abstract. This keynote will shed light on real world challenges that companies face when dealing with cyber threats on a global scale. In global organizations and where cyber security has to scale to hundred thousands of employees, contractors, suppliers, and clients as well as thousands of business processes and applications, understanding the organization's risk exposure and implementing effective protection measures is very complex.

And the plethora of challenges related to the (Industrial) Internet-of-Things and managing cyber security becomes a daunting task. To secure an organization, understanding human behavior and mastering organizational change is as important as implementing security technology. This talk will discuss those security capabilities needed in an organization and it will highlight those topics that can benefit greatly from additional research.

Lab Sessions

Hacking your Way to Safety – A Beginner’s Guide to Security Games

Martin Drašar

CSIRT-MU, Masaryk University, Brno, Czech Republic
drasar@ics.muni.cz

Abstract. Maintaining infrastructure security or hardening a system is never a simple task. Nor it is a one-click operation. Often it requires the adoption of attacker’s mindset to identify correctly weak spots or to even understand that a threat is imminent. This, however, is not possible without acquiring a large body of knowledge, which is usually dispersed around the Internet or available only as dry technical reports. While the process of assembling these bits of information may appeal to somebody, a majority will prefer something more entertaining. Security games are one such approach.

This lab is aimed at beginners and will serve as a brief introduction to hacking as a way to better understand computer security. It will discuss available learning resources and focus mostly on security games: why, which, where, and how to play them for maximum benefit? It will also give participants an opportunity to try out some of these games in a guided manner. These games will be executed both locally as virtual machines on attendees’ laptops and remotely in a virtual sandbox environment [1]. Attendees will also be asked to participate in a survey regarding skill self-assessment and effectiveness of knowledge transfer, which fosters further research as presented in [2].

References

1. Kourill, D., Rebok, T., Jirsik, T., Čegan, J., Drasar, M., Vizvary, M., Vykopal, J.: Cloud-based Testbed for Simulation of Cyber Attacks. In: IFIP/IEEE Network Operations and Management Symposium. NOMS 2014, Krakow, Poland, May 2016
2. Ykopal, J., Bartak, M.: On the Design of Security Games: From Frustrating to Engaging Learning, In: USENIX Workshop on Advances in Security Education. ASE 2016, Austin, Texas, USA, August 2016

Programming Smart Contracts

Thomas Bocek and Moritz Schneider

University of Zürich UZH, Department of Informatics IfI, Communication
Systems Group CSG, Binzmühlestrasse 14, 8050 Zürich, Switzerland
bocek@ifi.uzh.ch, moritz.schneider3@uzh.ch

Abstract. Blockchains and smart contracts have gained a lot of attention. Public blockchains are considered secure and exist without centralized control. As one of the most prominent blockchain examples, Bitcoin has the potential to disrupt financial services. However, the blockchain technology is applicable to a wider range of application domains, such as smart contracts, public registries, registry of deeds, or virtual organizations.

Another prominent blockchain example, Ethereum, which is considered a general approach for smart contracts, is the second biggest public blockchain with respect to market capitalization. A smart contract in Ethereum [1] is written in the language Solidity [2]. These contracts allow not only sending and receiving funds, but since Solidity is a Turing-complete language, it allows for the definition of any kind of rules.

The introduction of this lab session will address the history and an overview of blockchains as well as their categorization. Blockchain basics are explained in terms of basic building blocks and how they work, including the essential consensus mechanisms. Thus, the Solidity language is introduced in terms of syntax and main constructs, combined with simple code snippets and examples [3]. The audience will compile and deploy a simple smart contract with the goal to familiarize itself with the language and the development environment. Furthermore, the lab shows on the basis of Ethereum smart contracts how to create your own tokens or cryptocurrency [4]. The tokens or cryptocurrency initiator can create initial tokens that can be transferred to any address.

References

1. Homestead Release: ethereum. <https://www.ethereum.org/>. Accessed May 1, 2017
2. Solidity. <http://solidity.readthedocs.io>. Accessed May 1, 2017
3. Contract examples for Ethereum. <https://github.com/fivedogit/solidity-baby-steps>. Accessed May 1, 2017
4. Create your own crypto-currency with Ethereum. <https://www.ethereum.org/token>. Accessed May 1, 2017

Programming Data Planes in P4 – A High-level Language for Packet Processors

Salvatore Signorello¹ and Jérôme François²

¹ SnT, University of Luxembourg, Luxembourg, and LORIA,
University of Nancy, Nancy, France

² MADYNES Team at INRIA, Nancy Grand-Est, France
salvatore.signorello@uni.lu, jerome.francois@inria.fr

Abstract. This lab will introduce the audience to the P4 language [1], providing them with the knowledge necessary to develop and prototype their own research ideas in P4. The lab starts by providing an overview of the research that led to the emergence of the language and by illustrating the P4 language consortium objectives and related ongoing activities. Additionally, the lab explains the P4 language programming model and introduces an open source development environment [2], which can be used to write and test P4 programs on a single machine. The presented software toolset includes a P4 front-end compiler, a P4 software target, and the Command Line Interface (CLI) used to program this target at run-time. Finally, the lab interactively presents the language’s syntax and main constructs.

Throughout the entire lab, simple P4 code snippets and examples are written, compiled, and executed by the participants. Furthermore, full assignments of increasing complexity are proposed to strengthen the understanding of the programming model and of the main language constructs. More in detail, simple tasks, like the definition of a custom encapsulation protocol and the implementation of an access control list, help the audience to familiarize itself with the definition and the parsing of new protocols and with the definition of the control flow of a P4 program. While more complex assignments, like the implementation of a port-knock firewall, are meant to explore advanced language constructs, which can be used to implement stateful network functions.

References

1. Bosshart, P., Daly, D., Gibb, G., Izzard, M., McKeown, N., Rexford, J., Schlesinger, C., Talayco, D., Vahdat, A., Varghese, G., Walker, D.: P4: Programming Protocol-independent Packet Processors. *Comput. Commun. Rev.* **44**(3), 87–95
2. P4. <http://p4.org/join-us>

Contents

Security Management

Making Flow-Based Security Detection Parallel	3
<i>Marek Švepeš and Tomáš Čejka</i>	
A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts	16
<i>Bruno Rodrigues, Thomas Bocek, Andri Lareida, David Hausheer, Sina Rafati, and Burkhard Stiller</i>	
Achieving Reproducible Network Environments with INSALATA	30
<i>Nadine Herold, Matthias Wachs, Marko Dorfhuber, Christoph Rudolf, Stefan Liebold, and Georg Carle</i>	

Management of Cloud Environments and Services

Towards a Software-Defined Security Framework for Supporting Distributed Cloud	47
<i>Maxime Compastié, Rémi Badonnel, Olivier Festor, Ruan He, and Mohamed Kassi-Lahlou</i>	
Optimal Service Function Chain Composition in Network Functions Virtualization	62
<i>Andrés F. Ocampo, Juliver Gil-Herrera, Pedro H. Isolani, Miguel C. Neves, Juan F. Botero, Steven Latré, Lisandro Zambenedetti, Marinho P. Barcellos, and Luciano P. Gaspary</i>	

Evaluation and Experimental Study of Rich Network Services

An Optimized Resilient Advance Bandwidth Scheduling for Media Delivery Services	79
<i>Maryam Barshan, Hendrik Moens, Bruno Volckaert, and Filip De Turck</i>	
The Evaluation of the V2VUNet Concept to Improve Inter-vehicle Communications.	94
<i>Lisa Kristiana, Corinna Schmitt, and Burkhard Stiller</i>	
Towards Internet Scale Quality-of-Experience Measurement with Twitter. . . .	108
<i>Dennis Kergl, Robert Roedler, and Gabi Dreo Rodosek</i>	

Short Papers: Security, Intrusion Detection, and Configuration

Hunting SIP Authentication Attacks Efficiently.	125
<i>Tomáš Jansky, Tomáš Čejka, and Václav Bartoš</i>	
MoDeNA: Enhancing User Security for Devices in Wireless Personal and Local Area Networks.	131
<i>Robert Müller, Marcel Waldvogel, and Corinna Schmitt</i>	
Flow-Based Detection of IPv6-specific Network Layer Attacks.	137
<i>Luuk Hendriks, Petr Velan, Ricardo de O. Schmidt, Pieter-Tjerk de Boer, and Aiko Pras</i>	
Towards a Hybrid Cloud Platform Using Apache Mesos	143
<i>Noha Xue, Hårek Haugerud, and Anis Yazidi</i>	
Visual Analytics for Network Security and Critical Infrastructures.	149
<i>Karolína Burská and Radek Ošlejšek</i>	
Preserving Relations in Parallel Flow Data Processing	153
<i>Tomáš Čejka and Martin Žádník</i>	

Ph.D. Track: Autonomic and Self-Management Solutions

SmartDEMAP: A Smart Contract Deployment and Management Platform . . .	159
<i>Markus Knecht and Burkhard Stiller</i>	
Optimizing the Integration of Agent-Based Cloud Orchestrators and Higher-Level Workloads	165
<i>Merlijn Sebrechts, Gregory Van Seghbroeck, and Filip De Turck</i>	

Ph.D. Track: Methods for the Protection of Infrastructure and Services

Situational Awareness: Detecting Critical Dependencies and Devices in a Network	173
<i>Martin Laštovička and Pavel Čeleda</i>	
A Framework for SFC Integrity in NFV Environments	179
<i>Lucas Bondan, Tim Wauters, Bruno Volckaert, Filip De Turck, and Lisandro Zambenedetti Granville</i>	
Multi-domain DDoS Mitigation Based on Blockchains	185
<i>Bruno Rodrigues, Thomas Bocek, and Burkhard Stiller</i>	

Author Index	191
-------------------------------	-----