Lecture Notes in Computer Science 9701

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Rémi Badonnel · Robert Koch
Aiko Pras · Martin Drašar
Burkhard Stiller (Eds.)

Management and Security in the Age of Hyperconnectivity

10th IFIP WG 6.6 International Conference
on Autonomous Infrastructure, Management, and Security, AIMS 2016
Munich, Germany, June 20–23, 2016
Proceedings

Springer

Editors
Rémi Badonnel
LORIA - Inria
Vandoeuvre-lès-Nancy
France

Martin Drašar
Masaryk University
Brno
Czech Republic

Robert Koch
Universität der Bundeswehr
Neubiberg
Germany

Burkhard Stiller
University of Zürich
Zürich
Switzerland

Aiko Pras
University of Twente
Enschede
The Netherlands

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-39813-6 ISBN 978-3-319-39814-3 (eBook)
DOI 10.1007/978-3-319-39814-3

Library of Congress Control Number: 2016939999

LNCS Sublibrary: SL5 – Computer Communication Networks and Telecommunications

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Preface

The International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2016) is a single-track event integrating regular conference paper sessions, tutorials, keynotes, and a PhD student workshop into a highly interactive event. Within the network and service management community, AIMS is focused on PhD students and young researchers. One of the key goals of AIMS is to provide early-stage researchers with constructive feedback by senior scientists and give them the possibility to grow in the research community by means of targeted lab sessions on technical and educational aspects of their research activity. This focus on early-stage researchers is immediately observable in the program, featuring a high number of educational sessions and PhD sessions, where young PhD students present their research.

AIMS 2016 — which took place during June 20–23, 2016, in Neubiberg, Germany, and was hosted by the Universität der Bundeswehr München — was the tenth edition of a conference series on management and security aspects of distributed and autonomous systems. It followed the established tradition of an unusually vivid and interactive conference series, after successful events in 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 2016 focused on management and security in the age of hyperconnectivity. New paradigms, smart and fully distributed algorithms, and large-scale virtualization are investigated to design scalable and resilient frameworks able to deal with more complex, more dynamic and hyperconnected environments. This theme was addressed in the technical program with papers related to monitoring, configuration, and security in areas from cloud infrastructures to the Internet-of-Things. AIMS 2016 was organized as a 4-day program to encourage the interaction with and the active participation of the audience. The program consisted of technical sessions for the main track and PhD sessions, interleaved with research keynotes, an educational panel, and lab sessions.

The lab sessions offered hands-on experience in network and service management topics and they were organized in on-site labs preceded by short tutorial-style teaching sessions. The first lab session addressed big data analysis for the Domain Name System (DNS), explaining how tracking DNS changes based on measurements may provide valuable information about the evolution of the Internet. The other lab sessions were centered on traffic mining for flow-based forensic and network troubleshooting, using Tranalyzer, a lightweight flow generator and packet analyzer designed for practitioners and researchers. In line with its educational mission, this year the conference also included an educational panel, which was chaired by Daphné Tuncer and Marinos Charalambides (University College London, UK) on “Experiences with MOOCs and Flipped Classrooms.” Additionally, AIMS 2016 featured two research keynotes: one on “Today’s Cyber Security Threats and Challenges for Telco Providers” by Bernd

Eßer (Telekom CDC, Germany) and one on "Cyber Resilience of Complex Interdependent Infrastructures" by Tobias Kiesling (IABG, Germany).

The technical program consisted of two sessions — covering the topics of autonomic and smart management, and security attacks and defenses — and included seven full papers, which were selected after a thorough reviewing process out of a total of 22 submissions. Each paper received at least three independent reviews. Three papers were also selected for presentation as short papers.

The AIMS PhD workshop is a venue for doctoral students to present and discuss their research ideas, and more importantly to obtain valuable feedback from the AIMS audience about their planned PhD research work. This year, the workshop was structured into two technical sessions covering the management of future networks and security management. All PhD papers included in this volume describe the current state of these investigations, including their clear research problem statements, proposed approaches, and an outline of results achieved so far. A total of nine PhD papers were presented and discussed. These papers were selected after a separate review process out of 21 submissions, while all PhD papers received at least three independent reviews.

The present volume of the *Lecture Notes in Computer Science* series includes all papers presented at AIMS 2016 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. Also, AIMS 2016 proved true to its defined DNA of a conference with a strong educational goal, as indicated by the number of submissions attracted by the PhD Workshop.

The editors would like to thank the many people who helped to make AIMS 2016 such a high-quality and successful event. Firstly, many thanks are extended to all authors who submitted their contributions to AIMS 2016, and to the lab session speakers, namely, Anna Sperotto, Mattijs Jonker, Christian Dietz, Stefan Burschka, and Benoît Dupasquier, and the keynote speakers Bernd Eßer and Tobias Kiesling. The great review work performed by the members of both the AIMS Technical Program Committee and the PhD Student Workshop Committee as well as additional reviewers is highly acknowledged. Thanks are also addressed to Volker Eiseler and Lars Stiemert for setting up and organizing the lab sessions. Additionally, many thanks to the local organizers for handling all the logistics and hosting the AIMS 2016 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 2016 supporters, Universität der Bundeswehr München, ITIS, and the European FP7 NoE FLAMINGO under Grant No. 318488.

April 2016

Rémi Badonnel
Robert Koch
Martin Drašar
Aiko Pras

Organization

General Chair AIMS 2016

Gabi Dreo Rodosek	Universität der Bundeswehr München, Germany

Technical Program Committee Co-chairs

Rémi Badonnel	LORIA - Inria, France
Robert Koch	Universität der Bundeswehr München, Germany

PhD Student Workshop Co-chairs

Martin Drašar	Masaryk University, Czech Republic
Aiko Pras	University of Twente, The Netherlands

Labs Co-chairs

Volker Eiseler	Universität der Bundeswehr München, Germany
Lars Stiemert	Universität der Bundeswehr München, Germany

Publications Chair

Burkhard Stiller	University of Zürich, Switzerland

Local Chair

Volker Eiseler	Universität der Bundeswehr München, Germany

AIMS Steering Committee

Guillaume Doyen	Troyes University of Technology, France
Anna Sperotto	University of Twente, The Netherlands
Pavel Čeleda	Masaryk University, Czech Republic
Filip De Turck	Ghent University - iMinds, Belgium
Aiko Pras	University of Twente, The Netherlands
Burkhard Stiller	University of Zürich, Switzerland

Technical Program Committee

Alexander Clemm	Cisco Systems, 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
Bruno Quoitin	Université de Mons, Belgium
Burkhard Stiller	University of Zürich, Switzerland
Clarissa Marquezan	Huawei Technologies, Germany
Daniele Sgandurra	Imperial College London, UK
Daphné Tuncer	University College of London, UK
David Hausheer	Technical University Darmstadt, Germany
Filip De Turck	Ghent University - iMinds, Belgium
Guillaume Doyen	Troyes University of Technology, France
Henning Sanneck	Nokia Networks, Germany
Isabelle Chrisment	TELECOM Nancy, Université de Lorraine, France
Jan Kořenek	Brno University of Technology, Czech Republic
Jérôme François	Inria Nancy Grand Est, France
Jürgen Schönwälder	Jacobs University Bremen, Germany
Kurt Tutschku	Blekinge Institute of Technology, Sweden
Lisandro Zambenedetti Granville	UFRGS, Brazil
Marinos Charalambides	University College London, UK
Martin Barrère	Imperial College London, UK
Martin Drašar	Masaryk University, Czech Republic
Martin Žádník	Brno University of Technology, Czech Republic
Mauro Tortonesi	University of Ferrara, Italy
Michael Menth	University of Tübingen, Germany
Michele Nogueira	Universidade Federal do Parana, Brazil
Michelle Sibilla	Paul Sabatier University, France
Paulo Simoes	University of Coimbra, Portugal
Philippe Owezarski	LAAS-CNRS, France
Piotr Chołda	AGH University of Science and Technology, Poland
Ramin Sadre	Université Catholique de Louvain, Belgium
Rashid Mijumbi	Waterford Institute of Technology, Ireland
Ricardo Schmidt	University of Twente, The Netherlands
Roberto Riggio	CREATE-NET, Italy
Shingo Ata	Osaka City University, Japan
Steven Latré	University of Antwerp - iMinds, Belgium
Thomas Bocek	University of Zürich, Switzerland
Thomas Schaaf	University of Munich (LMU), Germany

PhD Student Workshop Committee

Pavel Čeleda	Masaryk University, Czech Republic
Idilio Drago	Politecnico di Torino, Italy
Gabi Dreo Rodosek	Universität der Bundeswehr München, Germany
Gunnar Karlsson	KTH, Sweden
Abdelkader Lahmadi	University of Lorraine, France

Guy Leduc	University of Liege, Belgium
Emil Lupu	Imperial College London, UK
Edmundo Monteiro	University of Coimbra, Portugal
Corinna Schmitt	University of Zürich, Switzerland
Burkhard Stiller	University of Zürich, Switzerland
Sofie Verbrugge	Ghent University - IMEC - IBBT, Belgium
Jan Vykopal	Masaryk University, Czech Republic

Additional Reviewers

Detailed reviews for papers submitted to AIMS 2016 were performed by the Technical Program Committee as well as the PhD Student Workshop Committee as stated and additionally by the following reviewers:

Filipe Caldeira, Florian Heimgärtner, Michael Höfling, Christian Koch, Muhammad Naseer-ul-Islam, Leonhard Nobach, Luis Rosa

Keynotes and Panel

Keynote 1
Today's Cyber Security Threats and Challenges for Telco Providers

Bernd Eßer

Telekom Cyber Defense Center (CDC), Deutsche Telekom, Bonn, Germany
EsserB@telekom.de

Abstract. This keynote focuses on the threat landscape and its evolution as seen from a Tier-1 operator's perspective. This includes the development of threats that affect mainly consumers, such as botnets, as well as threats that address primarily organizations.

So called Advanced Persistent Threats (APT) are analyzed in the way offenders usually pursue such attacks. Strategic and operational options to detect and remediate such attacks are discussed. This keynote closes with thoughts on possible future roles of telcos in this threat context.

Keynote 2
Cyber Resilience of Complex Interdependent Infrastructures

Tobias Kiesling

Industrieanlagen Betriebsgesellschaft mbH, IABG, Ottobrunn, Germany
kiesling@iabg.de

Abstract. Most of the critical infrastructures that we utilize in our daily life are quite complex and interdependent on one another. This poses a huge challenge to our understanding with respect to major risks connected to those infrastructures. This is especially true when considering the imminent threat of potential cyber attacks that are generally seen as possible already in our current time.

What we need is a more thorough understanding of cyber-related risks that can guide the implementation of measures to secure the resilience of critical infrastructures. One example for a vulnerable infrastructure is the air traffic system at large, which is an attractive target for cyber attacks due to its importance and prominence. The current system is already vulnerable and the advent of more automation and pervasion of standard IT in the wake of future approaches leads to ever more complex and interconnected systems with an increasing attack surface.

To cope with this situation, we need to follow a resilience-oriented view and utilize suitable methods and tools to achieve understanding of the consequences in potential cyber threat situations. This keynote introduces the notion of cyber operational resilience and shows how this can be applied to the air transport infrastructure as an example of other complex interdependent systems.

Educational Panel Experiences with MOOCs and Flipped Classrooms

Daphné Tuncer, Marinos Charalambides

University College London, UK
d.tuncer@ee.ucl.ac.uk, marinos.charalambides@ucl.ac.uk

Abstract. Massive Open Online Courses (MOOC) are open access and scalable online higher education courses. MOOCs have been gaining increasing popularity in recent years mainly due to their extended outreach and lack of entry requirements as well as tuition fees. Given their initial success and the interest from the higher education community, they have the potential of becoming an essential part of the education system.

However, due to their online nature they do not follow the traditional teaching paradigm that requires classroom presence and involves direct interaction with the lecturer. In addition, MOOCs can be developed through various platforms and can have different formats. These factors can influence the student learning experience and the future uptake of such courses.

This panel will mainly consist of PhD researchers, that have followed at least one MOOC, who will discuss their personal experience and expectations, and share their insights with the audience. The panel will be structured in three parts. First, the panelists will present their views based on a short questionnaire that will be provided prior to the event. Second, the moderators will ask questions concerning, course integration, interaction with other students/instructor, MOOC format, course customization, and grading systems. Finally, an open discussion with the audience will conclude the panel. The overall objective is to collect valuable feedback of the panelists and potentially the audience, which can be used to suggest changes in current practices and make learning more effective.

Lab Sessions

Lab Session 1
The Internet of Names: Big Data Analysis for DNS

Anna Sperotto[1], Mattijs Jonker[1], Christian Dietz[2]

[1]University of Twente, The Netherlands
[2]Universität der Bundeswehr München, Germany
a.sperotto@utwente.nl, m.jonker@utwente.nl, christian.dietz@unibw.de

Abstract. The Domain Name System (DNS) is part of the core infrastructure of the Internet. Tracking changes in the DNS, therefore, provide valuable information about the evolution of the Internet. Think about adoption of protocols (e.g., IPv6 and DNSSEC) and applications (e.g., cloud e-mail providers), distribution of content (Web domains), and network security (e.g., botnets).
Since February 2015, the University of Twente, SURFnet, and SIDN run a largescale active measurement of the DNS, which cover the domain names in the .com, .net, and .org zones. Since February 2016, the .nl zone has also been added. In total, our measurement currently queries over 50 % of the DNS name space on a daily basis. The measurement results are stored in an Hadoop cluster for later analysis [1].

The goal of this hands-on tutorial is to familiarize the participants with DNS, DNS measurements, and possible research application. The session will start with a general introduction to the measurement including a few example use cases. Then, we will briefly introduce the participants to a virtualized lab environment, in which they can experiment with the data themselves. The remainder of the session is then spent "hackathon"-style, in groups, each of which will present their experiences and possible findings from the data at the end of the session in a short presentation. The lab environment will contain real data for the Alexa Top 1 Million domains.

Reference

1. van Rijswijk-Deij, R., Jonker, M., Sperotto, A., Pras, A.: The internet of names: a DNS big dataset. In: SIGCOMM 2015 Poster Paper, ACM, London, UK, August 17–21 (2015)

Lab Sessions 2 and 3
Traffic Mining (TM) using Brain and Tranalyzer

Stefan Burschka, Benoît Dupasquier

RUAG, Switzerland
stefan.burschka@ruag.com, benoit.dupasquier@ruag.com

Abstract. Tranalyzer is a lightweight flow generator and packet analyzer designed for practitioners and researchers [1]. Special value is set to simplicity, performance, and scalability. It extends netflow functionality and supports the analysis in processing ultra large packet dumps. It supports the drill down process to the very flow of interest, which can be analyzed in depth by tcpdump or wireshark. It provides support for assessing and generating key parameters and statistics from IP traces either being live-captured from ethernet interfaces or pcap files, in the context of flow forensics and network troubleshooting.
These lab sessions are literally defined by the title, Traffic Mining (TM) using your brain and Tranalyzer. Participants will do a hands-on job of analysists trying to find anomalies in real IP traffic.

After a short introduction to the most important IP protocols and header features, they will get familiar with Tranalyzer's main concepts, such as configuration and compilation operations, most important plugins including configuration constants, flows and global reports, and how to write their own plugins in C. They will experiment it in groups or alone on several pcaps traffic captures through different practical exercises. They might get stuck in a foxhole and have to learn how to dig themselves out. Nothing is like it initially seems, or maybe it is. It is addressed to everybody who is willing to learn further about IP traffic and the way of flow based traffic mining.

Reference

1. Opensource Version of Tranalyzer2-0.5.8 http://sourceforge.net/projects/tranalyzer/

Contents