Lecture Notes in Computer Science 8508

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

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, 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, Saarbruecken, Germany

Anna Sperotto Guillaume Doyen
Steven Latré Marinos Charalambides
Burkhard Stiller (Eds.)

Monitoring and Securing Virtualized Networks and Services

8th IFIP WG 6.6 International Conference
on Autonomous Infrastructure,
Management, and Security, AIMS 2014
Brno, Czech Republic, June 30 – July 3, 2014
Proceedings

Springer

Volume Editors

Anna Sperotto
University of Twente, Enschede, The Netherlands
E-mail: a.sperotto@utwente.nl

Guillaume Doyen
Troyes University of Technology, Troyes Cedex, France
E-mail: guillaume.doyen@utt.fr

Steven Latré
University of Antwerp, Belgium
E-mail: steven.latre@uantwerpen.be

Marinos Charalambides
University College London, UK
E-mail: marinos.charalambides@ucl.ac.uk

Burkhard Stiller
University of Zurich, Switzerland
E-mail: stiller@ifi.uzh.ch

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-662-43861-9 e-ISBN 978-3-662-43862-6
DOI 10.1007/978-3-662-43862-6
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014941086

LNCS Sublibrary: SL 5 – Computer Communication Networks
and Telecommunications

© International Federation for Information Processing 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in ist current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
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.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2014) is a single-track event integrating regular conference paper sessions, a keynote, lab sessions, and the PhD Student Workshop into a highly interactive event. This year AIMS has re-defined its "DNA" and was even more 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 of growing in the research community by means of targeted lab sessions on technical and educational aspects of the research activity.

AIMS 2014, which took place from June 30 to July 3, 2014, in Brno, Czech Republic, was hosted by the Masaryk University as the eighth 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 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.

This year, AIMS 2014 focused on monitoring and securing virtualized networks and services. This theme is addressed in the technical program with papers related to monitoring, security, and management methodologies in the application areas of wired and wireless networks, Internet-of-Things, and Cloud infrastructures. AIMS 2014 was organized as a 4-day program structured to encourage the interaction with and the active participation of the conference's audience. The program consisted of technical sessions for the main track and PhD sessions, interleaved with a keynote, an "Education Session Talk," and three lab sessions. The AIMS 2014 keynote presentation was given by Martin Rehak, Cisco Systems, on "Security Analytics: Finding a Needle in the Hay Blower". These lab sessions offered hands-on experience in network and service management topics and they were organized in practical exercises preceded by short tutorial-style teaching session. The first lab session presented the "Fast Network Simulation Set-up" tool chain, aiming at facilitating the set-up of complex scenarios for network simulations. The second lab session covered the topic of network management using software-defined networking. Finally, the third lab session focused on security and the session introduced the "Cybernetic Proving Ground", a testbed for Cloud-based security research. Finally, and in line with its educational mission, this year the conference also included an "Education Session Talk", which was given by Aiko Pras on the topic of scientific publications and with the goal of providing guidelines for PhD students and young researchers on publication venues and the advantages and drawbacks of related metrics to which each researcher is nowadays subject to.

The technical program consisted of three sessions — covering the topics of emerging infrastructures for networks and services, experimental studies for security management, and monitoring methods for Quality-of-Service and security — and included nine full papers, which were selected after a thorough reviewing process out of 29 submissions. Each paper received three or four independent reviews, followed by a shepherding process aimed at tutoring those nine accepted papers through the preparation of the camera-ready paper version and to the paper presentation.

The AIMS PhD Student Workshop provides 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 four technical sessions covering security, management of virtualized network resources and functions, software-defined networking, and monitoring. 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 13 PhD papers were presented and discussed. These papers were selected after a separate review process out of 27 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 2014 as defined within the overall final program. It demonstrates again the European scope of this conference series, since most of those papers accepted originate from European research groups. AIMS 2014 proved to be a conference with a strong educational goal, as indicated by the good number of submissions and the attractiveness of the PhD Student Workshop.

The editors would like to thank the many people who helped make AIMS 2014 such a high-quality and successful event. Firstly, many thanks are addressed to all authors, who submitted their contributions to AIMS 2014, and to the lab session speakers, namely, Lorenzo Saino, Niels Bouten, Maxim Claeys, Jeroen Famaey, Jakub Čegan, Martin Vizváry, and Michal Procházka, and the keynote and educational session speakers Martin Rehak and Aiko Pras. The great review work performed by the members of both the AIMS TPC and the PhD Student Workshop Committee as well as additional reviewers is highly acknowledged. Thanks go also to Petr Velan and Jeroen Famaey for setting up and organizing these lab sessions and the test-bed hardware. Additionally, many thanks are addressed to the local organizers at Masaryk University for providing all logistics and hosting the AIMS 2014 event.

Finally, the editors would like express their thanks to Springer and in particular to Anna Kramer for the smooth cooperation in finalizing these proceedings. Additionally, special thanks go to the AIMS 2014 supporter, the European FP7 NoE FLAMINGO under Grant No. 318488.

April 2014

Anna Sperotto
Guillaume Doyen
Steven Latré
Marinos Charalambides

Masaryk University

NoE FLAMINGO

Organization

General Chair AIMS 2014

Pavel Čeleda	Masaryk University, Czech Republic

Technical Program Committee Co-chairs

Guillaume Doyen	Troyes University of Technology, France
Anna Sperotto	University of Twente, The Netherlands

PhD Student Workshop Co-chairs

Steven Latré	Universiteit Antwerp, iMinds, Belgium
Marinos Charalambides	University College London, UK

Labs Co-chairs

Petr Velan	Masaryk University, Czech Republic
Jeroen Famaey	Ghent University, iMinds, Belgium

Publications Chair

Burkhard Stiller	University of Zürich, Switzerland

Local Co-chairs

Iva Krejčí	Masaryk University, Czech Republic
Jan Vykopal	Masaryk University, Czech Republic

AIMS Steering Committee

Burkhard Stiller	University of Zürich, Switzerland
Olivier Festor	Telecom Nancy, University of Lorraine, France
Ramin Sadre	Aalborg University, Denmark
Guillaume Doyen	Troyes University of Technology, France
David Hausheer	Technical University Darmstadt, Germany
Aiko Pras	University of Twente, The Netherlands

Technical Program Committee

Alessandro Finamore	Politecnico di Torino, Italy
Alex Galis	University College London, UK
Alexander Clemm	Cisco Systems, USA
Alexander Keller	IBM Global Technology Services, USA
Alva L. Couch	Tufts University, USA
Anandha Gopalan	Imperial College London, UK
Bertrand Mathieu	Orange Labs, France
Bruno Quoitin	Université de Mons, Belgium
Burkhard Stiller	University of Zürich, Switzerland
Danny Raz	Technion, Israel
David Hausheer	Technical University Darmstadt, Germany
Filip De Turck	Ghent University, iMinds, Belgium
Gabi Dreo Rodosek	University of Federal Armed Forces, Munich, Germany
Georgios Karagiannis	University of Twente, The Netherlands
Grégory Bonnet	University of Caen Lower Normandy, France
Isabelle Chrisment	TELECOM Nancy, Université de Lorraine, France
Jan Kořenek	Brno University of Technology, Czech Republic
Jérôme François	INRIA Grand Est Nancy, France
Jürgen Schönwälder	Jacobs University Bremen, Germany
Kurt Tutschku	Blekinge Institute of Technology, Sweden
Lisandro Zambenedetti Granville	UFRGS, Brazil
Martin Waldburger	WIK-Consult, Germany
Martin Žádník	Brno University of Technology, Czech Republic
Mauro Tortonesi	University of Ferrara, Italy
Michelle Sibilla	Paul Sabatier University, France
Olivier Festor	Telecom Nancy, University of Lorraine, France
Philippe Owezarski	LAAS-CNRS, France
Piotr Cholda	AGH University of Science and Technology, Poland
Radu State	University of Luxembourg, Luxembourg
Ramin Sadre	Aalborg University, Denmark
Raouf Boutaba	University of Waterloo, Canada
Remi Badonnel	INRIA, TELECOM Nancy, Université de Lorraine, France
Róbert Szabó	Budapest University of Technology and Economics, Hungary
Thomas Bocek	University of Zürich, Switzerland
Vojtěch Krmíček	Masaryk University, Czech Republic

PhD Student Workshop Committee

Aiko Pras	University of Twente, The Netherlands
Alberto Schaeffer-Filho	UFRGS, Brazil
Arosha Bandara	The Open University, UK
Bradley Simmons	York University, Canada
Carol Fung	Virginia Commonwealth University, USA
Clarissa Marquezan	Duisburg-Essen University, Germany
Daphne Tuncer	University College London, UK
Desislava Dimitrova	University of Bern, Switzerland
Dimitrios Pezaros	University of Glasgow, UK
George Pavlou	University College London, UK
Giovane Moura	Delft University of Technology, The Netherlands
Javier Rubio-Loyola	CINVESTAV, Mexico
Jeroen Famaey	Ghent University, iMinds, Belgium
Joan Serrat	Universitat Politecnica de Catalunya, Spain
Kostas Tsagkaris	University of Piraeus, Greece
Lefteris Mamatas	University College London, UK
Luciano Paschoal Gaspary	UFRGS, Brazil
Maxwell Young	Drexel University, USA
Ning Wang	University of Surrey, UK
Paulo Simoes	University of Coimbra, Portugal
Steven Davy	Waterford Institute of Technology, Ireland
Stylianos Georgoulas	University of Surrey, UK
Sven van der Meer	Ericsson, Ireland

Reviewers

Detailed reviews for papers submitted to AIMS 2014 were carried out by the Technical Program Committee as well as the PhD Student Workshop Committee as stated above and additionally by the following reviewers:

Abdelkader Lahmadi
Christian Koch
Corinna Schmitt
Gaëtan Hurel
Hammi Badis
Juan Pablo Timpanaro
Leonhard Nobach
Lisa Kristiana
Matthias Wichtlhuber
Natalie Matta
Nikolay Melnikov
Patrick Truong
Piotr Wydrych
Reaz Ahmed
Rida Khatoun
Vaibhav Bajpai

Keynote — Modern Security Analytics: Finding a Needle in the Hay Blower

Martin Rehak

Cisco Systems
Prague, Czech Republic
marrehak@cisco.com

Abstract. Detection of advanced security threats is one of the exciting problems of current computer science. The field, which has been traditionally considered an art, rather than science, has been undergoing major transformation due to the rapid evolution of attacks staged by government actors and organized crime, rather than by hobbyists and enthusiasts from the past. In order to keep the pace with these attackers, a mix of approaches from machine learning, "big data analytics", game theory and distributed computing is necessary to deliver a robust, scalable, and affordable solution to this problem.

This keynote will concentrate on the stream analytics, *i.e.,* the application of highly efficient machine learning methods to data in flight, prior to their serialization and more in-depth analytics steps. We will follow one case of malware detection on its path through the system, and we will also show that a bit of an art is still necessary to make science work in a highly adversarial environment.

Educational Session — Where to Publish?

Aiko Pras

University of Twente, The Netherlands
a.pras@utwente.nl

Abstract. In this educational session talk we stress the importance of publishing your research results at the right venues. First, we identify the workshops, conferences, magazines, and journals in the area of network and systems management, but also in the broader networking area. We will discuss the quality of some of our conferences and journals, as perceived by experts in our field, as well as people outside our area. In addition, we present acceptance rates, acceptance procedures, conference and journal rankings, as well as impact factors. Although some Ph.D. students may believe that a main goal is to publish as many papers as possible, this talk will stress that there are other important metrics, such as some key venues and the number of citations. We will discuss the pros and cons of the H-index, a metric that is currently quite popular for judging quality of people as well as conferences, but has several limitations. The talk concludes with explaining the importance of publishing in journals indexed in Thomson's Science Citation Index (SCI), or alternatives like Scopus. It also explains CPP, JCS, and FCS factors.

Lab Session 1 — Fast Network Simulation Setup

Lorenzo Saino

University College London, United Kingdom
l.saino@ee.ucl.ac.uk

Abstract. Arguably, one of the most cumbersome tasks required to run a network experiment is the setup of a complete scenario and its implementation in the target simulator or emulator. This process includes selecting an appropriate topology, provision nodes and links with all required parameters and, finally, configure traffic sources or generate traffic matrices.

Executing all these task manually is both time-consuming and error-prone. The Fast Network Simulation Setup (FNSS) tool chain addresses this problem by allowing users to generate even complex experiment scenarios with few lines of Python code and deploy them in the preferred target simulator. FNSS currently supports ns-2, ns-3, mininet as well as custom-built C++, Java, and Python simulators. The lab is divided in three parts.

In the first part, participants will be familiarized with various models and data sets of networks topologies. They will also learn the most commonly used models to assign link capacities, delays and buffer sizes and how to synthetically generate realistic traffic matrices. The second part will provide an overview of the FNSS tool chain. Participants will learn how to install and configure it and they will be walked through its main features. Finally, in the third part, participants will learn through live coding examples how to easily generate complex simulation scenarios and how to deploy them on a number of different simulators or emulators.

Lab Session 2 — Deploying OpenFlow Experiments on the Virtual Wall Test-bed

Niels Bouten, Maxim Claeys, and Jeroen Famaey

Ghent University, iMinds, Belgium
{niels.bouten|maxim.claeys|jeroen.famaey}@intec.ugent.be

Abstract. Software-defined networking (SDN) greatly increases network management flexibility by decoupling decision making (i.e., control plane) from traffic forwarding (*i.e.*, data plane) in network equipment. This enables network control to become directly programmable, and allows intelligent software components to dynamically reconfigure the network based on service requirements and network conditions. OpenFlow is without a doubt the most widely known implementation of the SDN concept. It is a protocol which structures the communication between the network's data and control plane and provides granular traffic control.

The goal of this hands-on lab session is to familiarize the participant with the concept of SDN in general and with OpenFlow in particular. We will explore OpenFlow's capabilities to dynamically reroute traffic, guarantee bandwidth, and differentiate flows. Participants will be given the opportunity to apply their acquired knowledge by setting up an OpenFlow-based experiment that guarantees the Quality-of-Service requirements of a networked video application. The experiment will be run in a live network setting, facilitated by the Virtual Wall test-bed.

The Virtual Wall is a test-bed facility for setting up large-scale network topologies. The Virtual Wall nodes can be assigned different functionalities and organized in arbitrary network topologies on the fly. As such, it is a generic experimental environment for advanced network, distributed software and service evaluation, and supports scalability research. The facility has been made available to the research community through different FP7 FIRE projects. The lab session will provide a brief theoretical introduction about the Virtual Wall's capabilities in preparation of the hands-on part.

Lab Session 3 — Cybernetic Proving Ground: A Cloud-Based Security Research Test-bed

Jakub Čegan, Martin Vizváry, and Michal Procházka

Masaryk University, Czech Republic
{cegan|vizvary|prochazkam}@ics.muni.cz

Abstract. Cyber attacks have become ubiquitous and in order to face current threats it is important to understand them. However, studying these attacks in a real environment is not often viable. Therefore, it is necessary to find other methods of examining the nature of the attacks. This lab session will present Cybernetic Proving Ground (CPG) that is being developed at Masaryk University. The CPG is a cloud-based framework that allows users to instantiate and run miscellaneous security and forensic scenarios.

The CPG provides a generic way to simulate and study a wide range of cyber attacks. It facilitates an establishment of isolated virtual environments that researchers can use to pursue controlled analysis of the attacks. Using virtualization and clouds, we managed to provide an environment, where it is possible to configure any common network configuration. Therefore, we are able to fulfill needs of many types of security scenarios. The user can use the CPG to set up isolated environments very quickly without the necessity of knowing details about network configuration or deploying auxiliary services such as a monitoring infrastructure.

The lab session is divided in three parts. In the first part of the lab session, participants will learn how to access the CPG infrastructure and how to configure a scenario. The second part of the lab session will focus on running a security scenario. The participants will take part in the scenario as each of them will have a machine to control. An overall status of the CPG scenario will be monitored in the course of the simulation. We will show how to use CPG to easily generate network scenarios, deploy them to simulate and evaluate experiments in a large cloud-based environment.

Table of Contents

Emerging Infrastructures for Networks and Services

Ph.D. Student Workshop — Management of Virtualized Network Resources and Functions

Ph.D. Student Workshop — Security Management

Experimental Studies for Security Management

Ph.D. Student Workshop — SDN and Content Delivery

Monitoring Methods for Quality-of-Service and Security

Ph.D. Student Workshop — Monitoring and Information Sharing