Report on the 8th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2014) : monitoring and securing virtualized networks and services

Journal of Network and Service Management manuscript No.
(will be inserted by the editor)

Report on the 8th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2014)

Monitoring and Securing Virtualized Networks and Services

Anna Sperotto · Guillaume Doyen · Steven Latré · Marinos Charalambides · Jeroen Famaey · Petr Velan · Pavel Čeleda

Received: date / Accepted: date

Neither the entire paper nor any part of its content has been published or has been accepted for publication elsewhere. It has not been submitted to any other journal.

Abstract This article is a report of the IFIP AIMS 2014, which was held at Masaryk University, Czech Republic from June 30 to July 3, 2014. AIMS 2014 focused on the theme "Monitoring and Securing Virtualized Networks and Services". AIMS 2014 has been characterized by a re-designed DNA, which positions the conference as an educational venue for PhD students and your researchers. AIMS program included hands-on tutorials and labs, a keynote, technical sessions

A. Sperotto
University of Twente
Faculty for Electrical Engineering, Mathematics, and Computer Science
P.O. Box 217, 7500 AE Enschede, The Netherlands
E-mail: a.sperotto@utwente.nl

G. Doyen
Troyes University of Technology
Charles Delaunay Institute (ICD)
12 Rue Marie Curie, CS 42060, 10004 TROYES CEDEX, France
E-mail: guillaume.doyen@utt.fr

S. Latré, J. Famaey
University of Antwerp - iMinds
Department of Mathematics and Computer Science
Middelheimlaan 1
2020 Antwerpen
E-mail: {steven.latre|jeroen.famaey}@uantwerpen.be

M. Charalambides
University College London
Department of Electronic and Electrical Engineering
Torrington Place, London WC1E 7JE, United Kingdom
E-mail: marinos.charalambides@ucl.ac.uk

P. Čeleda, P. Velan
Masaryk University, Institute of Computer Science
Botanická 68a, 602 00 Brno, Czech Republic
E-mail: {celeda|velan}@ics.muni.cz

and PhD Workshop sessions, but also an educational session for training young academics on tranversal topics. The highlights on each of the parts of AIMS 2014 program are summarized in this article.

Keywords Network management · Service management · Autonomous infrastructure · Security

1 Introduction

The 8th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2014) was held at Masaryk University, Czech Republic from June 30 to July 3, 2014 [1]. The four-day AIMS 2014 conference was a single-track event integrating technical paper sessions, a poster session, tutorials, keynotes, and a PhD student workshop into a highly interactive event. This year, AIMS 2014 focused on monitoring and securing virtualized networks and services. This theme was addressed in the technical program with papers related to monitoring, security, and management methodologies in the application areas of wired and wireless networks, cloud infrastructures and next-generation services. AIMS 2014 was co-sponsored by the IFIP WG 6.6 [5] and European FP7 NoE "FLAMINGO" (No. 318488) [4].

2 Hands-on Lab Sessions

The AIMS 2014 program contained three hands-on lab sessions on timely topics in the area of network and service management, presented on Tuesday, Wednesday and Thursday morning. The labs have been advertised as a structural part of the conference program and they offered a balanced mix of theoretical background information and practical exercises over a four-hour period. Between 15 and 30 participants attended every lab.

2.1 Fast Network Simulation Setup

The first lab session was delivered by Lorenzo Saino (University College London) and familiarized participants with the Fast Network Simulation Setup (FNSS) toolchain [12]. The FNSS toolchain allows users to generate complex network experiment scenarios using a simple Python-based API.

The lab session consisted of three parts, two theoretical and one practical. First, the presenter introduced participants to the concept of network experiment scenarios. The different components of a network model (i.e., the topology, link characteristics and node configuration) were described in detail. The presenter discussed the structure of network topologies commonly used in network simulation, such as AS-level, intra-domain and datacenter topologies, as well as the most prevalent synthetic models. The first part of the tutorial was concluded with an explanation of traffic matrices, which define the traffic flows in the network. Moreover, an algorithm to generate realistic synthetic traffic matrices was described in detail.

Second, the presenter introduced participants to the FNSS toolchain. A simple Python API that allows the user to quickly generate network models as described in the first part. FNSS greatly simplifies and speeds up this process as it comes with a wide range of models for automatically generating synthetic network topologies, link characteristics and traffic matrices, as well as the ability to generate them based on input datasets. The second part was concluded with an explanation of how to export the generated network models to a range of output formats (e.g., ns-2, ns-3 and mininet).

The third and final part of the lab session allowed participants to experiment with the FNSS toolchain themselves through a set of practical exercises. They were allowed to generate several different network models, and export them to multiple output formats. Finally, an exported network model was deployed using the mininet network emulator and executed as an experiment.

2.2 Deploying OpenFlow Experiments on the Virtual Wall

The second lab session was presented by Niels Bouten, Maxim Claeys and Jeroen Famaey (Ghent University). It dealt with deploying and running OpenFlow-based experiments on the Virtual Wall testbed infrastructure. OpenFlow is a standardized protocol that supports the separation of the control and data plane of a switch. It allows a software-based controller to communicate with OpenFlow-enabled switches and influence their packet forwarding behavior. The Virtual Wall is a network emulation testbed, based on the University of Utah's Emulab [2]. The Virtual Wall consists of 300 nodes, connected through several non-blocking Ethernet switches. Using a graphical interface, experimenters can define generic network topologies, link characteristics (e.g., bandwidth, delay, packet loss), and node configurations (e.g., IP address, operating system, software), which are then automatically deployed on the testbed infrastructure. As such, network scenarios can be quickly configured using real hardware, without a need for manual configuration.

The lab session itself consisted of two main parts, each comprising a theoretical and hands-on component. First, participants were familiarized with the Virtual Wall testbed itself, as well as the Fed4FIRE project [3]. Fed4FIRE is a European FP7 project that federates many European testbed facilities, including the Virtual Wall. Within the project, the jFed tool was developed, which is a graphical interface for defining experiment scenarios on the Virtual Wall as well as other testbeds, and even spanning across them. At the end of the first part, participants were allowed to experiment with jFed and deploy a small two-node experiment, connected by a single link. Participants were asked to configure and measure the bandwidth and latency on this link.

The second part of the lab session focused on OpenFlow. Participants were given a theoretical overview of the OpenFlow protocol and its capabilities. Additionally, an overview of existing OpenFlow software was provided. Finally, the tutorial was concluded with a hands-on OpenFlow session on the Virtual Wall. Participants were given a set of exercises to experiment with the Python-based POX OpenFlow controller [8] and Open vSwitch [7]. Open vSwitch is a software-based OpenFlow-enabled switch, implemented as a Linux kernel module. The presenters demonstrated how to configure Open vSwitch for use with POX, and partici-

pants subsequently ran several experiments that demonstrated the functionality of OpenFlow, including traffic duplication, port forwarding, and host redirection.

2.3 Cybernetic Proving Ground

The third and final lab session was presented by Jakub Čegan, Martin Vizváry and Michal Procházka (Masaryk University) and allowed participants to use the Cybernetic Proving Ground (KYPO) [11], a cloud-based security research testbed. The KYPO provides an artificial network environment to evaluate, study and understand security threats, when the use of real environments is not viable. It allows users to instantiate and run a wide range of cyber attack scenarios. Through network and computing virtualization, the test environment is isolated and any common network configuration can be easily set up.

The lab session itself was divided into two separate parts. First, participants were introduced to the KYPO project [6], infrastructure and functionality. The project's roadmap was described, showing the focus on Distributed Denial of Service (DDoS) attacks in 2013, critical infrastructure scenarios in 2014 and offering the KYPO as a virtualized service in 2015. Additionally, the graphical user interface used to configure, deploy and monitor experiments was described in detail.

In the second hands-on part of the lab session, participants executed a penetration testing scenario, in which they played the role of a hacker trying to compromise a company web server and set it up as a DDoS attacker machine. The challenge was split up into a series of four exercises: (1) exploring the network in order to locate the web server, (2) find vulnerabilities in the web server by using SQL injection, (3) take over the web server through the identified vulnerabilities, and (4) configure the server to serve as a DDoS amplifier. Finally, a set of guidelines was given based on the results of the exercises, showing how to detect and prevent the demonstrated attacks.

3 Educational Session and Keynote

This edition of AIMS extended its keynote tradition by having two keynote sessions. The first, named "Educational Session" has been included as part of AIMS effort of focusing on PhD students and young researchers. This year, the "Educational Session" was given by Aiko Pras (University of Twente) on "Where to publish". The second keynote session, with title "Modern Security Analytics: Finding a Needle in the Hay Blower" was given by Martin Rehák (Cisco Systems and Czech Technical University in Prague).

Aiko Pras has engaged the audience in a highly interactive presentation, challenging PhD students in forming an informed opinion on appropriate publication venue and recognizing high profile conferences. The talk presented several metrics that are nowadays used for quantifying conferences and journals quality (e.g., among others, h-index and impact factor), and highlighted how these are often used for creating conference and journals rankings and, indirectly, for judging the quality of researchers. The takeaway message, that was primarily targeted to PhD students, but it certainly was not lost on more senior researchers, is that one needs a publication plan. Although the presentation made clear that choosing a venue

is not a simple task and certainly experience plays a role, the talk ended with a series of practical tips for avoiding pitfalls and spot good publications venues.

The second keynote was delivered by Martin Rehák, senior engineer at Cisco Systems and lecturer at the Czech Technical University in Prague. The talk introduced step by step the audience security analytics in nowadays networks, highlighting the need for fast reaction as well as precision, while at the same time we are required to implement security in a big data. Martin Rehák has made a clear case for the different type of expertise that need to be combined for successfully counter-fight targeted malware, clearly indicating that the way forward in the security analytics is based on an "ensemble approach": combining and re-enforcing the output different detectors will ultimately improve the overall precision of the system and keep the number of events to handle within reasonable proportions.

For additional information on the keynote speakers and accessing their presentation, we point the reader to the AIMS 2014 website [1].

4 Technical Paper Sessions

The three technical sessions of AIMS 2014 – covering "Emerging Infrastructures for Networks and Services", "Experimental Studies for Security Management", and finally, "Monitoring Methods for Quality-of-Service and Security" – included 9 full papers, which were selected after a thorough reviewing process out of a total of 29 submissions. All papers received at least three independent reviews. This year, an important part of the submissions targeted security aspects of emerging networks and services, a theme that was reflected in the technical program while also bringing a particular emphasis with the keynote speech of Martin Rehák. Each paper was presented in a 20-25 minutes time slot followed by 5-10 minutes for questions and discussions. The richness and variety of papers, going from a high technical expertise (e.g., "Detection of Network Flow Timestamp Reliability" by Žádník et al.) to high level methodologies (e.g., "Trade-off-based Adoption Methodology for Cloud-based Infrastructures and Services" by Garg and Stiller) were an important component to still successfully follow the already established tradition of an unusually vivid and interactive conference series.

In order to select the best paper at AIMS 2014, a best paper award committee was established. The IFIP sponsored the award for the best paper. The best paper award committee was established among one TPC Co-chairs (Guillaume Doyen, associate professor at Troyes University of Technology, France), one PhD workshop TPC Co-chairs (Steven Latré, associate professor at University of Antwerp - iMinds, Belgium), the general chair (Pavel Čeleda, associate professor at Masaryk University, Czech Republic) and a TPC member (Jürgen Schönwälder, full professor at Jacobs University Bremen, Germany). In order to avoid any conflict of interest, committee members who were co-authors of a paper presented at AIMS 2014 were not allowed to evaluate any paper they were involved in. Papers were ranked, on the one hand, according to the respective reviews in the paper submission system, on the other hand by presentation quality. Both dimensions were given equal weight. In application of this evaluation process and after an informal discussion between the best paper committee members, which eventually confirmed the ranking, the best paper was "A Study of RPL DODAG Version Attacks" by

Anthéa Mayzaud, Anuj Sehgal, Remi Badonnel, Isabelle Chrisment and Jürgen Schönwälder.

The conference proceedings [13] include the papers presented at AIMS 2014 and the overall final program. The proceedings demonstrate again the European scope of this conference series since most of accepted papers are from European research groups.

5 PhD Workshop

The AIMS PhD workshop is a venue for early-stage 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, a total of 13 PhD papers were selected for presentation, out of 27 submissions, after a rigorous review process that provided at least 3 independent reviews for each paper. The workshop was structured into four technical sessions covering security, management of virtualized network resources and functions, software-defined networking, and monitoring. All papers presented at the workshop described the current state of the research, including a clear problem statement, the proposed approach and an outline of the results achieved so far.

The first session on management of virtualised network resources and functions featured three papers that focused on network virtualization: either combined with Information-Centric Networking, focusing on learning approaches for network embedding or focusing on the development of virtual router placement engine. While each author took a different perspective to the network virtualization paradigm, their resemblance was striking. Moderated by Prof. Aiko Pras, this resulted in a lively discussion amongst presenters and audience about the true definition of network virtualization and how each presenter could benefit from other presenters work. The second PhD session presented novel advances in the area of security management. The focus within this session was mainly on characterizing security aspects such as botnets, services that provide DDoS on-demand and the trustworthiness of a host. In addition, techniques were discussed for efficient security management for mobile devices using cloud-based principles. The topic of the third session focused on Software Defined Networking (SDN) and content delivery approaches. The authors discussed how an OpenFlow-based SDN architecture could be used to support IP mobility, how the SDN paradigm can be a potential solution for the distributed detection and mitigation of DDOS attacks, and on the content-delivery challenges for device-to-device communication in high density networks such as festivals or other mass events. In the last PhD session, we focused on monitoring challenges. The session included topics as how flow monitoring should also include application protocol information, the architectural challenges and a possible architecture for traffic sampling and how real-time dynamic spectrum management can be enforced and applied to 4GBB, the intermediate technology between DSL and FTTH.

The added value of the PhD workshop lies, since its first edition, in the lively discussions between the audience and the presenter. Such discussions are often led by the more senior researchers, who take upon them the role of challenging the new PhD students to look critically at their research. Also this year, the PhD workshop had a dynamic flavor to the presentation discussions. In addition, the students'

presentations have given the opportunity to the participants to identify common areas of interest and expertise, paving the way for possible future collaborations.

6 Evaluation and Conclusions

Since AIMS 2013, the organization committee and the steering committee have worked together to better define AIMS' DNA and its position within the network and service management community. This year edition of AIMS has followed up on AIMS 2013 report [10] and implemented several activities dedicated to the academic training of PhD students and young researchers. Two of such activities are the aforementioned structural integration of the labs into the conference and the creation of the "Educational Session". The feedback on these activities has been positive, as indicated for example by the interactive discussion during the "Educational Session" and the high attendance to the labs. In addition, AIMS 2014 has implemented a lightweight form of shepherding for the accepted papers in the main track, with the goal of offering the authors additional guidance during the camera-ready preparation. The paper shepherding has also been in overall positively received. We believe shepherding reinforces AIMS' DNA although we are also aware that it will need some years to be smoothly included in the conference structure.

AIMS 2014 conference was attended by 44 people, a number that conforms with the trend for the previous editions [9]. The majority of the attendees came from universities and research centers within Europe. We achieved highly interactive discussions in a relaxed environment. The event confirmed one of the key goals of AIMS to provide PhD students and young researchers with a constructive feedback by senior scientists and give them the possibility of growing in the research community.

We are pleased to announce the AIMS 2015 conference on June 23 – 26, 2015, hosted by Ghent University, Belgium. The organising committee, led by Filip De Turck (filip.deturck@intec.ugent.be), general chair, is delighted to invite you to join us in Ghent for another conference in this very successful series.

Acknowledgements We 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 the authors, who submitted their contributions to AIMS 2014, and to the tutorial and keynote speakers. The great review work performed by the members of both the AIMS TPC and the PhD workshop TPC as well as additional reviewers is highly acknowledged. Additionally, many thanks to the local organizers Iva Krejčí, Alena Janebová, Jan Vykopal and Tomáš Jirsík for enabling the logistics and hosting the AIMS 2014 event. AIMS 2014 was supported by FLAMINGO, a Network of Excellence project (318488).

References

1. AIMS 2014 Conference Web Site. URL `http://www.aims-conference.org/2014/`. Accessed July 2014
2. Emulab – Network Emulation Testbed. URL `http://www.emulab.net/`. Accessed August 2014
3. Fed4FIRE – Federation for Fire. URL `http://www.fed4fire.eu/`. Accessed August 2014
4. Flamingo European (ICT-FP7) Network of Excellence. URL `http://www.fp7-flamingo.eu/`. Accessed July 2014

5. IFIP TC6 Working Group 6: Management of Networks and Distributed Systems. URL http://www.simpleweb.org/ifip/. Accessed July 2014
6. KYPO – Cybernetic Proving Ground. URL http://www.muni.cz/ics/kypo. Accessed August 2014
7. Open vSwitch – An Open Virtual Switch. URL http://openvswitch.org/. Accessed August 2014
8. POX – Python-based OpenFlow controller. URL http://www.noxrepo.org/pox/about-pox/. Accessed August 2014
9. Almeroth, K.: Networking Conferences Statistics. URL http://www.cs.ucsb.edu/~almeroth/conf/stats/#aims. Accessed July 2014
10. Doyen, G., Waldburger, M., Sperotto, A., Čeleda, P., Gorricho, J.L., Schaaf, T., Serrat, J.: Report on the 7th International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2013): Emerging Management Mechanisms for the Future Internet. Journal of Network and Systems Management **22**(2), 289–296 (2014)
11. Kouřil, D., Rebok, T., Jirsík, T., Čegan, J., Drašar, M., Vizváry, M., Vykopal, J.: Cloud-based Testbed for Simulation of Cyber Attacks. In: Proceedings of the Network Operations and Management Symposium (NOMS 2014). Krakow, Poland (2014)
12. Saino, L., Cocora, C., Pavlou, G.: A toolchain for simplifying network simulation setup. In: Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques, SIMUTOOLS '13. ICST, Brussels, Belgium (2013)
13. Sperotto, A., Doyen, G., Latré, S., Charalambides, M., Stiller, B. (eds.): Proceedings of the 8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2014) – Monitoring and Securing Virtualized Networks and Services, *Lecture Notes in Computer Science (LNCS)*, vol. 8508. Springer (2014)

Author Biographies

Anna Sperotto is a postdoctoral researcher at the Design and Analysis of Communication Systems Group (DACS) of the University of Twente, The Netherlands. She received a MSc degree in Computer Science from the Ca' Foscari University, Venice, Italy, in 2006. After that she joined the University of Twente where, in 2010, she received the PhD degree with a thesis on "Flow-based Intrusion Detection". Her current research interests are in the field of network monitoring and network security.

Guillaume Doyen is an associate professor in Troyes University of Technology (UTT) since 2006. He is affiliated to both the CNRS Sciences and Technologies for Risks Management lab (STMR-ICD/ERA) and the INRIA Grand Est, as an associate researcher. His current research interest focuses on the design of autonomous management and control solutions applied to the performance and security of content distribution and cloud computing.

Steven Latré is an assistant professor at the University of Antwerp, Belgium. He received a Master of Science degree in computer science from Ghent University, Belgium and a Ph.D. in Computer Science Engineering from the same university. His research activity focuses on autonomous management and control of both networking and computing applications. His recent work has focused on Quality of Experience optimization and management, distributed control and network virtualization. He has also been involved in several national and European research projects. He is author or co-author of more than 45 papers published in international journals or in the proceedings of international conferences.

Marinos Charalambides is a Research Fellow at the Department of Electronic and Electrical Engineering, UCL. He received a BEng (First Class Hons.) in Electronic and Electrical Engineering, an MSc (Distinction) in Communications Networks and Software, and a PhD in Policy-based Management, all from the University of Surrey, UK, in 2001, 2002 and 2009, respectively. He has been working as a research associate in a number of UK national and EU projects since 2006. His research interests include policy-based management, resource optimization and traffic engineering, network monitoring, and software-defined networking.

Jeroen Famaey is post-doctoral researcher at the Department of Mathematics and Computer Science, University of Antwerp, Belgium and affiliated as a senior researcher with the iMinds

Future Internet department. He received his M.Sc. degree in Computer Science from Ghent University in 2007 and a Ph.D. in Computer Science Engineering, on federated management of multimedia streaming services, from the same university in 2012. His research interests include multimedia streaming services, federated and inter-domain network management, network and cloud resource management, and applied optimization theory and machine learning.

Petr Velan is a Ph.D. student at the Faculty of Informatics at the Masaryk University in Brno, where he received his master's degree in 2012. He works on several projects at the Institute of Computer Science at the Masaryk University. His research interests include network monitoring, flow data collection and analysis, and hardware-accelerated high-speed measurement of network traffic.

Pavel Čeleda is an associate professor affiliated with the Institute of Computer Science at the Masaryk University in Brno since 2006. He holds a Ph.D. in informatics from University of Defence. His main research interests include monitoring of any network, cyber security and development of network security devices. He participates in a number of academia, industry and defence projects.