Munich Internet Research Retreat 2016

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

This article summarises a 2 day long Munich Internet Research Retreat held in November 2016. The goal of the retreat was to provide a forum for both academic and industrial researchers to exchange ideas and get feedback on their current work. It was organized in a spirit that is similar to an highly interactive Dagstuhl seminars, with a very limited number of full-length talks, while dedicating most of the time to poster sessions, panels and group discussions. The entire set of presentations delivered during the seminar is made publicly available at [1].

Keywords

SDN, NFV, Security, IoT, Internet measurements

1. INTRODUCTION

2. INVITED PRESENTATIONS

The invited presentations were intended as a basis for triggering discussions and identifying areas for group work.

2.1 Edge Computing considered harmful

2.2 Towards A Clean Slate – Digital Sovereignty in the Post Snowden Era

2.3 On software network management

2.4 FlexNets: Quantifying Flexibility in Communication Networks

2.5 An Accidental Internet Architecture

2.6 Measuring IPv6 Performance

2.7 Path tracing and validation of IPv4 and IPv6 siblings

2.8 SWIFT: Predictive Fast Reroute upon Remote BGP Disruptions

2.9 Open Platforms for Cyber-physical systems

2.10 Collaborative intrusion handling using the Blackboard-Pattern

3. PARALLEL GROUP WORK

The afternoon sessions were used to discuss certain topics in more depth in smaller groups. This section summarises the discussions of each group.

3.1 SDN/NFV Measurements

3.2 SDN++: Applications Perspective

The breakout session entitled SDN++ dealt with SDN from the perspective of how to apply SDN, and how to introduce improvements to SDN (thereby creating SDN++), for better meeting the identified requirements. Participants of the breakout session were Laurent Vanbevier, Artur Hecker, Wolfgang Kellerer, Edwin Cordeiro and Georg Carle, the latter also being the presenter of the results. The method of the working group was first to identify relevant application areas of SDN, then assess to which extent known SDN approaches have shortcomings (i.e., identifying the 'SDN pain areas'), and subsequently identifying promising approaches for improving SDN. The application areas of SDN were (1) establishing means for programmability of the network, which can be used for improving certain network properties, (2) management of advanced cellular networks, in particular 5G networks, for different capabilities such as network slicing, and (3) providing means to add sophisticated control functionality to corporate networks, such as adding flexible access control. Identified weaknesses of existing SDN were the fact that existing SDN southbound interfaces, in particular OpenFlow, operate on a low level of abstraction, which makes programming of the network time-consuming and error prone. Identified areas of improvement and need for further work were specifying suitable high-level interfaces and abstractions. There further is the need to develop tools that are capable of automatically translate high-level specifications to low-level configuration. A complete tool chain is required. This includes measurement tools that are capable of monitoring changes. Network programmability is beneficial for measurement tools. It is expected that SDN management tools will facilitate to deal with the programmability of networks. Furthermore, verification tools will allow to detect and prevent attempts of wrongly programming the network. These tools will form a network operating system, with tools that operate on top of the operating system functions. Another need for improvement is the development of a clear transition path from today's networks to future SDN-based networks. This includes to identify which legacy functionalities from today's networks we assume being able to depend on in SDN deployments.

3.3 QUIC

3.4 DDoS Defence beyond Centralization

3.5 Security

The security breakout session covered civil liberties and privacy.

Firstly, the group set its focus and decided not to discuss the topics of trustworthy hardware or civil liberties, but instead to concentrate on SDN security and problems of cloudification

Key results: 1) Customer networks are converging: Customers want less own hardware, and want to be more independent and to lease remote services and equipment rather than owning it. 2) Virtualization (which happens when you cloudify applications) amplifies known problems in traditional fields like security, trust, verifiability or visibility. 3) A special challenge is the cloudification of services that already utilize virtualization in the traditional model, for example sandboxes that analyze malware. For a cloud case, one would end up with nested virtualization, which in turn comes with even new problems concerning performance and visibility of the virtualization to the malware being inspected 4) Encryption of data still leads to the usability of cloud scenarios being reduced to mostly SaaS, because homomorphic encryption is still not there to solve these problems 5) Special problems with end-to-end security, e.g., there is more end-to-end encryption happening, which is good. As a downside however, it makes life harder for people inspecting traffic in the middle If termination of encrypted connections is done in the cloud, there will be an unencrypted last mile as new security issue arising from this scenario.

3.6 IoT

4. POSTERS

Participants were also encouraged to volunteer to bring a poster to provide a perspective into their recent measurement research work.

5. CONCLUSIONS AND NEXT STEPS

Acknowledgements

This seminar was located at the TUM Science and Study Center in Raitenhaslach, Germany, supported by ... The organisers would like to thank the participants (alphabetically ordered by first name) for their contributions:

Aaron Yi Ding (TUM CM), Alberto Martínez Alba (TUM LKN), Alexander von Gernler (genua GmbH), Andreas Blenk (TUM LKN), Arsany Basta (TUM LKN), Artur Hecker (Huawei), Brian Trammell (ETH Zürich), Christian Prehofer (fortiss, TUM), Claas Lorenz (), Daniel Raumer (TUM NET), Dirk Kutscher (Huawei), Edwin Cordeiro (TUM NET), Florian Westphal (Red Hat), Georg Carle (TUM NET), Hagen Paul Pfeifer (Rohde & Schwarz), Heiko Niedermayer (TUM NET), Johannes Naab (TUM NET), Jörg Ott (TUM CM), Holger Kinkelin (TUM NET), Lars Eggert (NetApp), Laurent Vanbever (ETH Zürich), Marco Hoffmann (Nokia Bell Labs), Markus Klügel (TUM LKN), Matthias Wachs (TUM NET), Minoo Rouhi (TUM NET), Mirja Kühlewind (ETH Zurich), Nemanja Djeric (TUM LKN), Paul Emmerich (TUM NET), Pavel Laskov (Huawei), Peter Babarczi (TUM NET), Raphael Durner (TUM LKN), Rastin Pries (Nokia Bell Labs), Rolf Winter (University of Applied Sciences Augsburg), Sebastian Gallenmüller (TUM NET), Vaibhav Bajpai (Jacobs University Bremen), Wolfgang Kellerer (TUM LKN),

6. REFERENCES

[1] Munich Internet Research Reat 2016: Materials. https://www.cm.in.tum.de/en/mir.