A Report on the Munich Internet Research Retreat 2017

ABSTRACT

This article summarizes the two-day Munich Internet Research Retreat (MIR) held in May 2017. 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 highly interactive "Dagstuhl" seminars, with a very limited number of full-length talks, while dedicating most of the time to poster sessions and group discussions. Presentations delivered during the seminar are made publicly available [4].

1. INTRODUCTION

The MIR originated from informal discussions of different research groups at TUM and a team at NetApp on diverse topics related to networking. The discussions brought together PhD students and post-docs to present their respective research (including both work in progress as well as polished results) and provided an informal setting for intense and rich exchange among participants involved. We realised that there was notable potential in reaching out further, which eventually led to the instantiation of the MIR.

The main mission of the MIR is to ensure mutual awareness of different teams working on current (complementary) topics in networking. We want to lay the foundations for establishing, broadening, and deepening cooperation among a variety of groups doing networking research. In order to foster easily sustainable relationships, our initial scope has been deliberately limited to the area around Munich (which may reach as far as 400 km in some cases). As a common denominator, we target like-minded teams within the region, where the common mindset stems from practical research in networked systems, paired with interest and efforts in the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF) and the ACM SIGCOMM and SIGMOBILE communities.

The purpose of the MIR is threefold: 1) We seek to provide recurring opportunities for companies to get in touch with research groups that have expertise in fields relevant to the former. 2) We aim to support researchers in understanding current and emerging research and engineering problems from the commercial development and deployment perspectives. 3) We like to offer reality feedback to academic researchers and out-of-the-box ideas to those from industry. Overall, we hope to foster future bi- or multi-lateral collaboration between academics and industry.

The retreat is organized in a highly interactive fashion, combining posters (for providing variety) and group discussions intertwined with plenary talks that stimulate discussions. Organization directions are shaped by the feedback of the participants, keeping the format constantly evolving. We borrow some elements from the renowned Dagstuhl seminars: We limit the number of participants to $\sim$40 to maintain interactivity and allow all participants to meet one another. We hold the retreat in Raitenhaslach away from the daily activities to ensure focus and include an overnight stay and a social dinner to foster continued interaction and allow for digesting ideas. The seminar is by invitation only, and we put an emphasis on the industry, picking PhD students with matching topics, which helps with obtaining a compatible and energetic mix of people. Because we know that everybody's time is scarce, we organize each retreat in a way that it occupies just two days including arrival and departure. With a target of two workshops per year, presently scheduled for May and November, we shall be able to continuously engage with a growing regional community even if individuals cannot participate on every occasion.

Towards this mission, the 1st MIR retreat was organized on November 24–25, 2016 at the TU Munich (TUM) Science and Study Center inbb Raitenhaslach, Germany. A 2nd iteration of the MIR was organized at the same location and held on May 23–24, 2017. Presentations on topics such as: ... were solicited. The retreat consisted of six invited presentations and several posters presenting early and upcoming research, with several breakout sessions to discuss topics of interests in an informal setting. Synopses of these sessions are described in this report in more detail.

2. INVITED PRESENTATIONS

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

2.1 Opportunistic Content Dissemination Performance in Dense Network Segments

Many of the existing opportunistic networking systems have been designed assuming a small number links per node and have trouble scaling to large numbers of potential concurrent communication partners. In the real world we often find wireless local area networks with large numbers of connected users – in particular in open Wi-Fi networks provided by cities, airports, conferences and other venues. In this talk, Teemu Kärkkäinen (TU Munich) presented a 50 client opportunistic network in a single Wi-Fi access point and use it to uncover scaling problems and to suggest mechanisms to improve the performance of single segment dissemination. Further, we present an algorithm for breaking down a single dense segment dissemination problem into multiple smaller but identical problems by exploiting resource (e.g., Wi-Fi channel) diversity, and validate our approach via simulations and testbed experiments. The ability to scale to high density network segments creates new, realistic use cases for opportunistic networking applications.

2.2 Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication

The design and implementation of cryptographic systems offer many subtle pitfalls. One such pitfall is that cryptography may create unique identifiers potentially usable to repeatedly and precisely re-identify and hence track users. Quirin Scheitle (Technical University of Munich) presented his investigation of TLS Client Certificate Authentication (CCA), which currently transmits certificates in plain text. He demonstrated [8] CCA's impact on client traceability using Apple's Apple Push Notification service (APNs) as an example. APNs is used by all Apple products, employs plain-text CCA, and aims to be constantly connected to its backend. Its novel combination of large device count, constant connections, device proximity to users and unique client certificates provides for precise client traceability. He shows that passive eavesdropping allows to precisely re-identify and track users and that only ten interception points are required to track more than 80 percent of APNs users due to global routing characteristics. The work was conducted under strong ethical guidelines, with responsibly disclosing the findings, and a working patch by Apple for the highlighted issue was confirmed. The aim for this work is to provide the necessary factual and quantified evidence about negative implications of plain-text CCA to boost deployment of encrypted CCA as in TLS 1.3.

2.3 Dynamic MultiPath Routing Protocol

Safety critical communication platforms often deploy multiple heterogeneous wireless link layer access technologies like ETSI TETRA, IEEE 802.11, IEEE 802.15.4, 3GPP LTE, satellite terminals or proprietary waveforms. Depending on the interface characteristics, vendor specific decisions and other aspects, these often come shipped with suitable mobile ad-hoc routing protocols to form networks in an autonomous manner - independently for each link type. 802.11 links typically deploy OLSR, BATMAN or 802.11s, whereas proprietary waveforms often come with proprietary MANET protocols. To bridge these access networks at a logically higher level and provide an opaque operational network view, a network routing protocol at the top is required. Exterior routing protocols like BGP are limited in their use and features like automatic neighbor detection or reduced message overhead are required. Dynamic Multipath Routing (DMPR) tries to address these shortcomings and provides exterior routing protocol features for heterogeneous link layer environments even in low bandwidth environments. Furthermore, DMPR features policy based routing to route traffic through different paths if required or advantageous.

2.4 Internet of Things Security: TrustZone for v8-M architecture

Internet of Things (IoT) devices today use microcontrollers that are limited in CPU performance, as well as in RAM and flash size. Many of these devices use the ARM A-class or M-class processors. A-class CPUs are able to run popular operating systems (OS), such as embedded Linux, while M-class CPUs use Real-Time Operating Systems. So far, the security functionality of M- and A-class CPUs has been very different. A-class CPUs can use sophisticated hardware features, such as TrustZone offering physical separation between the normal and the secure world operating systems. M-class CPUs offer basic security protection using the memory protection unit (MPU), which offers memory isolation. Many IoT products, however, use very few operating system security techniques, if they run an OS at all, and often do not make use of hardware security support. While the exact reasons for these design decisions remain unclear, the growing list of IoT security failures calls for improved protection capabilities. With the introduction of the TrustZone for ARMv8-M architecture, security features known from the mobile world are now available in the IoT environment. Additionally, ARM v8-A processors enhance security with the Pointer Authentication Extension, which prevents return-oriented programming-based attacks. In this talk Hannes will explain the hardware security features offered by upcoming ARM processors and microcontrollers.

2.5 Redesigning Stack, API and Networks

Emerging Non-Volatile Main Memories (NVMMs), also known as storage-class memory and persistent memory push the majority of end-to-end latency that includes durable I/O to network stacks and their APIs. This not only impairs inherent performance of NVMMs that is one to two orders of magnitude faster than traditional persistent medias like SSDs, but prevents systems from adopting them to be reliable with relative ease. Our work investigates solving this problem, designing an efficient network stack and its APIs, and exploring new opportunities in networking such as software switches and middleboxes in addition to improving networked storage systems.

3. PARALLEL GROUP WORK

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

4. POSTERS

Participants were encouraged to bring posters to present their recent research work.

4.1 Dynamic MultiPath Routing

Safety critical communication platforms often deploy multiple heterogeneous wireless link layer access technologies like ETSI TETRA, IEEE 802.11, IEEE 802.15.4, 3GPP LTE, satellite terminals or proprietary waveforms. Depending on the interface characteristics, vendor specific decisions and other aspects, these often come shipped with suitable mobile ad-hoc routing protocols to form networks in an autonomous manner - independently for each link type. 802.11 links typically deploy OLSR, BATMAN or 802.11s, whereas proprietary waveforms often come with proprietary MANET protocols. To bridge these access networks at a logically higher level and provide an opaque operational network view, a network routing protocol at the top is required. Exterior routing protocols like BGP are limited in their use and features like automatic neighbor detection or reduced message overhead are required. DMPR tries to address these shortcomings and provides exterior routing protocol features for heterogeneous link layer environments even in low bandwidth environments. Furthermore, DMPR features policy based routing to route traffic through different paths if required or advantageous.

4.2 PASTE: A Networking Interface for NVMMs

Emerging Non-Volatile Main Memories (NVMMs), also known as storage-class memory and persistent memory push the majority of end-to-end latency that includes durable I/O to network stacks and their APIs. This not only impairs inherent performance of NVMMs that is one to two orders of magnitude faster than traditional persistent medias like SSDs, but prevents systems from adopting them to be reliable with relative ease. Michio Honda (NEC) presented an investigation of this problem, designing an efficient network stack [2] and its APIs, and exploring new opportunities in networking such as software switches and middleboxes in addition to improving networked storage systems.

4.3 Measuring the Performance of Mobile Users

In a mobile network, the mobile terminal (MT) continuously exchanges link related metrics and signals to the nearby base station to measure the strength and quality of the received signal. Quality of Service (QoS) metrics are used for handover decisions and cell reselection. A handover can occur if there is a strong radio signal in the neighboring cell while the serving cell's radio signal is getting diminished. However, previous studies [7] show that it is not always the value of signal strength that matters to have a good throughput performance. Therefore, knowing the possible achievable throughput value before making a handover is equally important along with link-related QoS metrics. Ermias Walelgne (Aalto University) proposes a solution to estimate the throughput value of post-handover using the metrics collected from the current serving base station. The result of this throughput prediction can be combined with other link QoS metrics such as RSSI and RSPQ values for better handover decision.

4.4 Lightweight Virtualization for Smart Cars

Modern vehicles are equipped with several interconnected sensors on board for monitoring and diagnosis purposes; their availability is a main driver for the development of novel applications in the smart vehicle domain. Roberto Morabito [3] presented a Docker container-based platform as solution for implementing customized smart car applications. Through a proof-of-concept prototype—developed on a Raspberry Pi3 board—we show that a container-based virtualization approach is not only viable but also effective and flexible in the management of several parallel processes running on On-Board Unit. More specifically, the platform can take priority-based decisions by handling multiple inputs, e.g., data from the CANbus based on the OBD II codes, video from the on-board webcam, and so on. Results are promising for the development of future in-vehicle virtualized platforms.

4.5 Data-driven Mobility Modeling

Ljubica Pajević Kärkkäinen (TU Munich) presents an analysis of a large trace of user associations in a university wireless network, which includes around one thousand access points on five campus sites. The trace was obtained from authentication logs of the RADIUS server collected over 16 months. User access patterns, specifically the arrival processes of users to wireless access points, visiting time duration, as well as the user arrival patterns to the buildings in the campus are studied. She observed that that a large fraction of the network – around half of all access points – exhibit Poisson arrival process, which is advantageous for modeling and prediction of network occupancy. By analyzing duration of associations with access points, she shows that the visiting time distributions can be modeled by two-stage hyper-exponential distributions. While network associations in campus wireless networks have been extensively studied in the literature, this study reveals changing access patterns, which seem to be characteristic for networks of predominantly mobile users.

4.6 iConfig - What I See is What I Configure

Michael Haus (TU Munich) presented iConfig to manage Internet of Things (IoT) devices in smart cities. The management of IoT devices in urban areas is becoming important due to that the majority of the people living in cities and the number of deployed IoT devices are increasing. Therefore, iConfig addresses three major issues in current IoT management: registration, configuration, and device maintenance. To achieve the goals of iConfig, the presented system relies on programmable edge modules, which can run on smartphones, wearables, and smart boards to configure physically proximate IoT devices.

4.7 Opportunistic Content Dissemination

Many of the existing opportunistic networking systems have been designed assuming a small number links per node and have trouble scaling to large numbers of potential concurrent communication partners. In the real world we often find wireless local area networks with large numbers of connected users – in particular in open Wi-Fi networks provided by cities, airports, conferences and other venues. In this talk, Teemu Kärkkäinen (TU Munich) presented a 50 client opportunistic network in a single Wi-Fi access point and use it to uncover scaling problems and to suggest mechanisms to improve the performance of single segment dissemination. Further, we present an algorithm for breaking down a single dense segment dissemination problem into multiple smaller but identical problems by exploiting resource (e.g., Wi-Fi channel) diversity, and validate our approach via simulations and testbed experiments. The ability to scale to high density network segments creates new, realistic use cases for opportunistic networking applications.

4.8 A Group Recommender System for Trips

Recommender systems (RSs) in tourism often recommend single Points of Interests (POIs) such as restaurants or museums. However, tourists visiting a destination are usually looking for a tourist trip composed of multiple POIs along a practical route. Daniel Herzog (TU Munich) presented a Recommender system (RS) [9] recommending tourist trips to a group of users. This is a particularly complex problem as the RS has to aggregate the travel preferences of all group members before generating recommendations. Furthermore, he wants to research on how different devices and user interfaces can support groups in providing feedback on recommendations and finding a consensus.

4.9 Data Dissemination in Vehicular Networks

Lars Wischhof (Hochschule München) presented an architecture and preliminary results of an on-going research project at the research group where communication schemes combining cellular communication with direct-communication (such as Device-to-device (D2D) modes of the latest LTE-A releases or LTE-V) are combined for applications in intelligent mobility. The basic assumption is that future vehicles will most-likely have multiple communication technologies and modes available. Therefore, a context-aware selection of the communication mode is advocated. A suitable architecture is outlined. First simulation results for the example of a DENM-based application indicate that a context-aware selection can outperform a static assignment.

4.10 Accountability for Cyber-Physical Systems

Severin Kacianka (TU Munich) seeks to capture the essential features of an accountable (computer-)system. Logs are, for example, a common way to create evidence and establish "truth" in computer systems. Another facet are mechanisms to process those logs and techniques to formulate the questions of compliance with laws as queries against those logs. However, there are currently no "blue prints" on how to make a system "accountable". We wish to develop a comprehensive framework that makes it possible to explicate the accountability features of a system, reason about their effectiveness, compare it to other solutions and offer options to exchange one specific component for another.

4.11 Real-time TE in the Internet

Edwin Cordeiro (TU Munich) aims to create a network solution capable of detecting and avoiding congestions in the Internet. The avoidance is done automatically by a central controller adapting running network protocols and network routes to avoid congestion. Such objectives are divided in two parts. The first one is the creation of a method capable of detecting congestion in the Internet in real-time without probes at destinations. The second is the implementation of Software Defined Networks (SDN) ideas in the routing system using the Interface to the Routing System (I2RS) protocol, that is being specified by IETF.

4.12 Fine-Grained Edge Offloading for IoT

Vittorio Cozzolino (TU Munich) makes the case for IoT edge offloading, which strives to exploit the resources on edge computing devices by offloading fine-grained computation tasks from the cloud closer to the users and data generators (i.e., IoT devices). The key motive is to enhance performance, security and privacy for IoT services. The proposal bridges the gap between cloud computing and IoT by applying a divide and conquer approach over the multi-level (cloud, edge and IoT) information pipeline. To validate the design of IoT edge offloading, a unikernel-based prototype is developed and evaluated the system under various hardware and network conditions.

4.13 CARISSMA

Center of Automotive Research on Integrated Safety Systems and Measurement Area (CARISSMA) is a new center for vehicle safety. Its focus is on passive as well as active vehicle safety research. The main goal is to develop a global safety system to support 'Vision Zero', achieving the ultimate goal of zero traffic deaths. Therefore, all relevant disciplines are combined in one building. Nine professors alongside 47 staff members pursue are working in, e. g. an indoor driving area and full-vehicle crash test facility, a drop tower, a HiL-lab, a full-vehicle test bench, a lab for safe energy storage, a car2x-laboratory, a simulation lab and an open-air ground for performing full-vehicle tests.

4.14 Car2X Lab

Research on Car2X communication, the wireless communication between vehicles and other road participants, is gaining a major part of CARISSMA. The Car2X research facilities feature a powerful simulation computer, which helps to leverage our Open Source in-house Car2X simulation tools "Artery" and "Vanetza". These tools will also be integrated in our Car2X experimental vehicle, blending virtual simulation and real test drives for semi-virtualized testing. In addition to this, the research is focusing on HIL-testing of Car2X equipment. Further research topics are Teleoperated Driving and the use of Mobile Edge Computing for vehicular applications.

4.15 SENDATE Project

– Nemanja Deric

4.16 FlexNets - Quantifying Flexibility in Communication Networks

– Alberto Martínez:

4.17 Internet Architecture and its Security Implications

Quirin Scheitle (TU Munich) presented research directions in both Internet Architecture and Security questions. Examples for this are Geolocation of Routers using Ripe Atlas [5], mapping the communication flows and backend infrastructures of Mobiles Messaging Services such as WhatsApp or WeChat [6], and about creation and operation of an IPv6 hitlist [1].

5. CONCLUSIONS AND NEXT STEPS

The 2nd Munich Internet Research retreat concluded successfully on May 23–24, 2017. All the presentation material and contact information of presenters are available online [4]. The readers are encouraged to contact the organizers to learn more about the the next retreat.

We also collected some feedback from the participants.

Acknowledgements

This seminar was located at the TUM Science and Study Center in Raitenhaslach, Germany, supported by NetApp, Huawei, and TUM. The organizers would like to thank the participants (alphabetically ordered by first name) for their contributions— Alberto Martínez Alba (TUM) Alf Zugenmaier (Hochschule München) Arend Martin (BMW AG) Christian Facchi (TH Ingolstadt) Christoph Nufer (Rohde & Schwarz) Daniel Herzog (TUM) Dirk Kutscher (Huawei German Research Center) Dominik Scholz (TUM) Edwin Cordeiro (TUM) Ermias Walelgne (Aalto University) Florian Westphal (Red Hat) Georg Carle (TUM) Hagen Paul Pfeifer (Rohde & Schwarz) Hannes Tschofenig (ARM) Holger Kinkelin (TUM) Johannes Naab (TUM) Jörg Ott (TUM) Lars Eggert (NetApp) Lars Wischhof (Hochschule München) Ljubica Pajević Kärkkäinen (TUM) Marius Strobl (NetApp) Michael Haus (TUM) Michio Honda (NEC) Nemanja Deric (TUM) Quirin Scheitle (TUM) Roberto Morabito (Ericsson Research Finland) Severin Kacianka (TUM) Simon Leinen (SWITCH) Stefan Neumeier (TH Ingolstadt) Teemu Kärkkäinen (TUM) Vaibhav Bajpai (TUM) Vittorio Cozzolino (TUM)

6. REFERENCES

[1] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle. Scanning the ipv6 internet: towards a comprehensive hitlist. *Proc. 8th Int. Workshop on Traffic Monitoring and Analysis*, 2016.

[2] M. Honda, L. Eggert, and D. Santry. PASTE: Network Stacks Must Integrate with NVMM Abstractions. *Proc. ACM HotNets*, pp. 183–189, 2016.

[3] R. Morabito, R. Petrolo, V. Loscri, N. Mitton, G. Ruggeri, and A. Molinaro. Lightweight Virtualization as Enabling Technology for Future Smart Cars. *International Symposium on Integrated Network Management (IM)*, 2017.

[4] Munich Internet Research Retreat 2017. Presentation Materials: https://www.cm.in.tum.de/en/mir/2017.

[5] Q. Scheitle, O. Gasser, P. Sattler, and G. Carle. Hloc: hints-based geolocation leveraging multiple measurement frameworks. *Network Traffic Measurement and Analysis Conference (TMA)*, 2017.

[6] Q. Scheitle, M. Wachs, J. Zirngibl, and G. Carle. Analyzing locality of mobile messaging traffic using the matador framework. *Passive and Active Measurements Conference (PAM) 2016*, Mar. 2016.

[7] S. Sonntag, L. Schulte, and J. Manner. Mobile network measurements - it's not all about signal strength. *2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, Shanghai, China, April 7-10, 2013*, pp. 4624–4629, 2013.

[8] M. Wachs, Q. Scheitle, and G. Carle. Push Away Your Privacy: Precise User Tracking Based on TLS Client Certificate Authentication. *Network Traffic Measurement and Analysis Conference (TMA)*, Jun. 2017.

[9] W. Wörndl, A. Hefele, and D. Herzog. Recommending a sequence of interesting places for tourist trips. *J. of IT & Tourism*:31–54, 2017.