The Munich Internet Research Retreat (MIRR)

Vaibhav Bajpai
TU Munich
bajpaiv@in.tum.de

Aaron Yi Ding
TU Munich
ding@in.tum.de

Holger Kinkelin
TU Munich
kinkelin@in.tum.de

Georg Carle
TU Munich
carle@in.tum.de

Lars Eggert
NetApp
lars@netapp.com

Wolfgang Kellerer
TU Munich
wolfgang.kellerer@tum.de

Jörg Ott
TU Munich
ott@in.tum.de

ABSTRACT

This article describes the format of an outset series of research retreats and our efforts to improve the outcomes and the participation experience. We believe that our lessons learned are beneficial for organizers of similar events. The Munich Internet Research Retreat (MIRR) is a two-day gathering of Internet researchers from academia and industry locating in Munich, Germany area. The goal is to provide a forum for researchers to exchange ideas, get feedback on their current work, enlarge their professional network, and to foster collaboration between industry and academia. MIRR is organized in a highly interactive style. It consists of six short talks and most of the time is dedicated to poster sessions, group discussions, and breakout sessions. A further important element is the feedback session at the end of the retreat where we collect suggestions for improvement. After the inaugural event in November 2016, MIRR took place for the second time in May 2017. Further successors are planned every six months. Presentations delivered during the seminar are made publicly available online [19].

1. INTRODUCTION

The Munich Internet Research Retreat (MIRR) originated from informal discussions of different research groups at Technische Universität München (TUM) and a team at the Munich branch of NetApp[20] on diverse topics related to networking. In these meetings, PhD students and postdoctoral fellows (post-docs) presented their respective research, including both work in progress as well as polished results. The meetings created an informal setting for intense and rich exchange among participants. We realized that there was notable potential in reaching out further, which eventually led to the instantiation of the MIRR.

The main mission of the MIRR is to ensure mutual awareness of different teams from industry and academia working on current (complementary) topics in networking. Our scope ranges from network measurements, to systems engineering, to security and privacy problems in networks. 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 MIRR 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.

Towards this mission, the 1st MIRR retreat was organized on November 24–25, 2016 at the TUM Science and Study Center in Raitenhaslach, Germany[1]. A 2nd iteration of the MIRR was organized at the same location and held on May 23–24, 2017.

With this editorial we hope to provide useful insight for first-time organizers of similar research retreats, or start discussions with organizers of comparable formats. In section 2, we outline our highly tentative agenda and explain the purposes of the various action points. One quite important action point at the end of the retreat is collecting feedback from our participants. We summarize our insights from this session in section 4 and other lessons that we have learned. Besides focusing on the MIRR format itself, we also provide a rather short overview on the topics that have been discussed at both retreats in section 3.

2. RETREAT FORMAT

The main concern while organizing the retreats is to create an opportunity where researchers of academia and industry

meet each other and discuss about their work. We try to put this goal into practice with the approach described below. Some selected elements were adapted from seminars held in the renowned Leibniz Center for Informatics in Dagstuhl, Germany [16].

1) We hold the MIRR in the TUM Science and Study Center in Raitenhaslach, a former monastery, away from the daily activities of our participants to ensure focus. We also include an overnight stay and a social dinner to foster continued interaction and allow for digesting ideas. 2) The seminar is by invitation only. We put an emphasis on the industry and hand pick PhD students or post-docs with matching topics. This helps with obtaining a compatible and energetic mix of people. 3) We limit the number of participants to ∼40 to maintain interactivity and allow all participants to meet one another and create professional contacts. 4) MIRR is organized to provide a maximum of interactive action points on the agenda. Each participant is requested to bring two slides that include his/her photo, some keywords describing ones current research focus, and questions that he/she likes to discuss during the retreat. The slides are used at the beginning of the retreat in a self-introduction session to familiarize participants with another. In the first two iterations of MIRR, we already limited ourselves to about six 20 minutes talks which allows us to dedicate most of the time to more interactive formats like poster or breakout sessions. We furthermore ask all participants to bring a poster. Posters provide variety of topics and introduce the participant's research more profoundly than the short intro slides, and in a more personal and interactive fashion than talks. Furthermore we emphasize discussions both in the plenum as well as in small subgroups (breakout sessions). For breakouts, the plenum first agrees on most relevant topics or questions previously presented by individuals and forms groups with sizes between three to a maximum of six persons. The discussions of the various groups and their most interesting insights are later shared with the plenum in five to ten minutes, improvised talks. For our tentative agenda, see table 1. 5) 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. 6) As we previously mentioned, organization directions are shaped by the feedback of the participants, keeping the format constantly improving.

3. OVERVIEW ON SELECTED TOPICS

In this section we provide an overview on the topics that have been covered in invited talks, breakout sessions, and posters through MIRR.

3.1 System Networking and Measurement

A major theme covered in MIRR is on networking and measurement, which encompasses topics of Software-Defined

Table 1: Tentative MIRR Agenda

	Day 1
10:00	Welcome and self-introduction of participants
12:00	Lunch
13:00	Poster session 1
14:00	Talk session 1
16:00	Poster session 2
17:00	Breakout sessions
18:30	Social dinner

	Day 2
09:00	Reports from breakout sessions
11:00	Talk session 2
13:00	Lunch
14:00	Closing discussion and evolving the retreat
15:00	End

Networking (SDN), Network Function Virtualization (NFV), Internet architecture, networking flexibility, reproducibility, BGP and MultiPath routing management, IPv6 measurement, protocol development of QUIC, and network stack optimization.

In the talk "On software Network Management" by Artur Hecker (Huawei), he argued that the paradigm change brought by software networks does not suit well planning approaches for network dimensioning and design, including but not limited to planning or pre-provisioning of management and control planes. In contrast, he proposed a new model and protocol, aiming to autonomously bootstrap, construct, adjust and maintain control plane including the elastic placement of control compute nodes [17] and control paths without presuming any particular network purpose.

The talk by Wolfgang Kellerer (TUM) on "FlexNets: Quantifying Flexibility in Communication Networks" proposed a definition for flexibility as a new measure for network design space analysis [15] and gives an illustrative example with Software Defined Networks (SDN) controller placement. The goal is to provide a deeper understanding of the flexibility vs. cost trade-off which is missing so far in networking research.

Brian Trammell (ETH Zürich) introduced PostSockets [26] in his talk on "An Accidental Internet Architecture". The work-in-progress proposal intended to allow applications to be developed separate from (possibly runtime-bound) transport protocol dynamics, in turn accelerating the deployment of recent innovations at Layer 4.

The talk on "Measuring IPv6 performance", Vaibhav Bajpai (Jacobs University Bremen) presented his work using 80 dual-stacked SamKnows [4] probes deployed at the edge of the network to measure IPv6 performance of operational dual-stacked content services on the Internet. The talk presented a comparison of how content delivery [5, 2] over IPv6 compares to that of IPv4, and also identified glitches in this content delivery [9] that once fixed can help improve user experience over IPv6. The talks also pointed out areas of improvements

[6] in the standards work for the IPv6 operations community at the IETF.

In "SWIFT: Predictive Fast Reroute upon Remote BGP Disruptions", Laurent Vanbever (ETH Zurich) presented a general fast re-route framework supporting both local and remote failures. The framework SWIFT isbased on two novel techniques. First, SWIFT copes with slow notification by predicting the overall extent of a remote failure out of few control-plane (BGP) messages. Second, SWIFT introduces a new data-plane encoding scheme which enables it to quickly and flexibly update the impacted forwarding entries. The evaluation has shown that SWIFT is able to predict the extent of a remote failure with high accuracy (93%) and SWIFT encoding scheme enables to fast-converge more than 95% of the impacted forwarding entries. Overall, SWIFT reduces the average convergence time from few minutes to few seconds.

Hagen Paul Pfeifer presented in "Dynamic MultiPath Routing Protocol" his proposal Dynamic Multipath Routing (DMPR), which provides exterior routing protocol features for heterogeneous link layer environments even in low bandwidth environments. DMPR features policy based routing to route traffic through different paths if required or advantageous.

In their talks "Persistence in Networking: Redesigning Stack, API and Networks" and "State of Linux Network Development", Michio Honda (NEC) and Florian Westphal (Redhat) highlighted the existing status of kernel development and the demand for more efficient network stack and its APIs. Their talks illusrated new opportunities in networking such as software switches, NIC hardware offloading, extension of the BSD socket API to provide a full zero-copy interface and improvement of networked storage systems.

SDN/NFV Measurements and Applications Perspective

QUIC development

Measurements and Reproducibility

P4 and SDN

Networking APIs

Following active discussions, on-going work has been presented in several posters, including

Cost of Security in the SDN Control Plane

The Baltikum Testbed

FlexNets

Boost Virtual Network Resource Allocation

HyperFlex

SarDiNe

StackMap

PATHspider

PASTE: A Networking Interface for NVMMs

Real-time TE in the Internet

Center ofAutomotiveResearch on Integrated Safety Systems and Measurement Area (CARISSMA)

Project SENDATE

Quantifying Flexibility in Networks

The second theme covered in MIRR is the intersection of IoT, Information-Centric Networking (ICN) and Edge Computing. There were three invited talks that triggered lively discussions.

In the talk "Edge Computing considered harmful" by Dirk Kutscher (Huawei), he challenged the mainstream notion of running application-specific VMs at the network edge and discussed the related security/privacy issues. He argued that low latency should be first-order general requirement and will point at corresponding network and transport layer approaches.

The talk "Open Platforms for Cyber-physical systems" by Christian Prehofer (fortiss) illustrated a timely trend towards open systems which can be extended during operation by instantly adding functionalities on demand. He presented results of the TAPPlications (Trusted Applications for open CPS) project [21], which includes trusted hardware and virtualization of networking and CPU, as well as dedicated execution environments and development support for trusted applications.

Teemu Kärkkäinen (TU Munich) presented in "Opportunistic Content Dissemination in Dense Network Segments" 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. He further proposed 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.

Inspired by those talks, discussion groups on IoT, ICN and Edge Computing have been formed to review the existing issues, open problems, and research directions. The identified problems include: 1) Limitation of existing protocols such as Constrained Application Protocol (CoAP) that handles poorly the frequent leaving/joining events in the network. 2) The stereotype of "IoT gateway design" has hindered novel design. 3) We still have not yet come up with a suitable Internet architecture that integrates IoT coherently.

There are six open questions highlighted by the group: 1) Where does the network end nowadays? This question couples with the ICN where nodes can contribute to the computation/content along the path. 2) What functions on gateway functions we can remove? 3) How to do naming "translation" without changing name/label? 4) Can we do packet processing while it is passing through queue? 5) How to avoid looping in the network functions? This is a key concern since we need to keep a boundary for resource usage in the network. 6) How to maintain the state on the constrained nodes?

The discussion groups also identified a set of potential research directions: 1) Design of end-to-end naming scheme, to facilitate IoT application composition and bring down the overhead of porting applications for the cloud to "gateways". 2) Semantics for individual sensor and equivalence group. 3) Trade accuracy with replication. 4) A new computation abstract suitable for IoT. 5) Abstract of distributed registry for

3.2 IoT, ICN and Edge Computing

network function. 6) Rethink how we distribute computing and content.

Besides invited talks, MIRR also featured several posters, including topics on IoT edge computing "iConfig - What I See is What I Configure", "Fine-Grained Edge Offloading for IoT" [7], "Accountability for Cyber-Physical Systems", from the angle of mobility and opportunistic content distribution "Opportunistic Content Dissemination", "Data-driven Mobility Modeling", "Data Dissemination in Vehicular Networks", and vehicular edge virtualization "Lightweight Virtualization for Smart Cars" [18], "Car2X Lab".

3.3 Security and Privacy

Topics around security and privacy form the third thematic pillar of MIRR. Topics spanning the full spectrum from hardware-related, to protocol-specific, to problems of and introduced by cloud computing were covered.

In their talks "Digital Sovereignty in the Post-Snowden Era" and "IoT Security: TrustZone for v8-M" Alexander von Gernler (genua GmbH) and Hannes Tschofenig (ARM) motivated for hardware offering security features implemented in hardware resp. reported on the latest developments in the 8th version of the ARM A- and M-class processors.

Quirin Scheitle (TUM) presented his investigations on "User Tracking Based on TLS Client Certificate Authentication" [27]. He explained that currently devices often transmit their certificates in plain text and demonstrated the impact of this problem on client traceability using the Apple Push Notification service as an example.

In his talk on "Collaborative intrusion handling using the Blackboard-Pattern" [14], Holger Kinkelin (TUM) presented an approach how the individual components of intrusion handling (intrusion detection, alert processing, intrusion response) can be better intertwined using a blackboard as an information broker between components.

Inspired by Hannes Tschofenig's talk on "IoT Security", a breakout session was formed covering this topic. The participants collected their concerns about IoT security, in particular collateral damage caused by vulnerable IoT devices in the Internet, and listed challenges with IoT security and options for mitigation. This discussion included, for instance, mandatory firmware updates to close vulnerabilities from remote. This approach however is also problematic, as the update might introduce incompatibilities with running applications or might lead to data leaks harming user privacy [13].

Another group discussed Blockchains and other types of distributed ledgers as foundation for security and privacy solutions. Based upon a distributed ledger, a trustworthy logging mechanisms could for instance be created that store information from autonomous systems (cars, planes, etc.) for post-mortem analyses in a non-mutable and non-modifiable manner. Another application example includes a ledger-based configuration distribution mechanism for systems of any kind, which could bring clear benefits namely accountability and transparency of configuration.

The third group we want to highlight discussed on cloud security. Companies own less physical hardware but lease more and more virtual machines or services in the Cloud. Besides amplifying known problems in traditional fields like security, trust, verifiability, and privacy, the cloudification also brings entirely new questions and problems. One example are services that already utilize virtualization, for example, sandboxes that analyze malware. The nesting of virtualization will decrease performance and change visibility of the malware analyzer to the inspected malware.

Besides highlighted talks and group discussions, security and privacy topics were also represented by following posters "Securebox - A Platform for Securing IoT Networks" [11, 12], posters highlighting ongoing research projects like "Safe-Cloud" [22], "sKnock: Scalable Secure Port Knocking" [25], "AutoMon" [3], and "Towards an Information Model for Decentralized Anomaly Detection for DecADe" [8] and finally "Research Directions in Internet Architecture and Security" [23, 24, 10].

4. EVOLVING THE RETREAT AND LESSONS LEARNED

The last action point on the MIRR agenda is collecting feedback from our participants. In this section we want to summarize most often suggested ideas for improvement, praise, but also critics from the 2nd MIRR.

The most surprising but also most controversially discussed feedback was that some participants would have liked to have the opportunity to prepare for the retreat in advance. Others responded that they would not have time for this. The preparation supporters especially suggested to collect, publish, and refine topics of breakout sessions several days or a few weeks ahead of the actual event. For this purpose, one participant proposed to use mailing lists or more modern online discussion systems. The just described online interaction might even prove beneficial to "break the ice" between participants, who are (quoting another participant) "typically quite shy IT guys who mostly have not met before". Furthermore, a leader of the breakout session shall be elected in advance, who quickly presents the topic to the plenum before the breakout session starts. Hence, participants who had no time to prepare for the retreat can still select the group of their choice group easily. Further ideas were to make introduction slides of participants, abstracts of talks and posters available before the event. This step might prove helpful to cherry pick partners for discussions. In our opinion, an approach that allows participants to prepare for the event but does not leave others behind is sound. Hence we will implement preparation in the upcoming 3rd MIRR.

Both, representatives of academia and industry, stated that the participation of industry was too low. This is true for the number of persons (so far the academia to industry split was about 80% to 20%) as well as for active contributions of representatives of companies, i.e. talks or topics for breakout sessions. Participants suggested that short industry talks that describe problems or open questions could be a good starting

4

point for breakout sessions or provide interesting research ideas to the academia.

The by far most often suggested improvement was to increase the amount of interactive and individual elements in the agenda. Participants liked both poster and breakout sessions with a slight preference towards the breakouts. Some persons even proposed to have two slots for breakout sessions. Participants mostly enjoyed the talks given in the plenum but felt that shorter talks of max. ten minutes would be enough to spark further discussions in smaller groups after the talk. Spending less time for "compulsory" talks might also mitigate a potential weakness of the MIRR format pointed out by a participant: the participant felt that the scope of topics of the retreat was too wide. While we understand the problem, we also see the advantage of getting to know work of other fields of network and Internet research as this can help to break out of ones own "mental filter bubble" and broaden ones overall knowledge. However, the amount of time one spends with (personally experienced) non-relevant content can be decreased when time is shifted from compulsory agenda points to such ones that can be picked by the participant individually. This step is, as we believe, highly important to optimize a participants personal outcomes from and perception of the retreat. Hence, shorter compulsory talks to maximize the amount of individual interaction is another important aim for the upcoming MIRR.

One participant proposed to include talks in tutorial style. While some agreed, other participants pointed out that such talks would again reduce the time available for more interactive action points. This finding led to the proposal of having two parallel tracks for talks.

Further feedback included to increase gender diversity and have changing, random seating arrangements during mealtimes. Even though we think gender diversity is desirable, we also feel that this suggestion is difficult to implement as our quite technical field seems to attract mostly men. Random seating arrangements can help to mixing people but could also backfire when participants feel patronized as the cannot talk to who they want.

5. CONCLUSIONS AND NEXT STEPS

The overall feedback of our participants has shown, that the 2nd Munich Internet Research Retreat that took place at May 23–24, 2017 was quite successful. However, the organizers of the upcoming MIRR will incorporate as much of the feedback of participants as possible to further improve the event. Talks shall be no longer than ten minutes and have the character of lightning talks, i.e. talks about work in progress and open questions instead of polished, already published results. Furthermore, we will prepare agenda and topics of the upcoming MIRR in a more interactive manner before the retreat and include our participants. This step will ensure that all participants will find a suitable breakout session and come preloaded with knowledge.

Most of the presentation material of outlined talks, summaries of breakout sessions, and contact information of presenters are available online [19].

A follow-up retreat will take place in November 2017. Interested readers are encouraged to contact the organizers to learn the exact day, about topics and about the organization. Furthermore we would like to share experiences with organizers of similar events.

6. REFERENCES

[1] 2017-05-30. TUM Science and Study Center Raitenhaslach. Webpage, last visited 2017-05-30. URL: https://www.raitenhaslach.tum.de.

[2] S. Ahsan, V. Bajpai, J. Ott, and J. Schönwälder. Measuring YouTube from Dual-Stacked Hosts. *Passive and Active Measurement Conference (PAM)*, 2015.

[3] AutoMon – Automated Performance Monitoring. http://automon-projekt.de/en.

[4] V. Bajpai and J. Schönwälder. A Survey on Internet Performance Measurement Platforms and Related Standardization Efforts. *IEEE Communications Surveys and Tutorials*:1313–1341, 2015.

[5] V. Bajpai and J. Schönwälder. IPv4 versus IPv6 - who connects faster? *IFIP Networking Conference*, 2015.

[6] V. Bajpai and J. Schönwälder. Measuring the Effects of Happy Eyeballs. *Applied Networking Research Workshop (ANRW)*, pp. 38–44, 2016.

[7] V. Cozzolino, A. Y. Ding, and J. Ott. Fades: fine-grained edge offloading with unikernels. *Proc. ACM SIGCOMM*, 2017.

[8] DecADe – Decentralized Anomaly Detection. https://www.net.in.tum.de/sites/decade/.

[9] S. J. Eravuchira, V. Bajpai, J. Schönwälder, and S. Crawford. Measuring Web Similarity from Dual-stacked Hosts. *Conference on Network and Service Management (CNSM)*, 2016.

[10] 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.

[11] I. Hafeez, A. Y. Ding, L. Suomalainen, S. Hätönen, V. Niemi, and S. Tarkoma. Demo: Cloud-based Security as a Service for Smart IoT Environments. *Workshop on Wireless of the Students, by the Students, & for the Students (S3@MobiCom)*, 2015.

[12] I. Hafeez, A. Y. Ding, L. Suomalainen, A. Kirichenko, and S. Tarkoma. Securebox: Toward Safer and Smarter IoT Networks. *ACM Workshop on Cloud-Assisted Networking (CAN)*, 2016.

[13] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott. Security and privacy in device-to-device (d2d) communication: a review. *IEEE Communications Surveys Tutorials*:1054–1079, 2017.

[14] N. Herold, H. Kinkelin, and G. Carle. Collaborative Incident Handling Based on the Blackboard-Pattern. *ACM Workshop on Information Sharing and Collaborative Security*, pp. 25–34, 2016.

[15] W. Kellerer, A. Basta, and A. Blenk. Using a Flexibility Measure for Network Design Space Analysis of SDN and NFV. *Proc. IEEE Infocom*, pp. 423–428, 2016.

[16] Leibnitz-Zentrum für Informatik Schloss Dagstuhl. Webpage, last visited 2017-05-30. URL: http://www.dagstuhl.de.

[17] Y. Liu, A. Hecker, R. Guerzoni, Z. Despotovic, and S. Beker. On optimal hierarchical SDN. *IEEE International Conference on Communications (ICC)*, 2015.

[18] 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.

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

[20] NetApp, Inc. Webpage, last visited 2017-05-30. URL: http://www.netapp.com/.

[21] C. Prehofer, O. Horst, R. Dodi, A. Geven, G. Kornaros, E. Montanari, and M. Paolino. Towards Trusted Apps platforms for open CPS. *International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC)*, pp. 23–28, Apr. 2016.

[22] SafeCloud. http://www.safecloud-project.eu.

[23] 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.

[24] 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.

[25] D. Sel, S. H. Totakura, and G. Carle. sKnock: Port-Knocking for Masses. *IEEE Symposium on Reliable Distributed Systems Workshops (SRDSW)*, 2016.

[26] B. Trammell, C. Perkins, T. Pauly, and M. Kühlewind. Post Sockets, An Abstract Programming Interface for the Transport Layer. Internet-Draft draft-trammell-post-sockets-00, Oct. 2016.

[27] 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.