Report from Dagstuhl Seminar 13322

The Critical Internet Infrastructure

Edited by

Georg Carle[1], Jochen Schiller[2], Steve Uhlig[3], Walter Willinger[4], and Matthias Wählisch[2]

1 **TU München, DE,** carle@in.tum.de
2 **FU Berlin, DE,** {jochen.schiller,m.waehlisch}@fu-berlin.de
3 **Queen Mary University of London, GB,** steve@eecs.qmul.ac.uk
4 **AT&T Research – Florham Park, US**

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 13322 "The Critical Internet Infrastructure". The scope of the seminar includes three main topics, rethinking perspectives on the Internet backbone, methodologies to analyze the Internet structure, and paradigms overlaying IP connectivity. The results are based on fruitful discussions between people from the research and operational community.

Seminar 04.–09. August, 2013 – www.dagstuhl.de/13322
1998 ACM Subject Classification C.2.1 Network Architecture and Design, C.2.5 Local and Wide Area Network—Internet, C.2.6 Internetworking
Keywords and phrases Internet, Backbone, Internet Services, Critical Infrastructure
Digital Object Identifier 10.4230/DagRep.3.8.27
Edited in cooperation with Thomas C. Schmidt

1 Executive Summary

Georg Carle
Jochen Schiller
Steve Uhlig
Walter Willinger
Thomas C. Schmidt
Matthias Wählisch

The Internet was designed to offer open data transfer services on a planetary scale. However, its success has turned it into a mission-critical infrastructure of vital importance for most countries, businesses, and industries. The aim of this seminar is to bring together the research and network operator communities to discuss and analyze the Internet as a critical infrastructure. We will address the vulnerability of the Internet from a number of different angles (e.g., physical infrastructure, control plane, data plane, services, etc.), with an emphasis on the core transport infrastructure as well as the content delivery side. The seminar will contribute to a better understanding of the Internet as a system of interdependent elements and pursue extensions of current research perspectives to consider novel (and maybe unusual) approaches to studying the local or region-specific substrates as parts of the Internet's global ecosystem.

Rethinking Perspectives on the Internet Backbone

Analyzing the mutual impact between ASes, the vulnerability and efficiency of the backbone requires the identification of ASes and their role in mutual transit. In particular, stakeholders do not want to ground their internal data exchange on weak third parties. In Internet terms, AS interconnections between key players of a country should be part of a transparently visible Internet ecosystem. However, the Internet is a globally distributed network without boundaries, which makes the identification of locally relevant subparts hard. This seminar aims at being a platform to leverage new and uncommon research perspectives that go beyond the Internet backbone as a globally distributed system.

Methodologies to Analyze the Internet Structure

To analyze the Internet as a critical infrastructure, a clear picture is required about the kind and granularity of data needed to obtain relevant results and draw valid conclusions, even if the available dataset is restricted. Sampling and inference are common methods to assess the impact of the limited view on the real Internet. Current approaches to model the Internet backbone need to be revisited to reflect the Internet as critical infrastructure. The mapping of logical Internet nodes (ASes) to concrete entities (companies, points of presence etc.) as well as its annotation with meta data (e.g., administrative contact points) have been identified as important to cover the Internet structure from a non-technical perspective.

Paradigms Overlaying IP Connectivity

Delivering content to the end users is one of the main objectives of the Internet. In the early Internet, end users accessed content directly from a primary source. With the advent of CDNs this has changed. A single CDN operates as replication and distribution network for many content publishers, which brings data closer and more efficiently to end users. In fact, a very large portion of the current Internet content is maintained by only a limited number of CDNs, creating a limited competition in this area. Until now, this oligarchy has not been thoroughly studied, especially in the context of the Internet as a critical infrastructure.

Original Goals of the Seminar

The research questions to be pursued and answered include:

- How can we define and extract a locally relevant view of the globally distributed Internet?
- Which metrics are appropriate to measure the importance of Internet stakeholders and their mutual relationships?
- Which countermeasures and improvements are feasible to protect the Internet as critical infrastructure without narrowing its flexibility and openness?
- To what extent can we analyze the Internet structure in short time frames?
- What is the role of specific ASes for reliably interconnecting the Internet infrastructure of a country?
- How can we reveal weak transits and unintentionally strong dependencies between ASes and specific regions of the world?
- How can we predict Internet scale consequences of large scale problems (what-if-questions)?

The complexity of the Internet makes it equally complex to give complete answers to these questions. This seminar helped us to start *touching* the questions. During our discussions it

was clear that it is not only important to continue the work on these challenges but that it is also worth to follow up with a more specific focus on measurement aspects.

Acknowledgments

The editors of this report would like to thank all participants for very fruitful and open-minded discussions! In particular, we thank the operators for sharing practical insights.

We gratefully acknowledge the Dagstuhl staff for helping on all administrative coordination, for their patience, and most importantly for providing an extremely inspiring environment.

2 Table of Contents

3 Overview of Talks

3.1 The impact of amended copyright acts to broadband traffic in Japan

Kenjiro Cho (Internet Initiative Japan Inc. – Tokyo, Japan)

This talk describes the impact of two copyright acts in Japan, which are effective since January 2010 and October 2012, respectively. The first act implements a download ban, making illegal content download illegal. This had an impact on the long-term traffic trend. The second act criminalized illegal downloads. The impact was only temporary. Our analysis is based on a clean and simple measurement setup.

3.2 Can you ping me now? – or – Measuring Mobile Networks

David Choffnes (Northeastern University – Boston, US)

Joint work of Choffnes, David; Mao, Morley; Zarifis, Kyriakos; Flach, Tobias; Nori, Srikanth; Katz-Bassett, Ethan; Govindan, Ramesh; Welsh, Matt; Hamon, Dominic; Feamster, Nick

Mobile networks are currently the fastest growing, most popular and least understood systems in today?s Internet ecosystem. Despite a need for performance improvement and policy transparency in this space, researchers currently struggle to measure, analyze, and optimize mobile networks.

To address this problem, we propose building Mobilyzer, an open platform for network measurement from mobile devices, to capture a detailed view of this complex and dynamic setting. By measuring mobile network performance directly and intelligently from devices, we will fill a critical gap: visibility from users? perspectives. First, I demonstrate the usefulness of such information by using a large dataset of network measurements from mobile devices to diagnose path inflation experienced by mobile users. Then I describe a mobile-network measurement platform that captures a continuous, broad view of mobile system interactions, annotated with contextual information (e.g., GPS location, signal strength and radio state) necessary to interpret the raw measurements. To facilitate research and foster innovation in this environment, our platform will be open to all researchers, support a flexible set of measurement techniques, it will transparently manage data collection and reporting, and the measurements will be publicly available and easily accessible.

3.3 Toward Realtime Visualization of Garbage

Alberto Dainotti (San Diego Supercomputer Center, US)

Joint work of Alistair, King; Dainotti, Alberto;

CAIDA, the Cooperative Association for Internet Data Analysis, investigates practical and theoretical aspects of the Internet. Using the CAIDA telescope, we monitor backscatter traffic to complement BGP measurements and to analyze country-level outages as well as routing incidents. Getting real-time insights into the gathered data is nearly impossible due to the large amount of volume. In this talk, we report about ongoing work on real-time visualization of very large data sets. We describe our pipeline-based architecture and present a live demo. We conclude with lessons learned and next steps.

3.4 Security and Attacks

Roland Dobbins (Arbor Networks – Singapore, Singapore)

This talk discusses two topics. The first part deals with network core infrastructure protection and best practices. It includes an overview about infrastructure protection aspects, explains the different forwarding planes in routers, and presents for router and network hardening. The second part of this talk identifies wireless Internet traffic trends and challenges including comparisons between wireline and wireless mobile broadband traffic.

3.5 Internet census taken by an illegal botnet. A qualitative analysis of the measurement data

Anja Feldmann (TU Berlin, DE)

This talk gives a qualitative analysis of the Internet census 2012, an anonymous port scanning of the Internet address space using insecure embedded devices. After a brief discussion of who was interested in the data, the talk contrasts claims made by the anonymous writer with the actual data set. The results were not not only unethically collected, but are also based on methodological flaws (e.g., uneven probing rates). The talk concludes that using the data for further studies is nearly impossible as insufficient meta and measurement data is provided.

3.6 Resilience of the Interdomain Routing System

Thomas Haeberlen (ENISA – Athens, GR)

We briefly give some points on what could be done to further improve the resilience of the interdomain routing, and present an approach with a slight change in perspective, which we are currently investigating in a project under ENISA's 2013 work programme

3.7 How I Will Measure Routes in 2014

Ethan Katz-Bassett (USC – Los Angeles, US)

Joint work of Katz-Bassett, Ethan; Calder, Matt; Zarifis, Kyriakos; Feamster, Nick; Cunha, Italo; Choffnes, Dave; Madhyastha, Harsha

In this talk we give a brief overview about past, present, and future work on how we measure routes. We explain the concept of the Transit Portal (or BGPMux) project, which lets researchers experiment with BGP in the wild by emulating an autonomous system. Transit Portal has been used in several analysis, e.g., for root cause analysis of BGP path changes. The second part of this talk deals with a unified platform for path queries. We discuss the need for single interface to access all sets of vantage points such as academic testbeds, enduser measurements, or route collectors.

References

1 E. Katz-Bassett, C. Scott, D. Choffnes, I. Cunha, V. Valancius, N. Feamster, H. Madhyastha, T. Anderson, A. Krishnamurthy. *LIFEGUARD: Practical Repair of Persistent Route Failures*. Proc. of ACM SIGCOMM, 2012

2 U. Javed, I. Cunha, D. Choffnes, E. Katz-Bassett, A. Krishnamurthy, T. Anderson. *PoiRoot: Investigating the Root Cause of Interdomain Path Changes* . Proc. of ACM SIGCOMM, 2013.

3.8 About ENISA. Security and resilience of the European communications networks

Rossella Mattioli (ENISA – Athens, GR)

ENISA, the European Union Agency for Network and Information Security, works on the improvement of network and information security in the European Union. ENISA gives advice on information security issues to national authorities, EU institutions, citizens, and business. It acts as a forum for sharing good NIS practices and facilitates information exchange and collaboration. In this talk, I will present background about ENISA and the NIS landscape. I will discuss the difference between Critical Infrastructure (CI) and Critical Information Infrastructure (CII). I will also consider EU legislation.

3.9 Configuration Complexity

Matthew Roughan (University of Adelaide, AU)

Network complexity is an important topic for network designers. The choice of design often comes down to "simple is better", but we lack metrics that quantify complexity. This talk is about defining complexity, at least for a limited domain – network configuration complexity. We argue that when the problem is decomposed correctly into network and protocol components we can use an analogue of Kolmogorov complexity to quantify how hard it is to define a network configuration, but there are still many unknowns. For instance, how to relate such a metric to the cost of operational tasks.

3.10 Internet PoP Level Maps and Beyond

Yuval Shavitt (Tel Aviv University, IL)

Joint work of Shavitt, Yuval; Zilberman, Noa

A large amount of monitoring and analysis research is devoted to the study of the Internet topology. There are several levels on which the Internet maps are presented, each level of abstraction is suitable for studying different aspects of the network. The most detailed level is the IP or router level, which represents separately each and every entity connected to the network. This level is far too detailed to suit practical purposes, and the large number of entities makes it very hard to handle. The coarsest level is the Autonomous System (AS) level. It is most commonly used to draw Internet maps, as it is relatively small (tens of thousands of ASes) and therefore relatively easy to handle: There is only one node for every AS, and may have only one edge between every pair of ASes. One limitation of using the AS level is that it cannot serve as tool to track the internet evolution, since AS sizes may differ by orders of magnitude. While a large AS can span an entire continent, a small one can serve a small community, yet both seem identical of the AS level map.

An interim level between the AS and the router graphs is the PoP level. Service providers tend to place multiple routers in a single location called a Point of Presence (PoP), which serves a certain area. A PoP is defined as a group of routers which belong to a single AS and are physically located at the same building or campus. Thus, for studying the Internet evolution and for many other tasks, PoP maps give a better level of aggregation than router level maps with minimal loss of information. PoP level graphs provide the ability to examine the size of each AS network by the number of physical co-locations and their connectivity instead of by the number of its routers and IP links. Points of presence can be annotated with geographical location, as well as information about the size of the PoP. Thus, using PoP level graphs it is possible to detect important nodes of the network and understand network dynamics as well as many more applications.

In the talk I present an algorithm for classification of IP addresses into PoPs and then present PoP level maps that are built by connecting the PoP nodes with edges that are aggregation of IP level links. I will then present algorithms for embedding this map in geography, namely assigning a geographic location to points of presence. I will present

analysis of the different algorithm performance, and validation studies against ground truth data.

References

1 Lior Neudorfer, Yuval Shavitt, Noa Zilberman. *Improving AS relationship inference using PoPs*. Proc. of IEEE INFOCOM, IEEE Press, USA, 2013
2 Dima Feldman, Yuval Shavitt, Noa Zilberman. *A structural approach for PoP geo-location*. Computer Networks 56(3): pp. 1029-1040, 2012
3 Yuval Shavitt, Noa Zilberman. *Geographical Internet PoP Level Maps*. Proc. of TMA, Springer-Verlag, pp. 121-124, 2012

3.11 Economics

Bill Woodcock (PCH – San Francisco, US)

This talk discusses economic aspects of the critical Internet infrastructure from a cost perspective. It identifies critical infrastructure costs and how resiliency and defense affect these costs. Furthermore, this talk reflects 'perverse' incentives, zero tolerance vs. risk management, and deterrence versus mitigation versus retribution.

4 Working Groups

4.1 Control Plane Attack

The group identified the following vulnerable parts of the control plane: routing (BGP and IGP), DNS, MPLS, mobile packet control, higher layer control loops (e.g., CDN, VPN), and the so-called metaplane. The metaplane comprises authorized information about a third party, e.g., PKI in general and RPKI in particular for routing.

These parts can be attacked by misconfiguration and hacking. A major challenge are control loop problems as well as cascading failures. The operation of the current Internet is based on a highly complex system with several interacting components. In contrast to previous time where lower layer control loops were visible (e.g., BGP wedgies that lock into undesirable states), today there are much more higher layer control loops. A typical example are Content Delivery Networks (CDNs). ISPs itself do not need to implement traffic engineering because CDNs can very quickly shift traffic to other CDNs or ISPs. Under bad circumstances this may lead to slow oscillations. The group explained a scenario, in which an ISP changes its IGP. This results in large swing in BGP egress decision and thus causes traffic change, which finally will be countered by the CDN. Consequently, there is a significant relocation of traffic for the ISP. The ISP may try to rebalance load by using IGP. The whole process repeats as IGP operations and CDN traffic engineering interact with each other.

The group also illustrated cascading failures. One example is the Baofeng outage in 2009. Boafeng is a popular media player in China. The attack did not target the Boafeng service but the DNS infrastructure of Boafeng's registrar. In combination with a design flaw within the Boafeng client, which continuously started DNS requests, this led to a DNS amplification attack: In the first stage the DNS servers were not available due to the attacker.

In the second stage Boafeng clients started accidentally a DNS flood as they were not able to contact the originally originally DNS servers. These DNS queries flooded the network of China Telecom affecting several hundred millions of users for hours.

Control plane attacks are complicated. Even though an attack does not directly target the control plane, the attack may affect this layer due to many interacting protocols on different layers.

4.2 Government-Level Adversaries

The Internet is a critical infrastructure that should be protected by the government. However, it gives also new potential for misusing by the government to conduct attacks. The group analyzed the differential of power between attacker and defender. A government that attacks an individual will most likely be successful as end users lack sufficient resources. This perspective changes in case of a governmental adversary against a corporation or another government. Larger companies provision much more (Internet-based) resources to some state resources.

In the second part the group discussed how do governmental attacks characteristically differ from non-governmental attacks. The identified three items: (a) Government are more likely to make long-term investments and preparations; (b) governments are more likely to use cyber attacks as a component in a broader IO, which is itself more likely to be a component of a larger coordinated operation; (b) governments are more likely to apply classic espionage tradecraft in combination with cyber techniques.

A prominent example for a governmental adversary is TOR, The Onion Router. TOR was designed as 'circumvention' tool that allows for hiding information. A widespread deployment of TOR scatters data in such a way, which makes decryption costly. This is not only useful for the common public but also helps to cover agents. Unfortunately, Moore's Law gradually democratised TOR. It allows more intelligence services to compete for control, causing the US government to lose interest in TOR and support the development of new competing platforms.

Finally, the transition from certificates to DNS-based Authentication of Named Entities (DANE) has been discussed briefly. The deployment of X.509 PKI gives certificate issuers significant power. This makes certificate authorities very attractive for governmental attacks. DANE (cf., RFC 6698) vastly reduces the number of potential compromisers, but arguably gives governments more direct ability to attack their own citizens and corporations, since governments often control the signing of their country-code domain (ccTLD).

4.3 Disaster Recovery

The group started the discussion based on two talks. The first talk was given by Kenjiro Cho who presented insights from Japan Earthquake with respect to the impact on traffic and routing observed by IIJ, a local ISP. The second talk was given by Randy Bush who presented the DUMBO project, which is about using MANET for disaster management, exemplified on recovering from South-East Asian Tsunamis. The group agreed that the Internet matters after a disaster; e.g., for coordinating emergency responses or the dissemination of food, water, etc. Furthermore, the role of the Internet after a disaster is to provide information. The communication service is not necessarily email, because it needs to reach the broader

public to prevent panic.

The main outcome of the discussion was that the *culture* is surprisingly important in case of disaster recovery. In the example of the Japan Earthquake, IIJ had enough spare capacities to deal with rerouting all network traffic. This high over-provisioning was by intention and is different in other countries.

The DUMBO project illustrated nicely another aspect, the consideration of the local environment. The project partners used elephants to carry equipment in South-East Asia because it is both, culturally appropriate and handy after a disaster.

Bill Woodcock gave an example where not only the cultural of a society but also of organizations need to be considered. After the Haiti earthquake in 2010, ISPs had 90 % of the network up using wireless technology. However, However, NGOs that arrived soon after to help accidentally broke network communication by taking over the wireless spectrum.

4.4 Mapping (Inter-)National Infrastructure

The group discussed the localization of the Internet infrastructure with respect to geographic, political, sociological, or organisational aspects. Perspectives are national (i.e., seen from within countries) or international (i.e., between countries). However, rather unclear is what entities can/shall be mapped, and what can(not) be done on a technical level. The group identified four building blocks of interest:

1. Provisioning of infrastructure.
2. Civil organization and business.
3. Relations to legislature.
4. Aspects of Internet use.

As major problem in order to map the infrastructure, missing public information has been identified. The level of public information depends on the country and regulatory requirements. In Poland, for example, complete maps of cables are publicly available. In contrast to this, in Germany operators are required to provide certain information about location etc. However, this information is treated confidentially.

Another challenge in evaluating the quality of public data is the question of intended purpose while publishing the information, in particular in the business context. Searching the web for public data usually brings more data to light than expected (e.g., on operator websites). But what is the motivation for a company to publish such data? The data maybe highly specific to distract from the actual (desired) insights.

Currently there are no central databases that can provide a complete and correct view on all aspects related to the Internet infrastructure. In fact, we expect that such a view is unlikely to be available soon. There are on-going activities to build new and to refine existing mapping approaches. Evaluating the quality of the solutions depends significantly on the ground truth in the data.

4.5 Non-Adversarial Threats to Availability

During this break-out session the group discussed threats that have not been introduced by an attacker. Several concrete examples have been identified. For example, (and maybe the most important) the lack of power. Many critical data centers etc. are protected by uninterruptible

power supplies. A proper working of those systems requires regular maintenance (e.g., test of generators), which is surprisingly often missed.

Another example is the lack of hardcopy critical documentation and contact information, or failure to train employees to find such, or failure to keep such documentation up-to-date. Accessing this information should not be bound to the correct function of the technical system (e.g., authorization).

A common problem is the misunderstanding of redundancy. The group illustrated this by the following anecdote: Microsoft was buying 150 % of all of the capacity into Seattle, mistakenly thinking they were buying three redundant DS3s of Internet connectivity, at a time when there were only two data DS3s leaving the city. It was also observed that several people believe that they are creating redundancy, while they are actually putting components in serial (increasing fragility) rather than in parallel. Or they put components in parallel, but in such a way that the operation of one is in some subtle way dependent upon the operation of the other, which amounts to the same thing.

The main outcome of this session was that non-adversarial threats are multi-dimensional including technical and non-technical aspects.

4.6 A Unified Interface for Measurements

This group discussed the potential of a unified access to the plethora of existing measurement data sets. The group provided insights from relevant past EU projects and found that involvement of people with long-term stakes in essential, simple approaches are better than complex ones, and differentiation between “small” and “large” data queries is critical.

One important design decision in building the related data infrastructure is the question of a central versus distributed repository. Central repositories need periodic data updates but may support more subtle queries. On the other hand, a distributed repository lowers the barrier for entry and is easier to maintain. On idea was to implement a gradual deployment, i.e., start with a distributed system and migrate to a central system later. As hosting options M-Lab, ISI, and RIPE have been identified.

Participants

- Bernhard Ager
ETH Zürich, CH
- Lothar Braun
TU München, DE
- Randy Bush
Internet Initiative Japan Inc. – Tokyo, JP
- Georg Carle
TU München, DE
- Nikolaos Chatzis
TU Berlin, DE
- Kenjiro Cho
Internet Initiative Japan Inc. – Tokyo, JP
- David Choffnes
Northeastern University – Boston, US
- Alberto Dainotti
San Diego Supercomputer Center, US
- Roland Dobbins
Arbor Networks – Singapore, SG
- Anja Feldmann
TU Berlin, DE
- Timothy G. Griffin
University of Cambridge, GB
- Thomas Häberlen
ENISA – Athens, GR
- Ethan Katz-Bassett
USC – Los Angeles, US
- Stefan Katzenbeisser
TU Darmstadt, DE
- Rossella Mattioli
ENISA – Athens, GR
- Matthew Roughan
University of Adelaide, AU
- Jochen Schiller
FU Berlin, DE
- Johann Schlamp
TU München, DE
- Thomas C. Schmidt
HAW – Hamburg, DE
- Yuval Shavitt
Tel Aviv University, IL
- Georgios Smaragdakis
T-Labs/TU Berlin
- Rade Stanojevic
Telefónica Res. – Barcelona, ES
- Steve Uhlig
Queen Mary University of London, GB
- Matthias Wählisch
FU Berlin, DE
- Walter Willinger
AT&T Labs Research – Florham Park, US
- Bill Woodcock
PCH – San Francisco, US