Report from Dagstuhl Seminar 18242

Secure Routing for the Internet

Edited by

Phillipa Gill[1], Adrian Perrig[2], and Matthias Wählisch[3]

1 **University of Massachusetts – Amherst, US,** `phillipa@cs.umass.edu`
2 **ETH Zürich, CH,** `adrian.perrig@inf.ethz.ch`
3 **FU Berlin, DE,** `m.waehlisch@fu-berlin.de`

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 18242 “Secure Routing for the Internet”, which ran from Monday 11/6 (morning) to Wednesday 13/6 (noon), and employed 27 participants in total (including 3 network operators).

Seminar June 10–13, 2018 – http://www.dagstuhl.de/18242

2012 ACM Subject Classification Computer systems organization → Dependable and fault-tolerant systems and networks, Networks → Network architectures, Networks → Network components, Networks → Network properties, Networks → Network protocols, Networks → Network security, Networks → Network services

Keywords and phrases Anonymity, BGP, BGP Prefix Hijack, Denial of Service, Deployment Incentives, Detection, Monitoring, Network Operations, Privacy, Protocol, Public Key Infrastructure, Routing, Routing Policy, Routing Security, Testbed

Digital Object Identifier 10.4230/DagRep.8.6.40

Edited in cooperation with Vasileios Kotronis

1 Executive Summary

Vasileios Kotronis (FORTH – Heraklion, GR)

The seminar was focused on the following aspects of routing security, mostly in the context of traditional inter-domain routing security: (i) Protocol design vs tooling, (ii) sources of relevant routing data and their accuracy/collection challenges, including policy databases, (iii) the need for metadata and dataset “labelling”, (iv) monitoring and detection of routing attacks and anomalous incidents, such as BGP hijacks and route leaks, incentives for network operators to adopt routing security protocols, (v) testbeds for routing experiments, (vi) hijacks as enabling attacks against ToR and Bitcoin, on the application level, (vii) prevention of routing attacks, (viii) anonymity, privacy and (anti-)censorship. Moreover, we discussed in depth about (ix) PKI and cryptographic verification and protection mechanisms, and their use in securing routing infrastructures, such as the RPKI and BGPsec protocols. Finally, we (x) approached BGP flowspecs, DDoS attacks and QoS in the Internet as separate topics of interest in the field. Another goal of the seminar was to touch upon (xi) future network routing architectures which offer routing security “by design”, especially in light of demanding upcoming applications such as IoT, car-to-car communications, sensor swarms, and wireless routing at scale, and identify related security and privacy concerns and objectives.

Secure Routing for the Internet, *Dagstuhl Reports*, Vol. 8, Issue 06, pp. 40–62
Editors: Phillipa Gill, Adrian Perrig, and Matthias Wählisch
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Besides the specific goals of the seminar, it is also worth noting some interesting aspects of Dagstuhl seminars in general, that played a critical role in fueling the related talks, discussions and reports. In summary, the 3-day seminar in which we participated, focused not solely on the presentation of established results but also on ideas, sketches, and open (research and operations) problems. The pace and program was guided by topics and presentations that evolved through discussions. This report contains an executive summary of the material that was transcribed during the entire seminar.

Overall, some participants of the seminar seem to be more "pessimistic" about routing security. Both the research and operator communities need to consolidate more data sources to facilitate progress. Any deployment progress is only possible if operator incentives are improved, however, it remains an open problem on how to provide strong incentives. In practice, a good technical solution is insufficient without first tackling the "politics". We discussed about routing/network testbeds and the role they can play in emulating and verifying many of the discussed concepts. However, in the wild (or the "real world"), it is surprisingly hard to implement something like RPKI; even more so for BGPsec. We all need a better understanding of the problem space; formal taxonomies of routing attacks, such as hijacks, would be of great help on this front. Regarding improving BGP itself, we have seen many prevention mechanisms, whose deployment is the end-goal for the Internet. However, as we have to live with BGP at least in the intermediate term, we can also explore research on overlay solutions to achieve the properties that we need, at least for the time being. These solutions need to support incremental deployment for obvious reasons.

In general, deployment progress has been slow which is feared not change in the near future. It is reassuring to see that a lot of work is being done in the measurement area; we were also reminded how hard is it to get the ground truth, labelled with useful metadata. Some fundamentally new and secure approaches were discussed, for instance the SCION secure Internet architecture, however, the deployment of new inter-domain routing protocols is very challenging. To improve the deployment incentives of secure routing protocols for operators, the creation of a catalog of routing incidents could be beneficial.

Moreover, it seems that the community may have underestimated the importance of monitoring tools and their utility in the wild. We have learned about new data sets, as well as interesting insights on the Impact of prefix hijacks on the application layer. In general though, we were hoping to see more enthusiasm for new solutions.

Finally, it is worth noting that having a mixed group of researchers and operators is very important to exchange information and discuss potential approaches, which made the seminar an interesting and worthwhile experience.

2 Table of Contents

Executive Summary

Overview of Talks

Working groups

Panel discussions

3 Overview of Talks

3.1 PEERING: An AS for Us

Ítalo Cunha (Federal University of Minas Gerais-Belo Horizonte, BR)

Joint work of Brandon Schlinker, Kyriakos Zarifis, Ítalo S. Cunha, Nick Feamster, Ethan Katz-Bassett
Main reference Brandon Schlinker, Kyriakos Zarifis, Ítalo S. Cunha, Nick Feamster, Ethan Katz-Bassett: "PEERING: An AS for Us", in Proc. of the 13th ACM Workshop on Hot Topics in Networks, HotNets-XIII, Los Angeles, CA, USA, October 27-28, 2014, pp. 18:1–18:7, ACM, 2014.
URL https://doi.org/10.1145/2670518.2673887

Internet routing suffers from persistent and transient failures, circuitous routes, oscillations, and prefix hijacks. A major impediment to progress is the lack of ways to conduct impactful inter-domain research. Most research is based either on passive observation of existing routes, keeping researchers from assessing how the Internet will respond to route or policy changes; or simulations, which are restricted by limitations in our understanding of topology and policy. We propose a new class of inter-domain research: researchers can instantiate an AS of their choice, including its intra-domain topology and inter-domain interconnectivity, and connect it with the "live" Internet to exchange routes and traffic with real inter-domain neighbors. Instead of being observers of the Internet ecosystem, researchers become members. Towards this end, we present the Peering testbed. In its nascent stage, the testbed has proven extremely useful, resulting in a series of studies that were nearly impossible for researchers to conduct in the past. In this paper, we present a vision of what the testbed can provide. We sketch how to extend the testbed to enable future innovation, taking advantage of the rise of IXPs to expand our testbed.

3.2 ARTEMIS: Neutralizing BGP Hijacking within a Minute

Vasileios Kotronis (FORTH – Heraklion, GR)

Joint work of Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas A. Dimitropoulos, Danilo Cicalese, Alistair King, Alberto Dainotti
Main reference Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas A. Dimitropoulos, Danilo Cicalese, Alistair King, Alberto Dainotti: "ARTEMIS: Neutralizing BGP Hijacking within a Minute", CoRR, Vol. abs/1801.01085, 2018.
URL https://arxiv.org/abs/1801.01085

ARTEMIS (Automatic and Real-Time dEtection and MItigation System), is a research effort between the INSPIRE group, FORTH, Greece (www.inspire.edu.gr) and the Center for Applied Internet Data Analysis (CAIDA), University of California San Diego, USA (www.caida.org). ARTEMIS is a defense approach versus BGP prefix hijacking attacks (a) based on accurate and fast detection operated by the AS itself, leveraging the pervasiveness of publicly available BGP monitoring services and their recent shift towards real-time streaming, thus (b) enabling flexible and fast mitigation of hijacking events. Compared to existing approaches/tools, ARTEMIS combines characteristics desirable to network operators such as comprehensiveness, accuracy, speed, privacy, and flexibility. With the ARTEMIS approach, prefix hijacking can be neutralized within a minute.

3.3 Next-Generation Public-Key Infrastructures

Adrian Perrig (ETH Zürich, CH)

Joint work of all seminar participants

Public-key infrastructures form the core of authentication systems that are in use in today's Internet. Unfortunately, the inadequacies of the design of currently used PKIs are emerging with the constant evolution of the Internet and its uses.

In this talk, we discuss the different types of PKIs that are needed to secure Internet communication, and show how we can design next-generation PKIs to achieve better scalability, security, trust agility, and usability.

In particular, we address the following challenges. How can we design a highly available PKI system to support a routing infrastructure? Can we design a PKI that allows to control/limit the power of authorities (e.g., no kill switch possibilities)? How can we securely, scalably, and efficiently update compromised root keys? What considerations do we have for the design a DNS PKI? Should we base the TLS PKI on the DNS PKI as proposed in DANE? Or should we design a TLS PKI that is independent of a secure DNS system? What are the human aspects of running a PKI of an ISP?

In terms of "kill-switches" [1], nation-state adversaries could potentially "turn off" communication for entire regions; could their power be limited through the user of isolation domains? Another major challenge in PKI is key management and tooling (hosted vs non-hosted model, management of private keys, BBN, key revocation). Monitoring is of paramount importance; heuristics used for tracking suspicious information/changes and for taking action are still open research questions. Open-source libraries to ease developer's processes for secure applications should also be considered and developed. Distributed ledgers (e.g., blockchain) cannot currently serve as a solution, due to the critical cyclic effect of communication between the participating nodes (routing – routing verification dependency).

References

1 Cooper, Danny, et al. "On the risk of misbehaving RPKI authorities." Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks. ACM, 2013.

3.4 SCIONLab: A Next-Generation Internet Architecture Testbed you can use Today

Adrian Perrig (ETH Zürich, CH)

Joint work of Adrian Perrig, Pawel Szalachowski, Raphael M. Reischuk, Laurent Chuat
Main reference Adrian Perrig, Pawel Szalachowski, Raphael M. Reischuk, Laurent Chuat: "SCION: A Secure Internet Architecture", Springer, 2017.
URL http://dx.doi.org/10.1007/978-3-319-67080-5

The Internet has not been designed for high availability in the face of malicious actions by adversaries. Recent patches improving security and availability are constrained by the current Internet architecture, business, and legal aspects.

To address these issues, we propose SCION [1], a next-generation Internet architecture that is secure, available, offers privacy, and considers economic and policy issues at the design stage.

We have implemented SCION and deployed it worldwide as a global testbed called SCIONLab, which consists of more than 20 collaborators including research institutions, companies and ISPs. With SCIONLab, researchers can explore today the desirable properties that a next-generation secure Internet architecture can provide.

References

1 Perrig, Adrian, et al. SCION: a secure Internet architecture. Springer International Publishing, 2017.

3.5 Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

Laurent Vanbever (ETH Zürich, CH)

We study the impact that Internet routing attacks (such as BGP hijacks) and malicious Internet Service Providers (ISP) can have on the Bitcoin cryptocurrency. Because of the extreme efficiency of Internet routing attacks and the centralization of the Bitcoin network in few networks worldwide, we show that the following two attacks are practically possible today:

- Partition attack: Any ISP can partition the Bitcoin network by hijacking few IP prefixes.
- Delay attack: Any ISP carrying traffic from and/or to a Bitcoin node can delay its block propagation by 20 minutes while staying completely under the radar.

The potential damage to Bitcoin is worrying. Among others, these attacks could reduce miner's revenue and render the network much more susceptible to double spending. These attacks could also prevent merchants, exchanges and other large entities that hold bitcoins from performing transactions.

References

1 H Maria Apostolaki, Aviv Zohar, Laurent Vanbever, *Hijacking Bitcoin: Routing Attacks on Cryptocurrencies* IEEE Symposium on Security and Privacy 2017. San Jose, CA , USA (May 2017).

3.6 Hijacks: myth or reality?

Pierre-Antoine Vervier (Symantec Research Labs – Sophia Antipolis, FR) and Marc C. Dacier (EURECOM – Sophia Antipolis, FR)

Some recent research presented evidence of blocks of IP addresses being stolen by BGP hijacks to launch spam campaigns. This was the first time BGP hijacking was seen in the wild. Since then, only a very few anecdotal cases have been reported as if hackers were not interested in running these attacks. However, it is a common belief among network operators and ISPs that these attacks could be taking place but, so far, no one produced evidence to back up that claim.

In this talk, we report on the analysis of 4 years of data collected by an infrastructure specifically designed to answer that question: are intentional stealthy BGP hijacks routinely taking place in the Internet. The identification of what we believe of more than 5,000 malicious hijacks leads to a positive answer. The lack of ground truth is, of course, a problem. We managed to get confirmation of some of our findings, thanks to an ISP unwittingly involved.

The talk aims of being an eye-opener for the community by shedding some light on this undocumented threat. Depending on BGP attacks that are carried out, they can be very disruptive for the whole Internet and should be looked at very carefully.

3.7 An RPKI Primer

Matthias Wählisch (FU Berlin, DE)

A fundamental part for securing BGP is the Resource Public Key Infrastructure (RPKI), which consists of a distributed public key infrastructure responsible for Internet resources, i.e., AS numbers and IP prefixes. An RPKI repository stores certificates and Route Origin Authorization (ROAs) objects. A ROA provides a secure binding between one or multiple IP prefixes and an AS that is allowed to originate that prefix.

Using ROA data, an RPKI-enabled router is able to verify the BGP updates it receives. The prefix information within the BGP update might be valid (i.e., the origin AS is allowed to announce this prefix), invalid (i.e., the origin AS is incorrect or the announced prefix is too specific), or not found (i.e., the announced prefix is not covered by the RPKI). Rejecting an invalid route helps to successfully suppress an incorrectly announced prefix, which finally secures network layer reachability of services assigned with an IP address of this prefix.

In this talk, we will give a brief overview about the design, implementation, and deployment of the RPKI.

4 Working groups

4.1 Anonymity

Nikita Borisov (University of Illinois – Urbana Champaign, US)

Joint work of anonymity breakout group participants

We first investigated the relationship between censorship and hijacking. For example, we ask the following questions:

- Could BGP hijacking be used for anti-censorship?
- In case hijacking is actually used for censorship (e.g., China Telecom case, Pakistan/Youtube hijack), then how could we do an associated analysis of the event? Could it be circumvented, e.g., via deaggregation? Moreover, it would be useful to have mechanisms to detect when hijacks leak out and prevent collateral damage.

Moreover, we discussed how one could prevent on-path and hijack attacks on ToR, by considering the following possibilities:

- Investigate strategic placement of ToR nodes, e.g., close to destinations to prevent destination-based attacks.
- Use feeds of information on BGP changes, by e.g., "subscribing" to the hijack alert feed of one or multiple hijack detection systems.
- Take into account that unlike everyday routing, a false-positive in ToR is far less costly.
- Investigate different optimal placement/interconnection strategies for different Internet applications (ToR, BTC, email, etc.).

As a thought experiment, we consider the requirements of a secure routing protocol in the context of ToR. Impossibility of performing hijacks is good, but maybe a weaker requirement would be more than enough for ToR, such as limited hijacking capability. Moreover, the protocol/mechanism should ideally provide the capability of notifications of potential hijacking events, as well as potential control and transparency of end-to-end paths. However, all this seems to run counter to ISP culture of "secrecy".

We further identify the following benefits that RPKI would bring for protecting ToR against hijacks:

- The attacker would need to hijack potentially longer paths to complete a successful attack.
- The attacker cannot announce more specifics if ROA limits the maximum prefix length, thus preventing many sub-prefix hijacks.
- When combined with BGPsec, the authenticity of the control plane would lead to much better robustness of the routing infrastructure.

However, the data plane (on which e.g., ToR packets flow) could still differ for malicious or benign reasons. We need to investigate the frequency with which inconsistent setups occur in the wild.

Finally, we ask whether there are benefits of partial deployment of routing security protocols. For example, we could locate relays which are hosted in networks covered by ROAs and matching valid announcements. We could also prefer paths to/via relays that have BGPsec validation. However, how much deployment is eventually useful? This remains an open question.

4.2 Operations of (R)PKI

Georg Carle (TU München, DE)

Joint work of operations of (R)PKI breakout group participants

The goal we target is to design a PKI system with high availability in the presence of human errors. For this we need formal verification of PKI (including actions done by human entities). However, a formal model would also possess certain limitations; for example, the perceived (by humans) system state might differ from the actual system state. Moreover, some artifacts may be missing, while others may be incorrect. Focusing on the requirement of formally specifying and verifying RPKI, we ask the following question: "Which are the right consistency models for (R)PKI?"

While trying to answer that question, operational aspects of RPKI may be the most difficult aspect to account for. For example, during its early operation stages, blackouts from the main databases occurred, but problems were not sufficiently analyzed. Regarding the structuring of operation, we note that one part is comparable to operation of a X.509-based PKI, while another part is routing-specific. Finally, there is the issue of management of private keys on routers, which could be dealt with e.g., HSM, Intel SGX, ASM trustzone, etc. This is critical: what would happen if an adversary who compromised the router accesses the private key?

In order to formally assess RPKI, one cat take a leaf out of the web security book. For example, the following work looks at the actual deployment of HTTPS, also assessing deployment effort and availability risks, which are critical metrics also for (R)PKI [1].

References

[1] Amann, Johanna, et al. "Mission accomplished?: HTTPS security after DigiNotar." Proceedings of the 2017 Internet Measurement Conference. ACM, 2017.

4.3 Hijack Detection

Ítalo Cunha (Federal University of Minas Gerais-Belo Horizonte, BR)

Joint work of hijack detection breakout group participants

We focused on the detection of BGP prefix hijacks. First, we classify them as follows:

- Malicious vs. accidental. A catalog could be useful for tagging accidental hijacks. An open question is: do these events differ w.r.t. their signature on the control/data plane? Knowledge of policies might be useful to identify the type of hijack.
- Prefix manipulation. This can be further divided into the following categories, depending on the kind of prefix advertised fraudulently:
  - Squatting, i.e., advertisement of unused prefixes that are not owned by the attacker AS.
  - Same-granularity (exact prefix).
  - More specifics (sub-prefix).
- Manipulation of the `AS-PATH` attribute. This can be divided into the following categories, depending on the rightmost location of a fake AS being present on the path:
  - Type-0 (fake origin)
  - Type-1 (fake first hop)
  - Type-2, ..., Type-N (fake N-hop)
  - Type-U (no path manipulation)
- How the packets are handled on the data plane. An attacker could drop (blackholing) or detour packets (man-in-the-middle), or terminate connections and use legitimate IPs to perform impersonation attacks.

An example of such a detection system is ARTEMIS, which for example detects (among others) AS-adjacencies that do not make sense, using previous AS-path information, link information, ground truth and other real-time or offline data sources.

Coming back to the basics, we ask the critical question of who wants to detect hijacks. We identify the following entities:

- The owner of the prefix. He/she requires visibility of all the routes towards their prefix. However, stealthy man-in-the-middle detours are hard to detect, even for owners.
- Third-parties. They are accompanied with a lot of ambiguity. For example, BGP "opimizers" may change routes without notice; on the control-plane, they might look very similar to hijacks.

Moreover, the power of the hijackers themselves depends on different factors, such as (i) the number of peers/customers, (ii) the provider cone, (iii) the respective locations and connectivity of the target/victim and attacker networks, as well as (iv) the stealthiness of the hijacker, e.g., in case of man-in-the-middle attacks. Note also that for example, shorter paths are generally harder to hijack, since they are more preferred by networks.

We further identified useful data sources for hijack detection:

- BGP itself (prefixes, AS-paths, topology). This can also be used to estimate AS sizes (e.g., depending on their connectivity and number of prefixes they advertise), as well as the most known/used peering links.
- BGP communities. However, these might get mangled, while knowledge about policies might be required to understand and properly use communities.
- Routing policies. They are private and quite dynamic.
- Data plane measurements (e.g., latency, bandwidth, traceroutes). They could be triggered via control-plane signaling, in order to detect more stealthy attacks. While they are very sensitive to factors not related to actual attacks (e.g., congestion), there is a lot of historical information available; moreover, they could possibly be very useful to the prefix owner, who knows the data-plane behavior of his/her own network.

Finally, we identified some open issues pertaining to hijack detection:

- The BGPv4 RFC does not mandate the following: if AS1 and AS2 neighbors, then a route to a prefix advertised by AS1 to AS2, is valid even if AS1 is not present on-path. Checking that one has received a route from its peer, and that the peer is present as the last-hop AS on the associated path, is not mandatory leading to all kinds of possible attacks.
- BGP optimizers monitor communications (and their quality) on critical paths, and "play" with BGP advertisements and traffic exit points in case, e.g., the latency increases. This is an attempt to avoid congestion events. However, such advertisements should be flagged by their originator to avoid false positives; for example consider the case where a customer has a private peering (with private ASNs) with its providers, and "optimized" advertisements leak to the outside world.
- It is quite hard to filter prefixes at the border of the Internet (i.e., close to the stubs), despite the availability of guides and best filtering practices, such as BCP38. In general, there are no incentives for operators to do this aggressively; they filter only what their customers tell them. Closer to the core of the Internet, performing filtering for transit is technically infeasible.

4.4 Policy Databases

Ítalo Cunha (Federal University of Minas Gerais-Belo Horizonte, BR)

The state of the art w.r.t. routing policy databases consists of Internet Routing Registries (IRRs) and the Routing Policy Specification Language (RPSL). Route objects within IRRs have some kind of authorization, but there is no information about the length of the IP prefix; some providers do not add more specifics to the DB. However, maximum length, e.g., in RPKI is required. It is worth noting that ISPs such as AT&T and Level3 have and maintain their own databases. AS-SET/RS-SET objects lack authorization function ("no man's land"). Moreover, there is no support for all possible real-world policies.

In terms of route authorization, since RPSL databases are not suitable for this task, RPKI could be employed. The generated route objects could then be safely inserted to an RPSL DB; essentially using RPKI for bootstraping RPSL authorization. Mechanisms on securing RPSL objects with RPKI signatures can be found at RFC7909.

Other ideas to make progress in this regard are the following:

- Track route propagation authorization.
- Make documentation and authorization workable processes for operations.
- Prefer operational relevance over provisioning of data for research.
- Use BGP monitoring tools to check alarms (e.g., about policy violations, route leaks).
- Identify and model what operators need to have in the DB, subject to RPSL limitations.

Moreover, we should note that tooling is necessary, but current tools have their own limitations. E.g., the `IRRtool` that came out with RPSL is not accompanied by useful documentation, while `rtconfig`, which is useful for generating configurations for major routers, might be tricky to apply in the wild. In general, there is no tool that is commonly agreed upon by the community. Moreover, continuous learning and formation of incentives is critical; operations, as a set of processes itself, is not rocker science.

4.5 Data Accuracy Breakout Group

Victoria Manfredi (Wesleyan University – Middletown, US)

The focus of the breakout group was put on traceroute, and in particular on its following aspects:

- How can we collect the needed Internet path data (active traceroute, using network monitoring points such as RIPE Atlas probes, information in databases, etc.)?
- Is traceroute accurate? Does data (i.e., actual user traffic) follow the same route that traceroute uses?
- How can we infer non-responding intermediate hops?
- Application of Paris traceroute in combination with sampling to infer TE changes.
- Limitations of traceroute, and relevant open questions:

  - Showing only a single route per run. How can we access information on alternate (e.g., backup) routes?
  - One way is to sample from multiple sources to the same destination. However, which paths should we sample? Could architectures like SCION be of help to specify what paths we want to use for sampling?
  - What is the utility of information about multiple routes withing an AS, and from an AS to other ASes? Can other ASes leverage this information in some way, even if it is not available in BGP? What is the utility of this for research?
  - If one makes statistical assumptions about actual network topology, combined with traceroute information, can the accuracy gap be evaluated, e.g., in terms of variance? How can this be done? One idea in this context is to combine this process with timing information (to improve accuracy) and network tomography mechanisms (to infer connectivity from timing measurements).
  - There are differences depending on whether you're an sampling end-user or on-path (AS) sources. What if we combine samples from both sources? W.r.t. the end-user, one samples close to the "edge"; on-path ASes would probably sample on their border gateway routers. What if no cooperation between different ASes exists though? Would this sampling be of use? Moreover, the ASes themlselves can make routing decisions that implement the decisions of others, causing different routes to be used (and thus sampled).
- Meta-sampling:
  - Accuracy of information.
  - Completeness of information. For example, are all feasible routes required to be known?
  - Per-route costs.
  - Can this information be aggregated?
  - Relationships between ASes (a "social" graph of ASes). Is this level of sampling abstract enough? If yes, how can this information be leveraged for bootstrapping?
  - Relationship of sampling to link bandwidth. For example, a low-bandwidth edge may be harder to sample, but maybe it is less important anyway.
- How dynamic is the collected information (route, BGP advertisement, connectivity)? Depending on the dynamics and importance of the available information, one can choose to use it for different reasons: e.g., an ISP to detect a live attack, or an academic user to verify information.
- Information in databases:
  - Can it be automatically verified?
  - What are the most prevalent reasons for inaccuracies? Examples include: out-of-date information, information hiding, human error or malicious intent.
  - Can one bootstrap queries from trusted data, to prove or disprove untrusted data?
  - An important motivation for keeping accurate information in the database, is that it helps detect different kinds of attacks, such as BGP hijacks.

Potentially useful related work in the context of this working group includes network discovery mechanisms from ad hoc networks, such as from non-cooperating nodes, as well as sampling of large graphs, such as the Facebook social network.

4.6 Routing Security Incentives

Adrian Perrig (ETH Zürich, CH)

Joint work of routing security incentives breakout group participants

First of all, there are incentives both for "good" and "bad" guys. The joint use of RPKI and BGPsec to ensure some kind of routing security is probably not going to happen any time soon; it is too expensive and a partial deployment would be completely useless. Even RPKI alone, as long as its deployment is not complete, is not very useful/impactful.

A trade-off solution would be to create communities of ISPs and other organizations deploying, for instance, RPKI. If the whole community deploys RPKI than they're in a position to enforce it (e.g., drop traffic violating ROAs). Ecuador is a particular example case where all ISPs are connected to a single IXP; the IXP enforces participating ISPs to use RPKI.

Another idea is to deploy routing security protocols in a large (e.g., research) sub-network like Internet2, where one can also apply and enforce policies they wouldn't be able to apply on the whole Internet (e.g., deploy RPKI, BGPsec).

It is important to encourage people to certify their prefixes, by taking advantages of large network operator meetings such as IETF and NANOG. To achieve that, one needs to educate people to convince them that this process useful and important and make it easy for ISPs to certify prefixes and create ROAs (for example, by using a nice and usable portal). Ease of deployment and maintenance is of paramount importance. Moreover, note that there is a big difference in adoption between EU and US, as the influence from government interest, research funding, customer requirements/procurement are different. A critical challenge is that, unlike RPKI, partial/incremental deployment of BGPsec would not bring any added value; rorcing adoption of RPKI/BGPsec requires that partial/incremental adoption will create incremental added value to the organization doing it.

Other potential incentives for ISPs to deploy routing security protocols are the following:

- Defense against attacks targeting their reputation or aiming at decreasing their income (inducing loss).
- Non-deployment would decrease the revenue of the non-deployer.
- Attacks could be turned into revenue-affecting events by getting attention on the victim (e.g., Youtube hijack)
- In the past, high-profile attacks lead to big leaps forward in security.

A "sad" conclusion is that ISPs and Internet organizations in general will always be more prone to doing detection rather than prevention. However, detection will never provide a perfect protection. In theory, RPKI+BGPsec should supposedly avoid high FP (False Positives) rates coming with detection techniques.

Next, we are looking at incentives for bad guys to abuse the routing infrastructure. The vulnerability of the infrastructure has been known for years, so how is this abuse not more common today? A potential response is that maybe there are much more hijacks than we observe/hear about. A lot of networks could be hijacked and don't want to disclose it. In the early 2000's, around 1/week, 2/month hijacks would be reported (Cisco), in parallel with the telephony network that also suffered from hijacks. Moreover, w.r.t. DDoS attacks, is it cheaper/easier for cybercriminals to just rely on booter services rather than entering the BGP hijack game. However, in the context of man-in-the-middle attacks, BGP hijacks would be a big enabler, for instance, to perform delay attacks.

It is also worth noting that even “bad guys” need the Internet to work to run their business. That being said, all techniques to perform targeted BGP hijacks are well known and can be used by them. An automated BGP hijacking tool, similar to booter services for DDoS attacks, could provide cybercriminals enough incentives to start leveraging that kind of attacks.

As a conclusion, we may not yet be at a stage where BGP hijacking is easy enough to see a lot of bad guys do it at scale.

4.7 Metadata

Pierre-Antoine Vervier (Symantec Research Labs – Sophia Antipolis, FR)

Joint work of metadata breakout group participants

We first discussed some examples of what metadata might be needed; for example, information on peering routers as well as the routing policies of the monitors would be useful metadata to annotate RouteViews datasets.

The most profound questions related to metadata are the following:

- Who needs metadata?
- For what purpose are metadata required?
- Depending on the data user, do the metadata requirements differ?
- Who is going to collect the metadata?

As a use case, we dig in example datasets and see what metadata could improve them. An example would be the labeling of data from bgpstream.com with information from network operators, as follows:

```
[AS1, AS2, AS3, Prefix1] : hijack by AS2 against Prefix1, or:
[AS4, AS5, AS6, Prefix2] : route leak from AS5 which acted as upstream of AS6.
```

However, this generates some challenges:

- What would be the incentives for operators to do that? Note that labeling large datasets requires joint effort from a lot of people.
- One motivation is to improve the quality of the feed by providing it with feedback about the incidents. However, ISPs are often reluctant to confessing they made a mistake.
- On the other hand, the victim itself might be ready to stand up; in the end, this approach could be turned into a reputation system.

We proceed with another example dataset which would benefit from metadata: jupyter notebooks, for which we envision the following uses:

- Publish along with research papers to encourage other researchers to reproduce their experiments.
- This would encourage researchers to be more transparent w.r.t. their work.
- This would also deal with the issue of reproducibility; reproducibility is often hindered by the unavailability of datasets, which are not necessarily open.
- This would require the whole data and code to be packaged together. Frameworks, such as BGPstream from CAIDA, could make this reproducibility easier by providing a uniform access to data.

Another example of useful metadata is the inter-AS business relationship dataset inferred from inter-AS links. While an initial, large-scale effort is done by CAIDA, such datasets are often kept private to avoid disclosing business relationships. The consequence is that everyone kind of redoes this mapping with their own approach; there is no incentive from ISPs' perspectives to make this information pubic as metadata. The same applies in general to network policies.

An interesting question is whether labeling e.g., BGP routing announcements would facilitate/enable using clustering/ML techniques to detect abnormal events (route leaks, policy violations, BGP hijacks, etc.). We are not so certain about the answer. The core problems are feature engineering and labeling. We need a ground truth. We also need to factor in the fact that attackers will try to fool the system, simply by changing their behavior. Results should also be finally explainable.

Moreover, we should also investigate how we should annotate data so as to maximize the added value of the metadata to improve the detection/information learned from the labeled data. Another way to look at the metadata problem is to try to label events by learning the processes/practices used by network operators that lead to the observed events (instead of trying to have the network operators label the data themselves).

On the hijack detection front, additional metadata can be collected and added to the raw data by using the output from:

- Hijack detection systems (e.g., presence of SSL/TLS-enabled server, the output from ARTEMIS, the output from bgpstream.com, etc.).
- IP-based reputation (spam senders, hosting malicious websites, etc).
- AS-based reputation (see circl.lu)

However, we need to find if there are other datasets different than "hijack candidates/abnormal events" that could benefit from metadata (e.g., data-plane data, IRR).

An interesting research direction is to investigate how testbeds (e.g., PEERING) could be used to enrich current routing-related datasets. For example, they could be used for testing how malicious announcements are propagated, and test patterns w.r.t. different attack/anomaly categories/classes. However, the value of these data might be limited due to inherent testbed limitations; for example, one can only hijack his/her own prefixes.

A suitable partner to initiate the routing data labeling would be Internet2 and/or Geant, which would probably be more open to help research. However, we ask how to aggregate metadata obtained from data enrichment/labeling, assuming that this effort turns large-scale.

Finally, an approach of automatically generating metadata in case of need, is performing active measurements in case an anomaly is detected. One example of this approach is setting up a TLS connection to an https enabled web server located in a prefix that may be subject to a hijack [1].

References

[1] Schlamp, Johann, et al. "Investigating the nature of routing anomalies: Closing in on subprefix hijacking attacks." International Workshop on Traffic Monitoring and Analysis. Springer, Cham, 2015.

5 Panel discussions

5.1 BGP Flowspecs

Vasileios Kotronis (FORTH – Heraklion, GR)

Joint work of all seminar participants

We started a discussion on BGP Flowspecs, a a trigger of a more general discussion on inter-domain routing security. BGP Flowspecs can be used to provide instructions on traffic redirection/blackholing, as long as it matches certain attribute filters. What would happen if Flowspecs start crossing domain borders, used between ASes for exchange of routing and traffic management instructions (i.e., blackholing/redirection/polishing, on a flow level)? This would potentially open new security holes enabling traffic manipulation, based on the exposure of network control to external entities. This can probably be done also today, but it is much harder. In general, there is no notion of accountability/verification/authorization w.r.t. BGP Flowspecs; some knobs allow to accept but not apply them, defeating their own purpose.

The main issue with such proposals, is that we are trying to overload BGP with all kinds of functionality, while "bolting" security on top. BGP Flowspecs are not an exception; we need to take a long hard look at new vulnerabilities of such proposals.

Moreover, we should also reconsider the BGP"trust" model. In inter-domain routing, "trust" stems from business relationships, at least currently. However, this model is currently disputed. In principle no e.g., BGP updates are/should be trusted without a proper infrastructure in place; however, we do not have a practical way to verify the information that the protocol provides. This is not the same as stating that "we assume trust between the domains"; we simply do not have a better alternative to remain inter-operable with the rest of the Internet. Therefore, current routing is essentially a compromise between mutually distrusting domains. Network operators cannot extend their non-transitive "fragile" trust towards even more BGP features.

BGPsec might help to restore some trust, making sure that at least the received BGP update includes an untampered, trusted path. However, it is not useful in the event of partial deployment; it is an open issue how we can achieve total deployment.

5.2 Data Sources

Vasileios Kotronis (FORTH – Heraklion, GR)

Joint work of all seminar participants

5.2.1 Existing Control-plane Data Sources

We discussed the following *existing* control-plane (CP) data sources for BGP and inter-domain routing.

- RouteViews [1], RIPE [2], PCH [3]. BGPStream [4] from CAIDA can be used as a software framework and API for accessing the feed of BGP route monitors.

- Looking Glasses. A unified interface (such as Periscope from CAIDA) can be used to access these Looking Glass servers.
- RPKI databases. Can be accessed with mechanisms such as RPKI MIRO [6].
- IRR (RSPL databases [7])
  - Documentation of routing policies.
  - Routing data from the entire global registry may be obtained by entering 'whois' commands such as:

    ```
    whois -h whois.radb.net <network_IP>
    ```

    or:

    ```
    whois -h whois.radb.net AS<Autonomous_System_Number>
    ```
  - One can obtain extensive IRR data through FTP [9] or access it indirectly through the use of free user resources.
  - A list of routing registries can be found at [10].
- BGPmon [8]. Detection of BGP hijacks, route leaks and Internet outages.
- CAIDA AS-level topologies [11].
- PeeringDB [12].
- BMP:
  - Protocol to share control-plane data.
  - In contrast to route monitors, one can acquire data before best path selection takes place.
  - Will be soon supported by BGPstream.
  - Supported in OpenBMP [13]; mostly for "local" ("my AS") analysis.
- Mapping of ASN to names:
  - http://stat.ripe.net
  - http://as-rank.caida.org/
  - http://www.cidr-report.org/as2.0/autnums.html
  - http://bgp.he.net/irr/as-set/AS-RR-Res
  - http://irrexplorer.nlnog.net/search/AS-RR-Res
- Mapping of IP to ASN:
  - CAIDA's pfx2as [15].
  - Team Cymru [14].

5.2.2 Existing Data-plane Data Sources

We discussed the following *existing* data-plane (DP) data sources for BGP and inter-domain routing.

- RIPE Atlas [16].
- PlanetLab [17].
- Ark [18].

5.2.3 Ideal Data Sources

We discussed the following *ideal* CP and DP data sources for BGP and inter-domain routing.

- BMP feed from all existing BGP vantage points and route collectors.
- More vantage points.
- Better metadata; for example, the peering policy of the vantage point AS.

- Labelled data about hijacks versus misconfiguration. Ideally, we would also like to have information about policy violations. In practice, we would like to start with ground truth on BGP hijacks and DDoS attacks. Of course, an open challenge here is how we verify the ground truth, as well as keeping track of who owns the data.
- Mechanism to more easily query the RIPE database. For example, "give me traces that go through AMS-IX". A related work is the one on practical Internet route oracles [19].
- IP-to-AS path mapping. Useful works are `MAP-IT` [20], `bdrmap` [21] and the work of Kai *et al.* [22]. The work of Nomikos et al. can further detect IXP crossings in traceroutes [23].
- Catalog of BGP communities (both for public and non-public ones). A useful database can be found at [24].
- Log of curious observations that people can label. One can simplify this process by applying clustering techniques. An important challenge here is crowd sourcing, i.e., making operators aware of such mechanisms and need for data.
- Information from companies doing BGP "tricks" (e.g., DDoS mitigation, BGP "optimizers").
- Reliable sibling AS detection.
- Dealing with ASes that cannot be modelled as a single router [25].

5.2.4 Data Collection Challenges

We identified the following challenges related to the collection of data related to BGP and inter-domain routing.

- Accuracy.
- Where to find relevant data?
- Authentication/authorization. What should the policies for inserting data be?
- Incentives:
  - Collect data, which provide benefit to others, accompanied by clearly described metadata.
  - Keep the provided data accurate.
  - How to validate? What needs to be known?
  - Incentives needed both for collectors and consumers of data, such as operators and academics/researchers.
- Regional differences between RIPE and other regions. Amongst other reasons, these are due to different data quality.
- Some of the IRR issues are documented in rfc7682.
- Queriability of traceroute data/VPs (e.g., RIPE Atlas, paths via AS/IXP).
- Data availability over time
- IP-to-AS path conversion
- Coverage of collectors. Need increased to see local events, such as targeted BGP hijacks.
- Dealing with inaccuracy / incompleteness. If sampling is applied, the robustness of the results needs to be evaluated to know inaccuracies.
- Related data to see impact / goal of a BGP hijack. Examples are attacks against DNS, Bitcoin, or TOR (deanonymization), as well as Spam campaigns. The challenging question is: "How to get the data?"
- Defining/finding "weird" (i.e., suspicious) activities. Can we cluster/group related "weird" items/entities?
- Dealing with companies doing DDoS mitigation based on BGP.
- Reliable detection of sibling ASes.
- ASes are not atomar entities.

5.2.5 Consumers of Data

We identified the following consumers of data related to BGP and inter-domain routing.

- Network operators.
- Academics / researchers.

References

1 University of Oregon. "Route Views Project." http://www.routeviews.org/routeviews/.

2 RIPE NCC. "Routing Information Service (RIS)." https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris.

3 Packet Clearing House (PCH). https://www.pch.net/.

4 CAIDA. "BGPStream: An open-source software framework for live and historical BGP data analysis." https://bgpstream.caida.org/.

5 CAIDA. "Periscope Looking Glass API." https://www.caida.org/tools/utilities/looking-glass-api/.

6 Andreas Reuter, Matthias Wählisch, Thomas C. Schmidt. "RPKI MIRO: Monitoring and Inspection of RPKI Objects." In Proc. of ACM SIGCOMM, pp. 107–108, New York:ACM, August 2015.

7 Merit. "IRR Internet Routing Registry." http://www.irr.net.

8 BGPmon. "BGPStream: a free resource for receiving alerts about hijacks, leaks, and outages in the Border Gateway Protocol." https://bgpstream.com/.

9 RADB. "RADB FTP database." ftp://ftp.radb.net/radb/dbase.

10 IRR. "List of Routing Registries." http://www.irr.net/docs/list.html#RADB.

11 CAIDA. "AS relationships." http://www.caida.org/data/as-relationships/.

12 PeeringDB. "Information related to Peering." https://www.peeringdb.com/.

13 Cisco. "Open BGP Monitoring Protocol (OpenBMP) Collection Framework." https://github.com/OpenBMP/openbmp.

14 Team Cymru. "IP to ASN Mapping." http://www.team-cymru.com/IP-ASN-mapping.html.

15 CAIDA. "Routeviews Prefix to AS mappings Dataset (pfx2as) for IPv4 and IPv6." https://www.caida.org/data/routing/routeviews-prefix2as.xml.

16 RIPE NCC. "RIPE Atlas." https://atlas.ripe.net/.

17 PlanetLab. "An open platform for developing, deploying, and accessing planetary-scale services." https://www.planet-lab.org/.

18 CAIDA. "Archipelago (Ark) Measurement Infrastructure." http://www.caida.org/projects/ark/.

19 Cunha, Italo, et al. "Sibyl: a practical Internet route oracle." (2016): 325-344.

20 Marder, Alexander, and Jonathan M. Smith. "MAP-IT: Multipass accurate passive inferences from traceroute." Proceedings of the 2016 Internet Measurement Conference. ACM, 2016.

21 Luckie, Matthew, et al. "bdrmap: inference of borders between IP networks." Proceedings of the 2016 Internet Measurement Conference. ACM, 2016.

22 Chen, Kai, et al. "Where the sidewalk ends: Extending the Internet AS graph using traceroutes from P2P users." Proceedings of the 5th international conference on Emerging networking experiments and technologies. ACM, 2009.

23 Nomikos, George, et al. "traIXroute: Detecting IXPs in traceroute paths." in Passive and Active Measurement (PAM), 2016.

24 One Step. "BGP Community Guides." https://onestep.net/communities/.

25 Mühlbauer, Wolfgang, et al. "Building an AS-topology model that captures route diversity." ACM SIGCOMM Computer Communication Review 36.4 (2006): 195-206.

5.3 DDoS / Routing Security Attacks

Adrian Perrig (ETH Zürich, CH)

Joint work of all seminar participants

We discussed DDoS attacks, as well as attacks against routing security in general.

We begin with algorithmic complexity attacks against routers; these can be used to exploit the "slow path" of a router, and, using a small number of packets (such as routing updates) crash a router. This attack is quite hard for well-protected IGP setups, where filtering is applied on routing updates on ingress (depending on the source of the update). However, this is a general problem when one has the capability to inject crafted updates in a network (IGP/BGP), e.g., via a compromised router. One possible solution to defend against such attacks is to rate-limit traffic from the data plane towards the slow path (i.e., the control plane of the router), effectively limiting the rate of packets that need to be processed by the router's CPU. However, this does not solve the problem of carefully crafted packets that aim to overload the router not through a volumetric attack, but through an algorithmic attack.

Another defense approach is to prevent control-plane traffic from being crippled by volumetric DDoS attacks on links carrying BGP traffic. In fact, this defense can be applied in practice by prioritizing control-plane traffic above all others. The latter action requires of course configuration and tuning of some knobs, and we do not know the extent at which this is applied in the wild.

With respect to identifying the "shape" of DDoS attacks, one could employ compromised honeypots. An example is the AMPPot Honeypot, used to detect/measure spoofed amplification attacks.

We also discuss other interesting types of attack in gaming setups; an attacker could force a player lag in e.g., "shoot-and-kill" games, by performing a short-lived amplification attack using spoofing against the opponent's IP address. Note that the gaming industry is quite large; DDoS can be used to "win" in different ways for financial or other gain (even for retaliation). One possible incentive is user dominance, leasing to "gang wars" between private server hosts. This leads to the natural consequence of "DDoS-as-a-service" for gamers? Moreover, one needs to consider attacks aiming to disrupt microtransactions which are heavily used in several online games.

An important attack vector usually employed to launch large-scale DDoS attacks and resurfaces every now and then, is IP spoofing. The question is: "will spoofing be eventually reduced?" According to network operators, today it is stricter than in the past, but this is still a problem. The main counter-argument that some providers put forth is that they want to allow their customers to do anything (including legitimate spoofing). This is rarer for customers with static routing, but providers will not invest effort in filtering by hand for BGP-based customers. So in fact, allowing anything is the practical choice currently, with the repercussions that this is associated with.

5.4 Quality of Service (QoS)

Adrian Perrig (ETH Zürich, CH)

Joint work of all seminar participants

We further discuss Quality of Service (QoS), w.r.t. routing. Fine-grained QoS (e.g., on the flow level) has been proven to be counterproductive, since it is associated with huge complexity to run in the core of the network due to practical constraints. QoS capabilities in the OSPF routing protocol mostly remain unused.

However, QoS is highly related to product management. A provider can sell a new business model to a customer. Currently, we best understand coarse-grained QoS. As an operational practice, the rule of thumb is the application of fine-grained QoS at the edge of the Internet (e.g., rate-limiting flows according to their traffic class), and coarse-grained `DiffServ` in the core. We note that there maybe a new need for QoS in upcoming applications; for scalability though, its delivery should ideally not keep any state in the network (`DiffServ` vs `IntServ`). Moreover, there should be (e.g., business-side) accountability in multi-hop scenarios; for example, if traffic related to an ongoing telesurgery is going through 5 providers, and failure happens, how does one know and resolve it, or know who to blame if it all goes wrong?

In general, QoS is mainly driven by business solutions rather than technical ones. Desired protocol properties, include but are not limited to, the following:

- Express policies in multi-hop scenarios, including business layer.
- Employ stateless protocols/mechanisms (at least in the core network).
- Report reliable data.

QoS itself may depend on physical deployment. For example, real-time translation requires low latency (and thus “close-by” servers). The main challenge that we face in the context of QoS is to come up with an approach that provides enough incentives for a small group to deploy (and then scale it up).

Participants

- Mai Ben-Adar Bessos
Bar-Ilan University –
Ramat Gan, IL
- Nikita Borisov
University of Illinois –
Urbana Champaign, US
- Georg Carle
TU München, DE
- Shinyoung Cho
Stony Brook University, US
- Ítalo Cunha
Federal University of Minas
Gerais-Belo Horizonte, BR
- Marc C. Dacier
EURECOM –
Sophia Antipolis, FR
- Phillipa Gill
University of Massachusetts –
Amherst, US
- Joel M. Halpern
Ericsson – Leesburg, US
- Raphael Hiesgen
HAW – Hamburg, DE
- Carlee Joe-Wong
Carnegie Mellon University –
Pittsburgh, US
- Mattijs Jonker
University of Twente, NL
- Vasileios Kotronis
FORTH – Heraklion, GR
- Taeho Lee
ETH Zürich, CH
- Hemi Leibowitz
Bar-Ilan University –
Ramat Gan, IL
- Victoria Manfredi
Wesleyan University –
Middletown, US
- Marcin Nawrocki
FU Berlin, DE
- Christos Pappas
ETH Zürich, CH
- Adrian Perrig
ETH Zürich, CH
- Alvaro Retana
Huawei Technologies –
Santa Clara, US
- Andreas Reuter
FU Berlin, DE
- Thomas C. Schmidt
HAW – Hamburg, DE
- Laurent Vanbever
ETH Zürich, CH
- Pierre-Antoine Vervier
Symantec Research Labs –
Sophia Antipolis, FR
- Stefano Vissicchio
University College London, GB
- Rüdiger Volk
Deutsche Telekom – Münster, DE
- Matthias Wählisch
FU Berlin, DE
- Bing Wang
University of Connecticut –
Storrs, US