jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2020, VOL. 66, NO. 1, PP. 1–6
Manuscript received October 10, 2019; revised January, 2020. DOI: 10.24425/ijet.2019.126xxx

Towards mutual routing security – a review

Mikołaj Kowalski, Wojciech Mazurczyk

***Abstract*—Historically, the inter-domain routing security had to be established based on trust, due to poorly designed BGP protocol. This approach is insufficient, as seen in practice numerous times. To prevent this, new kind of security measures were proposed and are needed to be implemented on Internet's majority AS'es.**

This article covers the current threat landscape and taxonomy of attack vectors on routing layer, as well as current and new protective measures with theirs future development plans and caveats.

However, due to current system design, the protection is based on mutual protection. This causes the chicken or the egg problem. Author will try to explain slow adoption rate.

***Keywords*—Routing protocols, Network security, Telecommunication network reliability, Wide area networks**

I. Introduction to routing security

AUTONOMOUS SYSTEMS (ASes) are main, essential entity in today's Internet. As defined in [1], "an AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy". When routing policy is configured and accepted by adjacent ASes (peers) traffic is allowed to flow.

If a traffic is traversing in an unintended fashion (conflicting with the routing policy), one can call a *routing incident*. Detailed breakdown of incident types and enumeration of different scenarios is presented in section II-A. Threat landscape and risk analysis are available in II-B.

There are well defined means of protection which mitigates impact for these attacks. Main division factor that should differentiate them is *passive* – traditionally used as basic BGP *hygiene* intended for verifying the trust of a peer or traffic engineering tricks, and *proactive* means – new generation technologies that guarantee an incident will not happen. Both categories are described in sections III-A and III-B,III-C, respectively.

In section IV-A author summarizes the RPKI implementation global progression and tries to give a prognosis on future efforts. To give complete view, section IV-D describes some unwanted scenarios and threat that RPKI introduces. The section IV-B provides the overview on future development directions.

Section V states author's conclusions.

This work was supported by the grant No. xxxxxx "Doktorat wdrożeniowy" by Ministerstwo Edukacji i Nauki.

M. Kowalski is with Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland (e-mail: 6796@pw.edu.pl).

Professor W. Mazurczyk is with Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland (e-mail: wmazurcz@(NOSPAM)elka.pw.edu.pl).

II. Routing incidents taxonomy – problem definition

In general, the routing incident is undesirable routing system change, to the state that it is no longer operational or working at suboptimal capacity.

There are several different metrics that can be used to classify routing incident, in this work we will explore criteria/benchmarks such as:

type most important, incident ought to be pinned to a category that ensure unambiguous classification. More on that in II-A

intent an incident may originate from intentional, malicious action (so called attack). If done on purpose, possible causes are interception of traffic to espionage, credential theft, censorship or denial of service (downtime, outage) specific website or company. In contrary, erroneous configuration that is result of human mistake, sometimes called *fat finger* mistake, does not have an ultimate agenda.

scale the targeted incident might be for one prefix only, but sometimes there will be plenty prefixes involved

impact there are multiple factors in this metric, so this will be discussed in II-B

duration usually, errors impacting substantial amount of networks or users are corrected in a timely manner, but some small incidents may last weeks unnoticed

range some incident will be accepted only by peer AS, but some of them will propagate globally (to the DFZ)

A. Routing incidents characteristics and taxonomy

The most basic division of routing incidents are *BGP Hijacks* and *Route Leaks*. In this paper we present ... (state of the art/ best in our opinion?) taxonomy.

1) Route leaks: As defined in [2], route leak is propagation of (single or multiple) routing announcement beyond their intended scope, which is defined by routing policy, implemented by a set of redistribution filters. Route leaks are typically not malicious, most often an effect of configuration mistake.

Most common scenario for leak is when a multihomed stub AS re-advertise a prefix from one of it's transit providers to another. The second provider won't detect a leak and propagate the route further. However, IETF suggest more detailed classification of leaks:

- **Type 1: Hairpin Turn with Full Prefix** – most common case, that makes the stub network that leaked a prefix a transit network. Leak is usually successful, as transit networks usually accept prefixes from their customers.

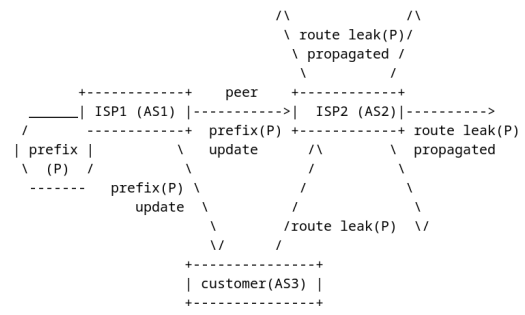

Figure 1. Route Leak topology [2] (do przerysowania?)

The traffic will reach the destination if stub network will be able to process higher volume of traffic.

- **Type 2: Lateral ISP-ISP-ISP Leak** – when ISP's are peering, they should announce only prefixes of their customers. Type 2 takes place when an ISP is propagating prefix of the another ISP whom peering agreement was established.
- **Type 3: Leak of Transit-Provider Prefixes to Peer** – this type is about propagating prefixes from transit provider to lateral network, effectively providing transit service to the peer.
- **Type 4: Leak of Peer Prefixes to Transit Provider** – comparing to Type 3, this has the flow in opposite direction . However, it is more dangerous, as it may hurt the peer when the AS-PATH is shortened
- **Type 5: Prefix Re-origination with Data Path to Legitimate Origin** – offending multihomed AS announces learnt prefix but without original AS-PATH. This case is similar to **Type-0, Exact Prefix, MitM Prefix Hijack** classified in [3], but it assumes that the prefix ought to be learnt from upstream ISP.
- **Type 6: Accidental Leak of Internal Prefixes and More-Specific Prefixes** – this type is different, as the prefixes in leak are originating from within offending AS. This is a common issue, typically a badly configured export policy, insufficient aggregation or weak outbound filters. More specific prefixes should not be present in DFZ when a less-specific route exists. In contrast to **Type-0 Sub-prefix BGP Hijack**, offending AS owns prefixes that are announced.

2) BGP Hijacks: Hijack event is when the adversary Autonomous System illegitimately advertise an IP prefix (or part of it) belonging to other AS. The advertisement needs to propagate towards other BGP speakers if hijack is considered to be successful.

Authors in [3] proposed a very detailed taxonomy, with three split categories. The *affected prefix* can be the same as rightfully originated (**Exact Prefix Hijack**) or more-specific (**Sub-Prefix Hijack**), but also not currently advertised (**Squatting Hijack**) by the victim. Furthermore *AS-Path announced* might be simply substituted for hijacker ASN only (**Type-0 Hijack**) or modified with victim ASN first and hijacker ASN last in the path (**Type-N Hijack**). Moreover when the AS-PATH is not modified, one should distinguish **Type-U Hijack**. The third category concerns data-plane traffic handling when a hijack takes place. Possible actions that can be taken by adversary are: **blackhole** when the traffic is simply dropped, **man-in-the-middle** for connection eavesdropping or manipulating, or **imposture** when adversary mimics the victim services and an interaction with legitimate hosts takes place.

B. Impact of routing incidents

1) BGP Hijacks: When a Autonomous System attempt Hijack it may affect availability, integrity, and confidentiality of communications in the victim network. The impact depends mostly on the intent of the incident, closely related to the adversary agenda. However, to break down to technical indicators, lets analyse it by the incident type data-plane traffic handling.

For blackhole there is availability problem for victim's network and possible full outage (denial of service situation). It is similar in effect to data-plane DoS attack, but it's less expected and harder to defend to.

When considering man-in-the-middle the adversary is creating malicious BGP Hijack it focused on getting the data and keeping the connection intact. Use cases include credential theft, data manipulation .... ¡TODO¿

The most advanced technique is impersonating victim's servers. ¡TODO¿

2) Route leaks: With Route Leaks, ¡TODO¿

Route leak will cause a redirection of traffic to the different path that it was intended. This may or may not result in overloading some network equipment and network links or blackholing the traffic altogether.

C. Measuring attack impact in the wild

Hijacks sometimes have a severe and lasting impact. While it is relatively easy to monitor the state of routing in the Internet's control-plane thanks to initiatives like RIPE RIS[1] and software build on top of it or Qrator Radar[2] directly detecting some kind of routing incidents, it is difficult to verify real impact – users affected and financial losses as companies tend to not disclose such details.

However, there has been attempt to check real impact of routing incidents. As surveyed among 75 networks from NANOG and RIPE mailing list subscribers in [4], 41% of the operators reported that their organization has been a victim of a hijack in the past. "The vast majority (76%) expects the impact of a hijack to last for a long time (few hours or more), while opinions are divided on whether the hijack will affect a few or many of their services/clients, indicating that there are concerns both for extended (e.g.route leaks) and limited/targeted (e.g. malicious attacks) hijacks. (...) More than 57% of hijacks lasted more than an hour, while 25% lasted more than a day; around 28% are short-term hijacks, lasting a few minutes (14.3%) or seconds (14.3%). "

[1]https://ris-live.ripe.net/
[2]https://radar.qrator.net/

D. Incident examples

MyEtherWallet, provider for Etherum cryptocurrency wallets has been attacked by a BGP hijack on April 24th, 2018[5]. The attack was not carried directly at MyEtherWallet, but instead on Amazon Web Services' DNS infrastructure. Worth noting is that AWS DNS was not compromised, but the AWS Route 53 prefix space was the subject of hijack. The resulting outcome was $365,000 stolen in ETH, in spite of users being warned of self-signed TLS certificate. The attacker was announcing more-specific prefixes (**sub-prefix hijack**) and running **man in the middle** proxy for DNS traffic. The cryptocurrency website was **impersonated**.

Telekom Malaysia (AS4788) and Level3 (AS3549) incident was massive **Type 4** and **Type 6** route leak. As described in [6], more than 176 000 prefixes learnt from peering session in DEC-IX and more-specific client prefixes were leaked to upstream provider. This resulted in huge amount of traffic being directed to AS4788 which caused network overload also for Level3. Typical symptoms like packet loss and RTT increase was observed.

Another case of among many route leak incidents resulted in outage of AWS and Amazon services unavailability. As described by researcher from ThousandEyes in [7], AS33083 announced AWS' prefixes to it's transit provider AS5580. This announcement wasn't in the path before, so the prefix leak is of **Type 4** II-A1. The leak has affected cloud services and therefore multiple companies.

E. Other techniques accompanying routing attacks

1) Acquisition of Bogus TLS certificate using BGP sub-prefix interception: Most of the times, to perform a successful attack an adversary is required to do some kind of MiTM attack. For example, the simplest way to redirect the traffic is to redirect DNS queries and spoof the DNS response. An attacker will be available to issue a valid TLS certificate, as he will be able to pass all checks that CA is using to verify remote side. [8]

As presented in [8], further executed and measured in [9],[10], there is a possibility to issue a valid certificate that should not be issued. The mechanism presented shows a bug in CA's verification procedure, however using BGP routing attack can exploit this bug, leading to further target impersonating by the attacker. Researchers suggest two countermeasures for CA's: *Multiple Vantage Point Verification* and *Monitoring BGP Route Age*.

III. Safeguards

TODO
preventive (mitigate risk) – vs post-incidental

A. Traditional protection

bgp filtering,classical approach
Considerations in Validating the Path in BGP [11]

B. Route Origin Validation

C. Full Path Validation

aka BGP AS_PATH attribute
BGPSec [12] [13]
Please see IV-C for more on Path Validation

IV. Current state of affairs and future work

In previously cited survey study [4], most of the network operators (71%) answered that they have not deployed RPKI as a proactive defense mechanism in their networks 2; very few (12%) use the full functionality of RPKI (Route Origin Authorization – ROA and Route Origin Validation – ROV). ROA is used by 15% of networks.

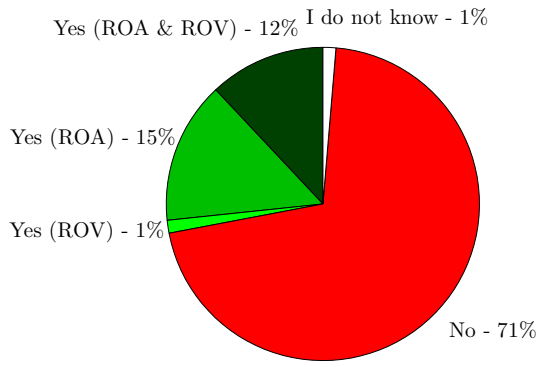

Figure 2. Usage of RPKI based on survey by [4]

However, these number seems to be changing, as cam be seen on 3 and 4.

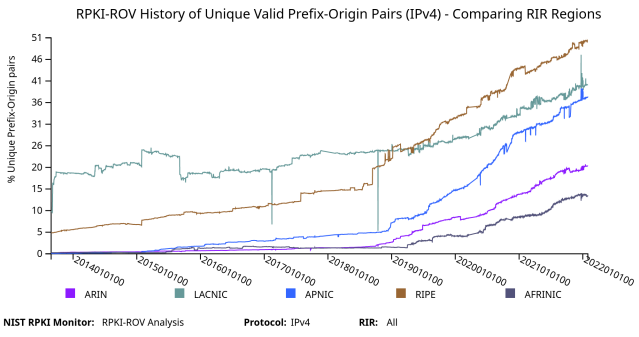

Figure 3. A percent of the total count unique announced Prefix-Origin pairs with prefixes in the corresponding RIR. Source: NIST RPKI Monitor

A. Slow adoption

1) Lack of awareness: TODO
MANRS is doing a great job[14]

2) Technical difficulties: Researches in [4] points that "deployment lags mainly due to RPKI's limited adoption and little security benefits, but also due to the increased CAPEX and OPEX costs, and increased complexity and processing overhead associated with the protocol mechanisms. Therefore, about 60% of the operators resort to other mechanisms and

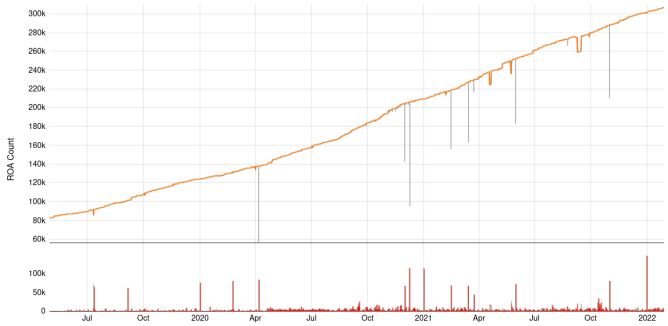

Figure 4. Total count of ROA over time. Source: Cloudflare RPKI Portal

practical defenses to protect their networks against BGP hijacks." For detailed breakdown of adoption slowiness causes, see fig. 5.

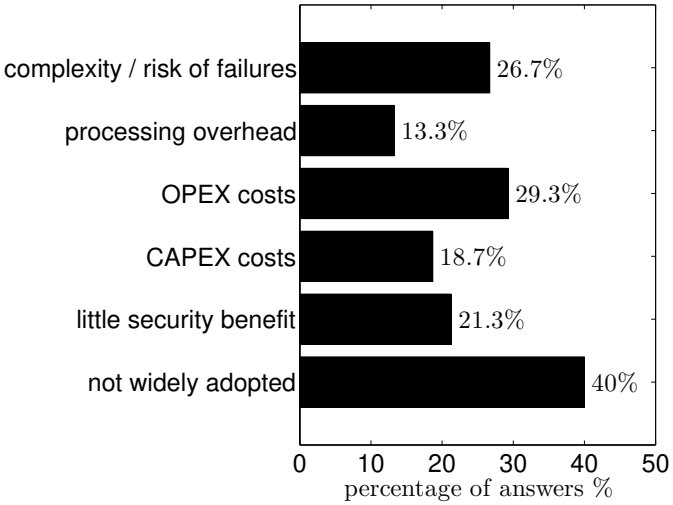

Figure 5. Main reasons not using RPKI based on survey by [4]

3) Legal issues: Widespread RPKI adoption may be limited due to specific status on ARIN's terms and conditions for RPKI repository. Third parties who wish to validate BGP routes had to agree *Relying Party Agreement*. As a result, most RP validating software does not come with ARIN TAL embedded by default.

This has a direct effect on ARIN members in North America – Route Origin Validation on ARIN AS' has been significantly lower. Almost 80% of those AS engaging in ROV omit the ARIN TAL, has been proofed by [15].

In the beginning of 2019, the gap between ARIN's ROA only grew. This state of affairs was criticized in work [16], but researchers presented 6 solutions. However, in late 2019 the RPA was changed [17]. The change "was intended to accommodate and overcome claimed barriers to RPKI adoption" and distribution in machine readable formats has been approved. In author opinion, although the change is in a good direction, a desired state of good and simple configuration is still obstructed.

4) Low RPKI deployment penetration factor among CDNs: Content Delivery Networks have crucial function in the global Internet, providing usually heavy content to the user in a fast, reliable and cheap manner. It is estimated that over a half of all web traffic is served over CDNs, therefore securing this segment is prominent in the global scale.

Researchers in [18] investigated some among most important CDNs: Akamai, Amazon, Cdnetworks, Chinacache, Cloudflare, Cotendo, Edgecast, Highwinds, Instart, Internap, Limelight, Mirrorimage, Netdna, Simplecdn, and Yottaa.

> (By the reverse IP lookup, they – note ed.) discovered 199 ASes operated by these CDNs. From these, we find only four entries in the RPKI. These four prefixes are owned by Internap and are tied to three origin ASes. One might mistakenly think that Internap has therefore engaged widely with RPKI. However, Internap operates at least 41 ASes, the bulk of which are not secured via RPKI. No other CDN has made any deployment. Thus, these CDNs do not actively participate in the creation of RPKI attestation objects.

To combat this low adoption progress, MANRS consortium has launched dedicated *program for CDN and Cloud Providers* on April 2020. As of December 3, 2020 the program has 14 members [19]. One of the mandatory Actions is "Fostering RPKI as the primary technology for validation of routing information on a global scale", while "Improving consistency of route validation based on route objects published in an IRR".

B. RPKI infrastructure work

1) rsync depreciation: RPKI repositories and Relying Party software performing RPKI Validation will use the RPKI Repository Delta Protocol (RRDP) [RFC8182] [20]

2) :

C. New approach on Path Validation

aha BGP AS_PATH validatin
ASPA? [21] [22]
[23] implementing BGP-SRx
[24]

D. Caveats

1) RPKI MaxLength parameter: subprefix hijack [25]
2) Unilateral IP space takedowns: [26]
3) MOAS: colision clash conflict [27]

V. Conclusion

Internet to dziki zachód ale robim co możem

In the Internet, routing announcements are accepted without almost any validation
•This opens a possibility for a network operator to announce someone else's network prefixes without permission

•The prefix may be announced with the same origin
•The prefix may be leaked
•A malicious operator can steal prefixes and blackhole them or intercept and modify traffic in transit
•A good operator can also steal someone's network occasionally, by an error
•A malicious employee of a good operator is then able to read and modify incoming traffic as well
•Unauthorized access to operator's equipment can also be used for hijacking [8]

REFERENCES

[1] J. A. Hawkinson and T. J. Bates, *Guidelines for creation, selection, and registration of an Autonomous System (AS)*, RFC 1930, Mar. 1996. DOI: 10.17487/RFC1930. [Online]. Available: https://rfc-editor.org/rfc/rfc1930.txt.

[2] K. Sriram, D. Montgomery, D. R. McPherson, E. Osterweil, and B. Dickson, *Problem Definition and Classification of BGP Route Leaks*, RFC 7908, Jun. 2016. DOI: 10.17487/RFC7908. [Online]. Available: https://rfc-editor.org/rfc/rfc7908.txt.

[3] P. Sermpezis *et al.*, "Artemis: Neutralizing bgp hijacking within a minute," Jan. 3, 2018. arXiv: 1801.01085 [cs.NI].

[4] P. Sermpezis, V. Kotronis, A. Dainotti, and X. Dimitropoulos, "A survey among network operators on bgp prefix hijacking," Jan. 9, 2018. arXiv: 1801.02918 [cs.NI].

[5] R. Brandom. "Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet." en, The Verge. (Apr. 24, 2018), [Online]. Available: https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum (visited on 01/16/2021).

[6] A. Toonk. "Massive route leak causes internet slowdown." (Jun. 12, 2015), [Online]. Available: https://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/.

[7] N. Kephart. "Route leak causes amazon and aws outage." (Jun. 30, 2015), [Online]. Available: https://www.thousandeyes.com/blog/route-leak-causes-amazon-and-aws-outage.

[8] A. Gavrichenkov, "Breaking https with bgp hijacking," in *Black Hat USA 2015*, Aug. 5, 2015. [Online]. Available: https://www.blackhat.com/us-15/briefings.html#breaking-https-with-bgp-hijacking (visited on 01/16/2021).

[9] H. Birge-Lee, Y. Sun, A. Edmundson, J. Rexford, and P. Mittal, "Using bgp to acquire bogus tls certificates," in *The 17th Privacy Enhancing Technologies Symposium*, Princeton Univeristy, Jul. 18, 2017. [Online]. Available: https://www.princeton.edu/~pmittal/publications/bgp-tls-hotpets17.

[10] H. Birge-Lee, Y. Sun, A. Edmundson, J. Rexford, and P. Mittal, "Bamboozling certificate authorities with BGP," in *Proceedings of the 27th USENIX Conference on Security Symposium*, ser. SEC'18, USA: USENIX Association, Aug. 2018, pp. 833–849, ISBN: 9781931971461. [Online]. Available: https://www.cs.princeton.edu/~jrex/papers/bamboozle18.pdf (visited on 01/16/2021).

[11] R. White and B. Akyol, *Considerations in Validating the Path in BGP*, RFC 5123, Feb. 2008. DOI: 10.17487/RFC5123. [Online]. Available: https://rfc-editor.org/rfc/rfc5123.txt.

[12] M. Lepinski and K. Sriram, *BGPsec Protocol Specification*, RFC 8205, Sep. 2017. DOI: 10.17487/RFC8205. [Online]. Available: https://rfc-editor.org/rfc/rfc8205.txt.

[13] W. George and S. L. Murphy, *BGPsec Considerations for Autonomous System (AS) Migration*, RFC 8206, Sep. 2017. DOI: 10.17487/RFC8206. [Online]. Available: https://rfc-editor.org/rfc/rfc8206.txt.

[14] A. Robachevsky, "Improving routing security through concerted action," presented at the RIPE 80, May 12, 2020. [Online]. Available: https://ripe80.ripe.net/wp-content/uploads/presentations/3-202005-MANRS-RIPE80.pdf.

[15] B. Cartwright-Cox. "Are bgps security features working yet?" (Sep. 10, 2018), [Online]. Available: https://blog.benjojo.co.uk/post/are-bgps-security-features-working-yet-rpki.

[16] C. S. Yoo and D. A. Wishnick, "Lowering legal barriers to rpki adoption," *U of Penn Law School, Public Law Research Paper*, no. 19-02, Aug. 1, 2019.

[17] J. Curran. "ARIN Announces New Relying Party Agreement (RPA) To Spur Use of RPKI," ARIN. (Oct. 21, 2019), [Online]. Available: https://www.arin.net/vault/announcements/2019/20191021.html (visited on 01/17/2021).

[18] M. Wählisch, R. Schmidt, T. C. Schmidt, O. Maennel, S. Uhlig, and G. Tyson, "Ripki: The tragic story of rpki deployment in the web ecosystem," Aug. 2, 2014. DOI: 10.1145/2834050.2834102. arXiv: 1408.0391 [cs.NI].

[19] A. Siddiqui, *MANRS Welcomes 500th Network Operator*, en-US, MANRS, Dec. 2020. [Online]. Available: https://www.manrs.org/2020/12/manrs-welcomes-500th-network-operator/ (visited on 01/17/2021).

[20] T. Bruijnzeels, R. Bush, and G. G. Michaelson, "Resource Public Key Infrastructure (RPKI) Repository Requirements," Internet Engineering Task Force, Internet-Draft draft-ietf-sidrops-deprecate-rsync-00, Aug. 2020, Work in Progress, 10 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-deprecate-rsync-00.

[21] A. Azimov, E. Uskov, R. Bush, K. Patel, J. Snijders, and R. Housley, "A Profile for Autonomous System Provider Authorization," Internet Engineering Task Force, Internet-Draft draft-ietf-sidrops-aspa-profile-04, Nov. 2020, Work in Progress, 9 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-profile-04.

[22] A. Azimov, E. Bogomazov, R. Bush, K. Patel, and J. Snijders, "Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization," Internet Engineering Task Force, Internet-Draft draft-ietf-sidrops-aspa-verification-06, Nov. 2020, Work in Progress, 13 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-06.

[23] O. Borchert, *BGP Secure Routing Extension (BGP-SRx) Prototype*, en, NIST, Ed., Aug. 2016. [Online]. Available: https://www.nist.gov/services-resources/software/bgp - secure - routing - extension - bgp - srx - prototype (visited on 01/06/2021).

[24] O. Junjie, N. Yanai, T. Takemura, M. Okada, S. Okamura, and J. P. Cruz, "Apvas: Reducing memory size of as_path validation by using aggregate signatures," Aug. 31, 2020. arXiv: 2008.13346 [cs.CR].

[25] Y. Gilad, S. Goldberg, K. Sriram, J. Snijders, and B. Maddison, "The Use of Maxlength in the RPKI," Internet Engineering Task Force, Internet-Draft draft-ietf-sidrops-rpkimaxlen-05, Nov. 2020, Work in Progress, 12 pp. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-rpkimaxlen-05.

[26] K. Shrishak and H. Shulman, "Limiting the power of rpki authorities," presented at the Applied Networking Research Workshop 2020, 2020. [Online]. Available: https://irtf.org/anrw/2020/slides-shrishak-00.pdf.

[27] X. Zhao *et al.*, "An analysis of bgp multiple origin as (moas)conflicts," *Internet Measurement Workshop*, 2001. [Online]. Available: https://www.cs.colostate.edu/~massey/pubs/conf/massey_imw01.pdf.