

SCION Versus Hardened BGP

Philip Falk, Michael Oberrauch*

**Chair of Network Architectures and Services*

School of Computation, Information and Technology, Technical University of Munich, Germany

Email: ge38fec@mytum.de, oberrauc@net.in.tum.de

Abstract—BGP has been the backbone of the Internet since its beginning. However, it is outdated and contains many security flaws. Various security extensions like BGPsec, RPKI-ROA and ASPA exist to mitigate these flaws. SCION is a new routing protocol, currently in development, with the aim to replace BGP in the future. With *security by design*, it wants to overcome BGP's security problems. This paper explores the main security mechanisms of both protocols and compares them to each other. We conclude that BGP's extensions improve its security significantly, but SCION's built-in cryptography is superior.

Index Terms—scion, border gateway protocol, bgpsec, resource public key infrastructure, aspa

1. Introduction

Today's Internet is a network of many autonomous systems (ASes). Each AS is a network of routers which is governed by an independent organization such as Internet service providers (ISPs), universities, or tech companies [1]. ASes regularly exchange information, so that the underlying routers, typically belonging to end-users, can communicate with each other. The border gateway protocol (BGP), originally created in the 1980s, is the protocol responsible for these frequent information exchanges (routing) between neighboring ASes. At the time of its conception, the Internet was still relatively small and security aspects were not a big point of focus. BGP therefore fundamentally works on unverified trust between networks. [2] Nowadays, unchecked false information about ASes, malicious or accidental, can spread over the Internet and can lead to issues like the famous YouTube hijack in 2008, which led to an hours-long YouTube outage [3]. This imposes a considerable security risk, which is why various mechanisms have been developed to reduce the dangers and flaws by extending BGP. These systems however, are not directly part of BGP but optional additions.

Further efforts try to eliminate today's dependency on BGP entirely through a new routing protocol called SCION. Scalability, Control, and Isolation On Next-generation networks (SCION) was designed with built-in security since its conception and is supposed to replace BGP in the future. It is, however, still in active development by the ETH Zürich and no standardized version exists at the time of writing in October 2025. [2]

We aim to compare the security aspects of different variations of hardened BGP to the new approach by SCION and show the differences between both protocols.

Section 2 first provides an overview on how both BGP and SCION work and presents the main security problems. The following Section 3 then describes the existing and proposed security mechanisms for both protocols to mitigate the addressed dangers. Section 4 discusses and compares the presented mechanisms, Section 5 indicates further research, and finally Section 6 highlights the key outcomes.

2. Background

This section provides necessary knowledge on the security challenges of plain BGP and presents an overview of the mechanisms of both BGP and SCION.

2.1. BGP

To understand BGP, it is essential to know the concepts of Autonomous System Numbers (ASNs) and IP prefixes. An ASN is a globally unique identifier assigned to each AS by a Regional Internet Registry (RIR) under the coordination of the Internet Assigned Numbers Authority (IANA) [4]. Each AS manages one or more IP prefixes, sets of IP addresses it can allocate internally, and advertises these prefixes to other ASes via BGP to enable inter-domain communication.

Consider AS1 advertising its prefix 192.0.20.0/24 to neighboring ASes, AS2 and AS3. After establishing a peering connection with both neighbors, AS1 sends an advertisement to each of them [4]. Advertisements are officially called *UPDATE* messages and contain certain attributes. The most relevant one for this context is *AS_PATH*. It is a sequence of ASNs that need to be traversed in order to arrive at the AS that owns the advertised prefix. This originating AS is the rightmost ASN in the sequence. [5]

The current example of the BGP functionality can be seen in Figure 1. AS1 is the originating AS which starts to advertise its prefix by adding its ASN to the initially empty *AS_PATH*. When an advertisement reaches an AS, the receiving AS will remember its routing information, prepend its own ASN to the *AS_PATH*, and propagate it further to other ASes. As a result, the originating ASN remains at the rightmost position of the sequence, allowing any AS that receives the advertisement to identify both the prefix owner and the sequence of ASes that must be traversed to reach the originating AS. [4]

As illustrated in Figure 1, it is possible that an AS receives multiple advertisements from different sources containing the same prefix. It is then up to the AS's

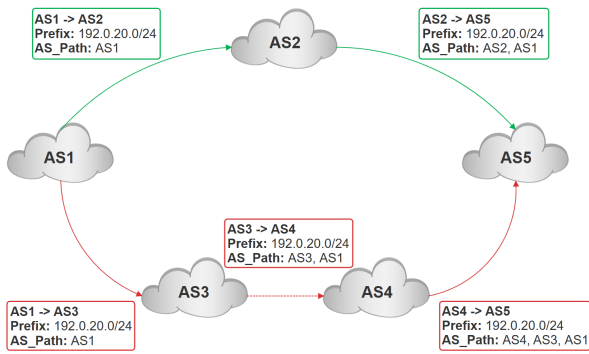


Figure 1: BGP routing process [4]

routing policy to prefer one path over the others. [4] It may also happen that some routes between neighboring ASes become unavailable. That is why these advertising messages get sent regularly, so a different path can be created instead.

2.2. BGP's security challenges

Plain BGP is solely based on trust relationships between ASes and has no security features. With nowadays over 80.000 active ASes, it is however, quite likely that not all are trustworthy [3]. An attacker controlling an AS has multiple options to hijack BGP traffic and subsequently force Internet traffic containing user-data through their malicious AS. The attacker can then either establish themselves as a Man in the Middle or simply drop the traffic, resulting in a Denial of Service (DOS) attack [6].

Suppose a malicious AS, controlled by an attacker, aims to replicate the mentioned YouTube hijack and force Internet traffic directed to YouTube through itself. The attacker could identify the prefixes belonging to YouTube and start advertising more specific subprefixes. These more specific prefixes subsequently spread through the Internet and users trying to access YouTube get redirected to the attacker instead. The reason for that is called longest prefix matching, which always redirects traffic to the most specific prefix available. [6] Alternatively, a prefix with a shorter path can also be announced [3]. The malicious AS takes the role of an originating AS wanting to advertise its prefixes when in reality it doesn't own the advertised prefixes. This type of attack works because plain BGP doesn't require origin validation, a check whether or not an AS owns its announced prefixes. Any AS can advertise any prefix, and any advertised prefix is implicitly trusted.

If an origin validator is however present, the same attacker has yet another way to hijack BGP traffic. Instead of pretending to own an advertised prefix, the malicious AS can also insert itself into a fake AS_PATH with the correct originating AS. An origin validator would check if the rightmost ASN in the AS_PATH owns the advertised prefix and would find it to be true, when in fact the malicious AS has placed its ASN at any place ahead of the origin ASN. [6] This makes it evident that a combination of origin validation and path validation is necessary to successfully validate an incoming prefix advertisement. Section 3 describes these two types of validation mechanisms.

It is important to note that route hijacks can also happen accidentally and are then referred to as route leaks. Usually, these are caused by misconfigurations. [7] An example for an accidental prefix hijack was the mentioned YouTube hijack where the government-owned Pakistan Telecom tried to block the access to YouTube country-wide. An accident caused this new BGP route, containing a more specific prefix, to spread over the Internet and effectively redirecting all YouTube traffic to Pakistan [3]. To fix the issue, an even more specific prefix had to be announced in order to hijack the traffic back [4].

2.3. SCION

SCION aims to become the next-generation Internet routing protocol by preventing the issues of BGP. It starts by logically grouping multiple ASes into Isolation Domains (ISDs), for example by country. Each ISD has a set of Core ASes which collectively create a common trust domain described in a Trust Root Configuration (TRC) which all Non-Core ASes agree upon. [2]

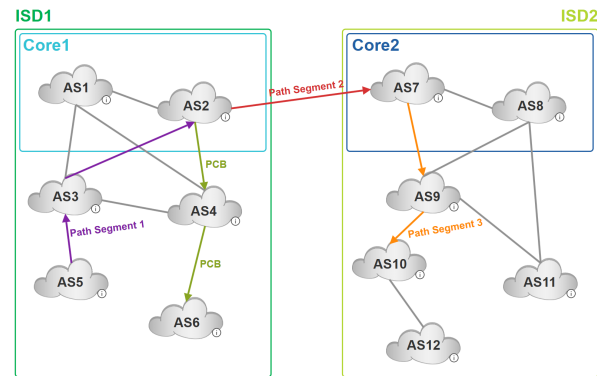


Figure 2: SCION beaconing and path segments [2]

As seen in Figure 2, communication inside of an ISD happens mainly between Core ASes and Non-Core ASes (Intra ISD) while communication between two different ISDs happens from Core1 to Core2 (Inter ISD). The goal of SCION is to create multiple path segments which are combined into a cryptographically secured forwarding path. An exemplary forwarding path, connecting AS5 from ISD1 to AS10 from ISD2, is illustrated in Figure 2, and consists of multiple path segments. A path segment is constructed through a process called beaconing, which works similarly to BGP's *UPDATE* messages. Intra ISD beaconing and Inter ISD beaconing function analogously. [8]

Intra ISD beaconing works by periodically sending Path Construction Beacons (PCBs) from Core ASes downwards to Non-Core ASes. PCBs consist of a sequence of AS Entries representing the path which the PCB has travelled so far. When a Non-Core AS receives a PCB, it first checks its validity as described in Section 3.4 and then adds its own AS Entry. An AS Entry cryptographically identifies the respective AS and contains a Hop Field (HF). An HF serves as a forwarding instruction for traffic within the respective AS, specifying how the traffic must travel to the next hop in order to correctly follow a path. The sequence of AS Entries, each containing an HF, is equivalent to the AS_PATH attribute in BGP with the

exception that each AS Entry is also cryptographically protected. [8]

When a PCB reaches a Leaf AS, the path discovery of that PCB is completed. Each Non-Core AS the PCB has passed through now has a valid path segment to its ISD's Core. Path segments are created from received PCBs and contain all the AS Entries from the respective PCB. PCBs are sent periodically in batches so that each Non-Core AS usually has multiple alternative path segments to choose from. [8]

SCION not only offers security in its path discovery beaconing process but also provides a SCION header for packet delivery. The SCION header encapsulates, next to the user-data, also the forwarding path to make sure that each packet stays on the selected path. The forwarding path is constructed from the Hop Fields from all AS Entries of all path segments. [9]

3. Security Mechanisms of BGP and SCION

This section explains the main security extensions for BGP and the built-in security features in SCION.

3.1. Security in BGP: RPKI (ROA)

As already stated, an AS can acquire its ASN and its prefixes from a RIR. Additionally, the AS also receives a certificate from its respective RIR, verifying that the AS owns said resources. In order to achieve origin validation, the AS can then create a Route Origin Authorization (ROA) record, which is a data object containing the resources (ASN and prefixes) owned by the AS [7]. ROAs essentially state which AS is authorized to originate which prefixes [10]. The AS can then cryptographically sign the ROA and have the certificate from the RIR validate its authenticity. The RIR thereby takes the role of a Certificate Authority (CA), a root of trust. ROAs can be saved in the RIR's repository publicly accessible for other ASes. When other ASes receive prefix advertisements, they can now validate their origin through the respective ROA by following the certificate chain to the trust anchor. [7]

This linking of resources to resource-owners by issuing certificates is called the Resource Public Key Infrastructure (RPKI) and it provides cryptographic origin validation [4]. Prefix hijacks, like the YouTube hijack, can be prevented this way.

3.2. Security in BGP: BGPsec

RPKI-ROA prevents ASes from originating prefixes which they do not own. What it does not prevent, however, are announcements of fake paths with correct origins. BGPsec is an extension to BGP which equips it with this necessary cryptographic path validation. It works on the basis of the already established RPKI by replacing the AS_PATH attribute from BGP advertisements with a cryptographically secured version called BGPsec PATH. [6] Figure 3 presents an example of BGPsec's functionality.

AS1 wants to announce its prefix to AS2. It therefore adds its ASN to the initially empty BGPsec PATH. To secure this initial advertisement, AS1 creates a cryptographic signature sig1, computed over the prefix, the

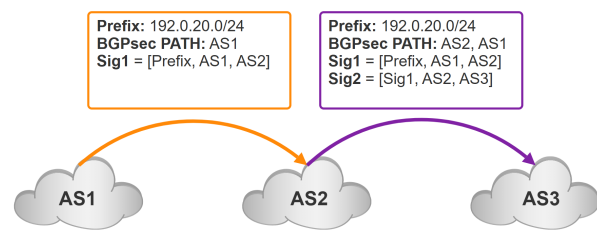


Figure 3: Example of BGP routing with BGPsec [4]

advertising AS (AS1) and the destination AS (AS2). This signature is added to the advertisement and sent to AS2. AS2 receives this advertisement and first checks the validity of all previous signatures. At this moment, that involves only sig1, which is validated by retrieving AS1's public key from its certificate through the RPKI. Advertisements with invalid signatures are dropped. If the signature is correct, then AS2 prepends its ASN to the BGPsec PATH and creates its own signature sig2. Sig2 and all further signatures are however not computed over the prefix anymore since that is already saved in sig1. Instead, sig2 is calculated over the current ASN (AS2), the destination AS (AS3) and the signature from the direct predecessor (sig1), thereby chaining the signatures together. All further ASes will have to follow the same steps as AS2, with the exception that the chain of signatures will grow and thereby involve more steps to validate. [4] This will result in increasing memory costs and processing power, which is one of the main drawbacks of BGPsec [6]. Another issue with BGPsec is the remaining vulnerability to an attack called wormhole attack [4].

3.3. Security in BGP: ASPA

Autonomous System Provider Authorization (ASPA) is a more lightweight approach to secure path validation. ASPA objects work very similarly to ROA records. They are data structures, created and signed by an AS and publicly available to other ASes at a RIR repository. ASPA also makes use of the RPKI by utilizing its CAs that hand out certificates to validate the signature of an ASPA object. The difference between ASPA and ROA is therefore only in their content. [11]

An ASPA object allows an AS (ASX) to specify a list of its authorized upstream providers. These are other ASes which are allowed to propagate any BGP advertisements that they have received directly from ASX. This customer-provider relationship (ASX is a customer) ensures that prefix advertisements can only propagate over trusted ASes. To fully secure a path, all ASes on the path must own ASPA objects in which they specify their respective providers. [12]

Consider the following exemplary AS_PATH: "AS3, AS2, AS1", with AS1 being the originating AS. ASPA path validation happens at every hop. This means that every AS, which receives an advertisement, must validate the entire received path. An AS receiving the stated path therefore has to acquire the ASPA object of AS1 and check if AS2 is part of AS1's list of upstream providers. If that is the case, then the next ASPA by AS2 is checked to validate the next customer-provider relationship between

AS2 and AS3. This continues until all relationships between two ASes of the path have been validated. Due to the nature of AS relationships, it is possible that at some point in the path, the relationship of "customer to provider" switches around to "provider to customer", resulting in an earlier AS in the path being the provider and the following AS being the customer. To successfully validate a path with ASPA, it is therefore allowed to have a single transition point. The validation of provider to customer relationships works the same by checking the customers' ASPA for its downstream providers. [11]

In the rare event that a compromised provider hijacks prefixes, ASPA is unable to detect such attacks [13]. Just like SCION, ASPA is still work in progress and no standardized version exists at the time of writing [11].

3.4. Security in SCION

SCION has two security mechanisms. First, there is a PKI that provides certificates for validation of PCBs in the beaconing process, and secondly, SCION cryptographically secures the forwarding path to ensure that packets travel along the selected path. In SCION, each ISD possesses a TRC, which serves as a trust root and enables a separate PKI per ISD. Each ISD has its own trusted CAs, which hand out certificates to the internal ASes. Unlike BGP, SCION therefore avoids global trust roots. By having multiple independent CAs, an ISD can still issue certificates even when one CA is compromised. [14]

In the intra-ISD beaconing process, PCBs are sent from Core ASes downwards to Non-Core ASes inside an ISD. Every AS on the path adds an AS Entry, which describes how traffic should flow through it. Each AS Entry is secured through a signature by the corresponding AS. The signature is computed over the current AS Entry, all previous AS Entries and all previous signatures, thereby effectively chaining the signatures. When an AS receives a PCB, it confirms its validity by checking the last signature through the respective AS's certificate. [8]

By having PCBs always originate from Core ASes, SCION does not have any origin validation like the RPKI. In SCION, prefixes are not advertised and origin validation is therefore not needed. [14]

SCION lets end-users choose the path their packets should travel along, by allowing them to combine their preferred path segments. To ensure that packets stay on the selected end-to-end forwarding path, SCION cryptographically secures the path information through Message Authentication Codes (MACs). These MACs are computed by all ASes of the path in the beaconing process, using each AS's local symmetric key. Every MAC secures a Hop Field which is added to the PCB and is computed the following way (1) [9]:

$$\text{MAC}_i = K_i(\text{SegID} \oplus \text{MAC}_0 \oplus \dots \oplus \text{MAC}_{i-1}, \text{Timestamp}, \text{HF}_i\text{-content}) \quad (1)$$

As can be seen, each MAC is calculated over a chain of all previous MACs and a SegID, which is a random value initially selected by a Core AS. This computation makes the subsequent validation of each MAC more efficient in the packet forwarding process. When an AS

receives a packet for forwarding, it recomputes its MAC and compares it with the corresponding MAC of the forwarding path to verify that the packet is following the intended path. An Accumulator (Acc) optimizes this recomputation by summarizing the SegID and all previous MACs into one value. The Acc is sent along with each packet and needs to be updated at each hop of the path. [9]

4. Security Comparison of BGP and SCION

One of SCION's biggest advantages compared to BGP is that it allows end-users to select a path they want their packets to travel along. This is especially important for national data protection when sending sensitive information related to healthcare, critical infrastructure or the military. BGP routing follows individual routing policies, which often send data across international borders over potentially unsecure hops. [2]

As soon as an end-user selects an end-to-end path, it is included and sent with each SCION packet. This mitigates computationally expensive longest prefix matching at each hop because the next hop is already included. MACs ensure that the chosen path is cryptographically secured. SCION therefore also provides security in the packet forwarding process and not only in path discovery. [9] Since the full path is contained in all SCION packets, SCION offers the option for returning packets to take the same route back, which also ensures a safe response [8]. Furthermore, SCION can be used interoperably with BGP through SCION-IP Gateways, which enable communication between SCION networks and BGP networks. This scenario however, loses SCION's property of cryptographically secured paths. [15]

SCION supports multipathing, which means that every hop always has multiple valid paths available. This gives SCION an advantage compared to BGP because it can switch to an alternative path more quickly, thereby making DOS attacks more difficult. [2]

BGP and SCION have different trust models. BGP's RPKI has global trust roots in all 5 RIR's while SCION's PKI splits its trust into individual ISDs, thereby having no reliance on third-party global CAs. [2]

BGP's security mechanisms are built on top of BGP's functionality and thereby optional and not universally employed. In 2024, only 51% of all prefixes were secured through RPKI-ROAs [6]. Mechanisms like ASPA require every AS on the AS_PATH to have created an ASPA object. Path validation cannot be fully guaranteed unless all ASes use ASPA [16]. SCION does not encounter these problems, as its security mechanisms are integrated from the start and enforced automatically [2].

BGP requires origin validation mechanisms like RPKI-ROA to verify if an AS is allowed to announce a prefix. SCION works fundamentally differently from BGP, as its PCBs always originate from Core ASes and carry path information rather than announcing prefixes. SCION therefore has no origin validation since it is unnecessary [14]. Path validation however is necessary in both SCION and BGP to protect the path discovery processes. In BGP, path validation is optional through extensions like BGPsec or ASPA, in SCION it is mandatory through the signing of AS Entries.

5. Related work

Recent research has further explored the security mechanisms and protocols discussed in this paper. As previously noted, BGPsec faces considerable performance challenges. Reference [6], therefore, presents several algorithms to optimize its path validation process. Another paper [17] analyzes the evolution and adoption of RPKI since its deployment in 2011, and a comprehensive survey [18] categorizes existing research on RPKI measurement studies. ASPA is less effective when it is not universally deployed, so a study [11] evaluates its security guarantees under partial deployment conditions. Furthermore, the performance of the SCION architecture, specifically latency and throughput, has been investigated in [19].

6. Conclusion

BGPsec, RPKI-ROA, and ASPA are optional but much-needed extensions designed to remedy BGP's lack of inherent security. BGPsec suffers from inefficient computing costs and still being vulnerable to attacks like the wormhole attack [4]. RPKI-ROAs are in active use, but their adoption remains limited and ASPA is still in development. These security mechanisms strengthen BGP, particularly against accidental route leaks, but malicious attackers still have various attack possibilities. It is clear that BGP's security extensions are far from ideal. Unlike BGP's optional extensions, SCION's security mechanisms are built-in and automatically enforced across all networks. From a security perspective, SCION clearly has the advantage. However, adopting a new routing standard also depends on factors such as performance and deployability, which lie beyond the scope of this paper.

References

- [1] "What is bgp? | bgp routing explained," <https://www.cloudflare.com/en-gb/learning/security/glossary/what-is-bgp/>, [Online; accessed 8-September-2025].
- [2] "Next-generation internet routing," <https://www.scion.org/about-scion/>, [Online; accessed 8-September-2025].
- [3] "What is bgp hijacking?" <https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/>, [Online; accessed 10-September-2025].
- [4] J. Oesterle, H. Kinkelin, and F. Rezabek, "Challenges with BGPsec," Technical University of Munich, Available: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2022-01-1/NET-2022-01-1_02.pdf, 2021.
- [5] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," Request for Comments: RFC 4271, IETF Datatracker, Available: <https://datatracker.ietf.org/doc/html/rfc4271>, 2006.
- [6] M. Abdelhafez and Y. Fadlalla, "BGPsec Deployment Challenges and Optimization Efforts," *2024 IEEE 22nd Student Conference on Research and Development (SCORED)*, 2024.
- [7] J. Fleury and L. Poinsignon, "Rpki and bgp: our path to securing internet routing," <https://blog.cloudflare.com/rpki-details/>, [Online; accessed 14-September-2025].
- [8] C. de Kater, N. Rustignoli, and S. Hitz, "SCION Control Plane," Active Internet-Draft, work in progress, IETF Datatracker, Available: <https://datatracker.ietf.org/doc/draft-dekater-scion-controlplane/>, 2025.
- [9] C. de Kater, N. Rustignoli, J.-C. Hugly, and S. Hitz, "SCION Data Plane," Active Internet-Draft, work in progress, IETF Datatracker, Available: <https://datatracker.ietf.org/doc/draft-dekater-scion-dataplane/>, 2025.
- [10] "Bgp origin validation," <https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/bgp-origin-validation/>, [Online; accessed 14-September-2025].
- [11] N. Umeda, T. Kimura, and N. Yanai, "The juice is worth the squeeze: Analysis of autonomous system provider authorization in partial deployment," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 269–306, 2023.
- [12] A. Azimov, E. Uskov, R. Bush, J. Snijders, R. Housley, and B. Maddison, "A Profile for Autonomous System Provider Authorization," Active Internet-Draft, work in progress, IETF Datatracker, Available: <https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-profile/>, 2025.
- [13] A. Azimov, E. Bogomazov, R. Bush, K. Patel, J. Snijders, and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects," Active Internet-Draft, work in progress, IETF Datatracker, Available: <https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/>, 2025.
- [14] C. de Kater, N. Rustignoli, and S. Hitz, "SCION Control Plane PKI," Active Internet-Draft, work in progress, IETF Datatracker, Available: <https://datatracker.ietf.org/doc/draft-dekater-scion-pki/>, 2025.
- [15] D. Sieciński, "Traditional Internet vs. SCION Architecture," <https://codilime.com/blog/scion-vs-traditional-internet/>, 2023, [Online; accessed 23-September-2025].
- [16] N. Geng, M. Huang, and Y. Wang, "An Analysis of ASPA-based AS_PATH Verification," Active Internet-Draft, work in progress, IETF Datatracker, Available: <https://datatracker.ietf.org/doc/draft-geng-sidrops-aspa-analysis/>, 2025.
- [17] T. Chung, E. Aben, T. Bruijnzeels, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, R. van Rijswijk-Deij, J. Rula, and N. Sullivan, "Rpki is coming of age: A longitudinal study of rpki deployment and invalid route origins," *Association for Computing Machinery*, p. 406–419, 2019.
- [18] N. Rodday, Ítalo Cunha, R. Bush, E. Katz-Bassett, G. D. Rodosek, T. C. Schmidt, and M. Wählisch, "The resource public key infrastructure (rpki): A survey on measurements and future prospects," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2353–2373, 2024.
- [19] E. Ståhl, "Performance analysis of the scion protocol," KTH Royal Institute of Technology, Available: https://www.academia.edu/97173450/Performance_analysis_of_the_SCION_protocol, 2022.