Zürcher Hochschule
für Angewandte Wissenschaften

Introduction to SCION

Farner Simon

Ergänzende Veranstaltung 1
ZHAW School of Engineering
Schweiz
December 17, 2021

Leitung:
Herr Dr. Stephan Neuhaus
Institut für angewandte
Informationstechnologie

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. In mattis nibh mi, a tristique metus tincidunt in. Integer in efficitur lectus, eget sagittis libero. Nunc non augue id nisi euismod venenatis. Nulla facilisi. Integer bibendum accumsan massa faucibus fermentum. Phasellus euismod viverra elit id pulvinar. Quisque eget augue eleifend, auctor erat tempus, ultricies dolor.

Ut elementum tempus pellentesque. Mauris rhoncus convallis dolor, non tempor lacus euismod non. Quisque elit enim, pulvinar a aliquet non, pharetra imperdiet risus. Vestibulum pharetra sollicitudin lorem, id tristique neque condimentum pharetra. Morbi vitae mauris eu lorem vehicula aliquet. Donec quis consequat lorem. Fusce ut ornare lectus. Integer posuere rhoncus urna in blandit. In maximus rhoncus consequat. Pellentesque eget pellentesque lectus, eget suscipit lorem. In pulvinar sapien nec semper dapibus. Praesent non auctor velit. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nam non nisl pretium, varius ex et, gravida tellus. Quisque ut tincidunt sapien.

Mauris id facilisis risus. Nunc vel leo vestibulum, cursus sem a, eleifend sapien. Praesent faucibus nisi interdum neque fringilla volutpat. Proin ornare sem et mauris scelerisque, ac viverra massa lobortis. Vivamus faucibus, nibh id dignissim cursus, lorem dolor volutpat est, sit amet malesuada augue est sed augue. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nam convallis diam enim, non ultrices odio vestibulum et. Integer in dolor imperdiet massa posuere vulputate. Aenean et convallis mi, ut varius elit. Interdum et malesuada fames ac ante ipsum primis in faucibus.

Donec ullamcorper blandit nibh, nec pellentesque est dapibus nec. Nunc tristique nisl ac scelerisque fermentum. Curabitur at pharetra odio. Praesent vitae eros scelerisque, rhoncus mi nec, elementum dolor. Vivamus eget quam non lacus laoreet vulputate vel et dolor. Vivamus malesuada sodales turpis, sed volutpat felis ultricies at. Cras ullamcorper sem malesuada urna pellentesque laoreet. Maecenas posuere non massa a dapibus. Donec.

Contents

1 Introduction

Today's world is extremely connected, and almost every branch of live heavily depends on the constant availability and security of data connections. What the social and economic impact of just a brief and local outage is, is hard to tell, and becomes even harder to grasp if one considers a global outage going on for hours or days at a time. As individuals, we seldom experience outages, which may lead one to the assumption that the internet is a reliable and highly available construct. However, upon closer inspection we are forced to the conclusion that it is neither engineered with that goal in mind, nor does it provide this quality practice. Furthermore, at least since the Snowden revelations, we also know that security, privacy, and trust are in an even more fragile state than the Internet's availability.

These shortcomings are deeply rooted in the architecture of the internet, since it has now grown far beyond the wildest assumptions at the time of its inception in the 1970s. When the internet and its core protocols were designed nobody cloud imagine the eventual scale it would reach, further solving the technical challenge of connecting computers over long distances reliably took precedence over matters like security and efficiency. In fact, making it work at all was seen as a major achievement. By the early 1990s, the internet as we know it today has come together. Since then, it has evolved little, and if so reluctantly. As a consequence, the current protocols are no longer up to the task of managing the scale and complexity of the internet, nor navigating the modern threat landscape.

In this paper, we give an introduction to *scalabilitiy, control, and isolation on next-generation networks* also known as SCION. The project aims to provide a clean slate reengineering of the core Internet infrastructure, in order to solve some of the most pressing concerns which plague the modern global internet. This paper will outline inherent shortcomings of the current, mostly BPG based, internet architecture and examine how SCION proposes to solve said challenges. We will explore the concepts contained in the suggested solution, as well as comparing SCION to BGP in multiple aspects. Our findings will be present in an easy-to-read form for fellow professionals familiar with the fundamentals of networking, but unfamiliar with SCION, thus giving an introduction into the subject.

2 Problem Analysis

In this section, we will analyse the current the global internet architecture and point out its current flaws and challenges. We establish a set of quality metrics and set the expectations regarding these metrics an internet architecture must meet, in order to fulfil the requirements the modern scale of the Internet poses.

2.1 The Global Internet

Many protocols and technologies are involved in transporting information from point A to point B in a computer network. However, the core protocols and services which are responsible for inter

AS communication and thus constitute what we will call the global internet, may be narrowed down to the following:

- Internet Protocol (IP): Provides addressing of devices and enables forwarding of data packets.
- Border Gateway Protocol (BGP): Provides route discovery [1]
- Domain Name System (DNS): Provides resolution between domain names and IP addresses.
- TLS Public Key Infrastructure (PKI): Provides cryptographic binding between names and an entity's public keys.

2.2 Quality Metrics

Now that we know what set of technologies we include in the discussion, it must also be defined what measures of quality we are concerned with and what the expectations are regarding these quality measures. Here again there are plenty of metrics to choose from. First and foremost we want to have availability —if a resource is unreachable, all bets are off. As a reference point for availability in a vital commination system, we might look at the *plain old telephony system* (POTS). Its availability is estimated to be around 99.999 % NEEDS REF.

Once a resource is available, we want to be able to trust that resource. Trust is hard, manly because meaningful trust is a social and political concept which can only be *conveyed* by technological means, not *generated* by them. As humans, we expect that if any entity is revealed to be untrustworthy or becomes compromised, we can revoke our trust quickly. We also expect that we can choose whom to trust without any out-of-scale repercussions. The current solution to the trust problem is subject of the TLS PKI [2], DNSSEC [3] and BGP Sec [4].

Now that trust is established, we would like to ensure that communication paths cannot be altered between two or more mutually trusted parties. This adds the requirement of data integrity. The current state of the global internet also suggest it would be wise to take scalability and efficiency into account as well. Adding and removing entities should be preferably low cost, quick, disruption free and error free. The same must be true for connection between entities.

The possible reasons why the above qualities may be degraded are manyfold, but here are the ones that are at play on a global scale:

2.3 Shortcomings of the Current Internet Infrastructure

There are many factors that can degrade the service quality we expect from our internet connections; however, the following are the main issues which can and do affect the global internet daily.

- (Distributed) Denial of Service Attacks (DoS)
- Disruptions or poisoning of DNS
- BGP route misconfiguration or high jack
- Physical route failures
- Compromise or corruption of trust roots

Any disruptions or attacks on BGP, DNS or the PKI can cause major degradation of service quality for large parts of the global internet. Currently, there are no borders in place which allow local containment of an issue.

The current protocols and services have only evolved little, which on one hand is a testament to the relative foresight and design rigour applied by their creators. 0n the other hand, are they no longer up to the task of managing the modern scale and complexity of the global internet and the current threat landscape. This becomes evident by the comparatively low availability of the internet. XY calculates the availability of the internet to around 99.9 %. This might seem high at first glance; however, this amounts to around xy seconds per day. Of course, (D)DoS attacks and physical failures in the carrier medium are the most obvious causes for outages. However, these tend to be often localized to one or just a few sites, only occasionally causing worldwide effects. In contrast, attacks on the BGP protocol like the route high jack attacks carried out by the Pakistani government against YouTube in 2017 **youtube_highjack** can frequently cause outages on a global scale. Misconfigurations in BGP are typically of similar disruptiveness and have wide-ranging consequences. One recent example is a 6-hour complete outage at Facebook on the xy. October 2021 [5].

Even during normal operations, BGP can cause a disruption of service by temporary dead routes or routing loops, which can occur during route convergence, which can take tens of minutes in extreme cases **route_convergence**.

Managing trust is notoriously difficult. There have been multiple attempts to implement certificate revocation, first with *certificate revocation list* (CRL) [6] and then with *online certificate status protocol* (OCSP) [7] in the past and all of them failed. Not only revoking individual certificates is hard, removing compromised roots of trust is even harder and heavily relies on updating of browsers and operating systems. This can often take days or weeks, or may never happen at all in the case of IoT devices. Taking inspiration from human social behaviour, the natural thing to do may be to drastically shrink the pool of trust roots one relies upon. However, doing this is almost impossible task. For one, the sheer number of available trust roots is immense. There is an estimate of 3000 [8] trusted entities an and around 150 roots of trust in the current TLS PKI. For the other, assessing them all reliably and continuously is an immense undertaking. Furthermore, removing a valid trust root which an individual user deems untrustworthy, my render numerous resources on the internet untrusted and thus inaccessible. This serves to illustrate that the current trust model neither works, nor scales well.

Finally, the question of scaleability and efficiency must be addressed. The current method by which available routes are propagated in BGP potentially requires a route-change to be propagated to every edge router of every AS on the entire internet. This leads to two problems: 1. Route convergence can take tens of minutes **route_convergence** 2. Routing tables have become extremely large. In fact, routing tables have become so huge that router manufacturer are resorting to purpose-built memory hardware to optimize the longest prefix look-ups required for packet forwarding. This hardware is not only expensive, but also power hungry. This indicates that adding and removing ASes from the internet does not scale well and is expensive. Further, the process is error-prone and insecure, as demonstrated by numerous BGP misconfiguration related outages and route high jacking attacks.

By now, the need for a profound change should have become evident. The current internet architecture does not or only partially provide the qualities its current scale and the surrounding threat landscape demand. Attempts to resolve these issues by evolution through grafting on solutions by extending existing protocols or replacing individual technologies have largely failed, as the current adoption of IPv6 and DNSSEC clearly demonstrate. Although technologies like TLS and BGP Sec have seen partial success, they still suffer from lack of unsolved issues outside their problem scope or incomplete adoption. From this, it follows that a wholistic solution

—revolution instead of evolution —is needed [9]. SCION endeavours to deliver this whole cloth reengineering of the global internet architecture.

3 Method

This paper is based a survey of existing literature. Its main purpose is to digest existing literature into a form easily accessible to other IT professionals familiar with the basics of networking but unfamiliar with SCION.

Literature for this paper was mainly selected from the publications section of the SCION project website [10]. We followed an iterative drill-down approach, in each iteration skimming a handful of papers and selecting some for in-depth study. After skimming the 32 listed publications on the project website, we selected a group of three overview papers covering inception and evolution SCION for in-depth study [11]–[13]. During this in-depth study, we collected references to related and cited works for later review. Having gained a good overview of the topic, we proceeded to repeat this process twice, applying the following the selection criteria:

1. The paper clarifies or enhances existing feature of the SCION architecture.
2. The paper specifies an extension to the SCION protocol to add optional features or properties.
3. The paper treats the implementation on a conceptional level of the SCION architecture.
4. The paper treats a technology or mechanism adopted in SCION.
5. The paper is cited by the authors an important precursor or competitor to SCION.
6. The paper does not treat an implementation of SCION on the code level.
7. The paper does not reference SCION as an implementation detail towards some other goal.

Additionally, Google Scholar [1], the IEEE explorer [2] and Science Direct [3] were all searched by the keywords "SCION internet architecture". All three searcher engines combined turned up around 3000 results which needed to be deduplicated and graded as for their relevance according to the above criteria. Unfortunately, but somewhat expectedly, this search did turn up some interesting related work outside the scope of this paper, but did not bring to light any further literature to be included in our introductory paper.

4 Results

In this section, we present the results of our literature research and describe the current state of the proposed SCION architecture. We examine the anatomy of *Isolation Domains* (ISD) and elaborate how the SCION control and data plane work, as well as examining trust management in SCION and deployment status.

[1] https://scholar.google.com

[2] https://ieeexplore.ieee.org/Xplore/home.jsp

[3] https://www.sciencedirect.com

4.1 Isolation Domains

SCION is designed for easy adoption by current BGP ASes; therefore it adopts and alters some ideas from BGP like the idea of an Autonomous System (AS) which, like in BGP, represents the smallest organizational unit. However, SCION introduces an additional organizational unit called the Isolation Domain (ISD). The structure of an individual ISD is illustrated in 2a.

An ISD shares a common set of operational rules and a set of trust roots. It is expected that ISDs will grow along social, political and economical borders and structures [11]. Landing the technical implementation of an ISD a common legal and contractual framework and social context, from which enforceability and a (for humans) meaningful sense of trust can be derived. To emulate these real-world structures, SCION supports recursive ISDs which inherit trust roots and rules from their parent ISDs [11]. As an example, one might imagine the tier-1 providers in a country forming the ISD core of a country level ISD, which is a member of an ISD representing a larger geopolitical entity like the EU. Inside a country, there might be a group of ASes which have stronger requirements regarding security and trust than the rest of the ISD; thus they may form a subISD inside the subISD of the country. One such example may be military and its associated organizations.

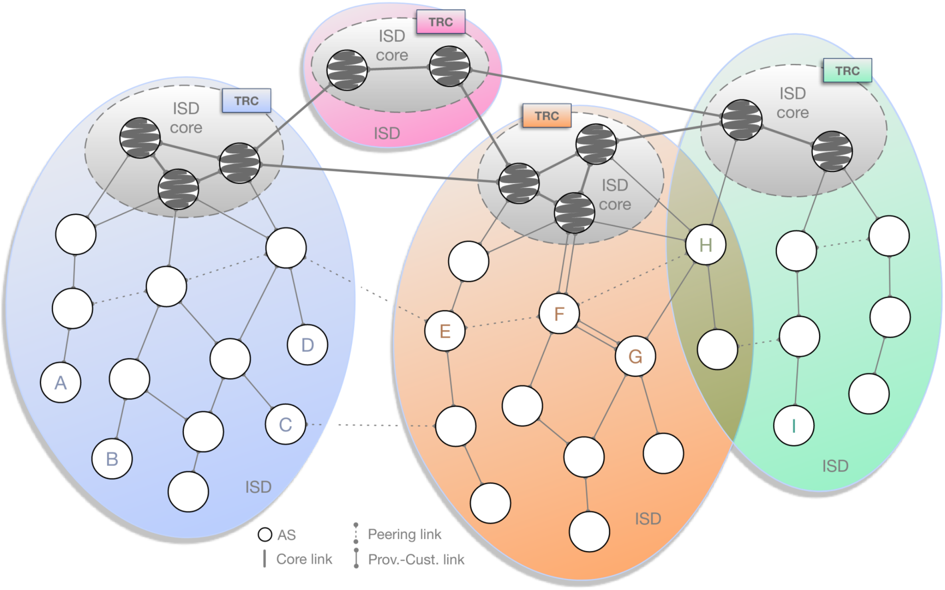

Figure 1: A hypothetical topology of ISDs each with their ISD core and member ASes. Image taken from [12]

4.1.1 IDS Structure

As shown in illustration 2a the main structure of an IDS is an undirected graph formed by a set of core ASes in the ISD core, client ASes, and bidirectional links between individual ASes. ASes may be connected by multiple redundant links. Although a link always carries bidirectional traffic, there is an implied top down hierarchy of providers and consumers between the tiers in the graph. As in BGP a pair of ASes may enter a peering agreement, which is illustrated is a dashed line. Links are also called path segments.

An ISD core is composed of multiple core ASes which form a fully connected clique and a logical unit. The ISD core hosts numerous function such as the ISDs certificate authority, core beacon-, certificate-, path-, and address-servers. The ISD core also maintains the *Trust Root*

Configuration (TRC). Furthermore, the ISD core provides links to other ISDs. Requirement to becoming a core AS is usually sufficient size or importance to offer direct connections to other core ASes in other ISDs, as well as the ability to replicate the other core services listed above [11].

An unassociated AS can join an existing ISD by purchasing connectivity from an ISD which is already member of a given ISD. This requires the joining AS to accept the TRC and operational rules of the ISD it wishes to join. Each AS can be a member of multiple ISDs.

4.1.2 AS and ISD Components

In the following we will explore the components which are required to run an SCION AS and by extension an ISD since each AS usually replicates all or most core services for caching purposes.

SCION ASes look similar too their BGP cousins, so fare as that they have internal and border routers and a set of routes through the AS. These ensure connectivity inside the AS and to neighbouring ASes. Border routers must be SCION capable and must adhere to the common rules agreed upon inside the ISD. However, each AS is free to choose its internal structure, such as the intra domain routing protocol and addressing schema. Initially SCION was designed to employ *Accountable Internet Protocol* (AIP) [11], [14] in all ASes, however this requirement has been relaxed later in favour of interoperability and ease of adoption [12]. Because of the way SCION forwards packets, there is also no need for a uniform addressing schema between ASes (see 4.3).

In addition, each AS needs at least a beacon server, a certificate server and a path server. Beacon servers are responsible for path discovery and are required for beaconing process described in section 4.2.1. Path server are responsible for caching and dissemination of path information. They are involved in path resolution and assembly discussed in section 4.3.2. As SCION makes extensive use of certificates to validate paths and entities [11], certificate servers are deployed to cache and provide certificates in an AS.

A core AS differs from other ASes in several important aspects. Most importantly, core ASes have border routers which are connected to cores ASes in neighbouring ISD. Further, the beacon servers in the core ASes also take part in inter ISD beaconing (see section 4.2.1), thus their path servers also hold path information on how to reach neighbouring ISDs. As mentioned above, the ISD core is responsible for maintaining the trust root configuration (TRC).

The *Trust Root Configuration* (TRC) is the policy which governs the operations of an ISD. The TRC lists the trust roots used in an ISD and thus is the central anchor of trust in an ISD. It is negotiated between the members of the ISD core, and all ASes wishing to join an ISD, need to accept the TRC. Neighbouring ISDs acknowledge an ISDs TRC by signing it. This makes ASes communicating across ISD borders able to trust signatures originating from a neighbouring ISD. Each TRC also holds a number of policies on how the TRC is used and modified. Modifications to the TRC are only possible of multiple core ASes signed the updated TRC, which prevents a rouge core AS from corrupting the TRC. The number of required signatures for different kinds of changes is governed by the policies encoded in the TRC.

4.2 Control Plane

Until now, we looked at the static components which constitute an ISD; however, the real-world internet is not a static thing, so an ISD isn't either. To better manage complexity, SCION is divided into a control plane and a data plane. The control plane is concerned with discovering and maintaining paths, while the data plane uses these paths in the processes of path assembly and packet forwarding. This division not only isolates complexity, but also isolates failures and attacks. As long as there are paths available to forward packets on, the data plane can operate without disruption, even if parts of the control plane are disrupted.

4.2.1 Path Discovery by Beaconing

As mentioned above, SCION has taken inspiration from BGP, the path-discovery mechanism is another place where this is evident. Like in BGP, SCION uses a beaconing process to discover all available paths between ASes. However, unlike in BGP in SCION beacons are not broadcast by every AS to every connected AS, also each AS has control over the paths by which it would like to by reachable. In BGP, an AS has no control over which routes its neighbouring ASes propagate. Beacons in SCION are called *Path-Segment Construction Beacon*s (PCB) and are sent from beacon servers in the ISD core to travel down the ISD graph as a policy constrained multipath flood. [11].

Initially, the path server in a core ISD issues a PCB containing only the exit interface it originates from and the current version number of the TRC. A path server in a neighbouring AS receiving an incoming PCB will first check the validity of the beacon's signature and then proceeds to process the PCB. First the version number of the TRC is checked and if necessary the newest TRC is fetched from the AS it received the PCB from. After adding its own path information to the PCB, the beacon server forwards it to all its client ASes [11].

Before forwarding the PCB, the path server creates a record of the ingress interface, egress interface, and available peers and appends this information to the PCB. These data fields are called *Opaque Fields* and are each protected by a MAC. Important to note is that there is no requirement for other ASes to be able to interpret this field because during packet forwarding an AS only has to read the opaque fields it has created itself (see section 4.3.1). Thus, this field is *opaque* to other ASes.

The new PCB, together with the old PCB information, is cryptographically signed before it is sent out, which leads to an onion like structure of signatures, protecting each step in the forwarding chain from tampering [11]. In this way, a PCB accumulates verifiable path information as a so called path-segment while it is forwarded through the ISD. The information received in PCBs is cached in the local path servers, so end hosts in an ISD have a way to look up path information. Important to note is that PCBs are not sent out through peering links, as this would lead to duplicate paths or might lead to intra-ISD beacons leaking into other ISDs.

PCBs travelling down collect what are called down-paths, but since all paths forward packets bidirectionally, each down-segment can be converted into an up-segment by inverting the order or traversed ASes. This one way propagation of PCBs has an important consequence: An AS always knows an up-path back to the ISD core, but it does not know how to reach other AS or ISDs, thus down-paths to other ASes must always be queried from the paths servers in the ISD core. Once an AS has received a number of path-segments, it can register some of them as down-paths segments with the core path servers in the ISD core. This gives an AS control over which down-paths are made available to other ASes, and creates the unique ability to control by which paths it wishes to be reached.

When selecting down-paths, an AS tries to select as diverse paths as possible in order to reach maximum redundancy. This makes SCION an inherently multipathed system. Apart from path diversity, ASes can select for a number of different quality measure in their paths like low latency or anonymous forwarding capability along the whole path [11].

So fare, we have looked at intra ISD path discovery. Inter ISD path discovery works much the same way; however, the PCBs are only forwarded between core ASes.

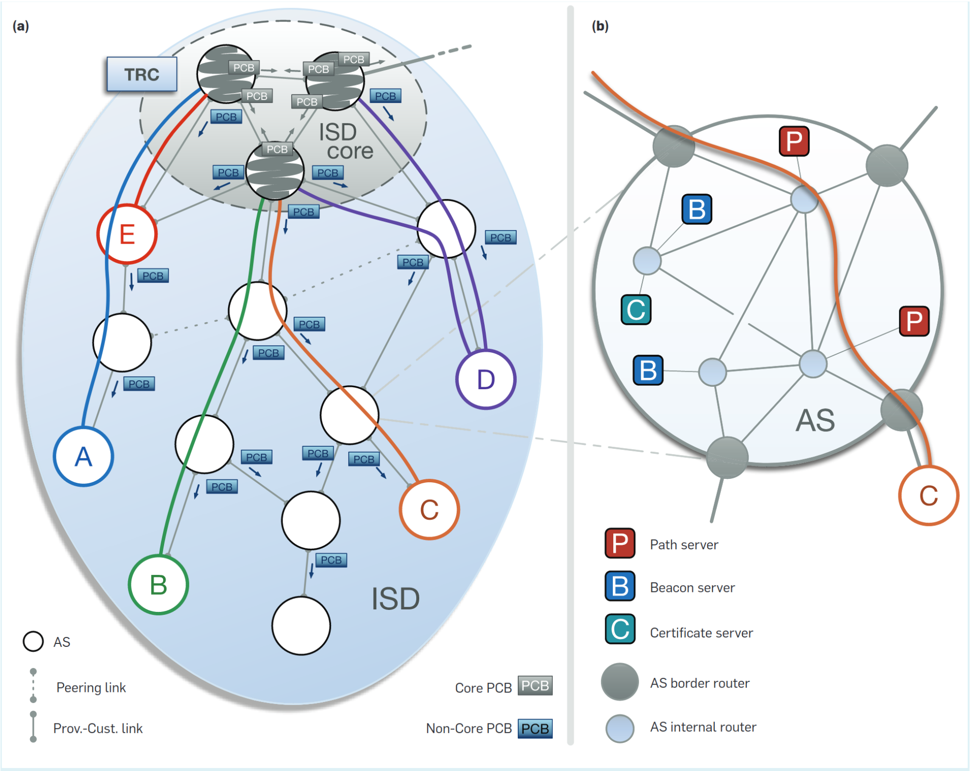

Figure 2: Internal structure of an ISD. Image taken from [12]

4.2.2 SCION Message Control Protocol

The control plane comes with its own control protocol, the *SCION Message Control Protocol* (SCMP). As its name already suggests, it operates quite similar to the already established ICMP protocol and serves many of the same functions [12]. One noteworthy aspect of SCMP is that, in contrast to its cousin, it is integrity protect. For efficiency reasons, a MAC generated by a per-AS symmetric key is preferred over digital signatures. In the event a transit AS needs to send a SCMP message to a source AS, the per-AS key is generated on demand using the *Dynamically Recreatable Keys* (DRK) algorithm and a common secret key shared among the ISDs border routers. The source AS (of the packet which caused the SCMP message) can then fetch the key from the transit AS sending the SCMP message, in case it does not already have it cached [12].

4.3 Data Plane

While the control plane deals with path discovery, the data plane deals with forwarding data packets. For this task, the data plane uses the path information supplied by the control plane to assemble paths.

4.3.1 Packet Carried Forwarding State

In SCION, information needed to reach a forwarding decision for a given packet is stored in the packet itself. This is referred to as *Package Carried Forwarding State* (PCFS) and several interesting properties of SCION are derived from this. Each packet at least contains a path, since source and destination addresses are optional, if the path is unambiguous in its context. Consequently, during forwarding, a router only needs to read the opaque field in the path and check its MAC in order to forward the packet to the next AS. Since all routing information is carried by the packet, the need for routing tables is eliminated.

SCION splits the addressing information of a resource into a locator (the path) and an identifier (the destination address), which facilitates another interesting feature: Only the destination AS needs to be able to interpret the destination address. This allows each AS to choose its own addressing schema. As a consequence, e.g., IPv4 and IPv6 hosts can talk directly to each other using SCION.

The absence of routing tables simplifies the routings process and thus allows the construction of simpler and more energy-efficient machines. XY have observed a gain of xx energy efficiency compared to traditional BGP routing. Thanks to hardware acceleration of cryptographic operations through technologies like Intel AES-NI, forwarding decisions in SCION become faster than in BGP. All a router needs to do is checking the validity of the path recorded in the packet and read the exit interface from it. If hardware acceleration is available, the signature validation is so efficient, it outperforms memory look-ups a BGP router needs to perform to reach its routing decision.

4.3.2 Path Combination

Path combination is the process performed by an end host to obtain a valid path before sending a packet. Up to three path-segments are combined into an end-to-end path. First, the end host looks up the AS and address of the destination with a name server. Then it queries a path server for a path to this destination. After the look-up process is complete, one of five scenarios will play out, depending on where the destination is located:

- **On path** (as shown in figure 2a $A \rightarrow E$) the destination lies directly on the up-path to the ISD core. The path is valid without any further processing. The up-path is truncated at the destination AS.

- **Direct combination** (as shown in figure 2a $B \rightarrow D$) The path can be constructed by chaining an up-segment with a down segment. The up- and down-segment intersect in a core AS.

- **AS shortcut** (as shown in figure 2a $B \rightarrow C$) This scenario is similar to the direct combination, but the destination lies on a down-segment which intersects the up-segment in a none core AS on the way to the ISD core. The unused segments up to the ISD core and back down to the intersection point are discarded.

- **Core path combination** (as shown in figure 2a $A \rightarrow D$) A up- and down-path do not intersect at any point and need to be connected by a core path-segment. This can either be an intra ISD or inter ISD path. This is one of three ways of traversing ISD borders.

- **Peering shortcut** (as shown in figure 2a $A \rightarrow B$) The up-segment and the down segment are connected by a peering link, such that the peering link allows a shortcut to the destination. Analogous to the AS shortcut, in this case the extraneous path segments are discarded as well. Note that this type of shortcut can also traverse ISD borders.

Once the host has constructed a path, it is encoded as PCFS in the packet header. The destination host can either take the path contained it the received packet and simply reverse it, or perform its own lookup and combination process. Of course, this process is assisted by various cashing mechanisms.

4.3.3 Source Routing and Path Transparency

One of SCION's biggest claims to fame is its secure and efficient implementation of source routing. Source routing means that the source of a data packet determines the route the packet will travel along to its destination. The path construction process described in the previous section is performed on the end host sending a data packet providing exactly this source routing feature. The path information is stored as PCFS data (see section 4.3.1) in the packet header and is cryptographically protected against tampering. This not only guarantees that the packet will be routed on the selected path, but also creates path transparency for the destination end host.

4.4 Isolation of Attacks

SCION carves the global internet up into smaller self-contained units through ISDs, and even these can be subdivided into subISDs. This by itself already provides a significant advantage, since all entities outside an ISD cannot influence the path discovery process (see section 4.2.1). Further, the compromise of a trust roots is isolated to an ISD as well and may not affect other ASes in other ISDs.

Attacks are further isolated in that no AS can influence the path construction process (see section 4.3.2) taking place on an end host. A malicious AS can only announce down-paths to reach that malicious AS. PCFS information is MAC protected, the chosen path for a packet cannot be altered by a malicious AS on the path.

4.5 Trust Management and Trust Agility

As stated in the introduction, trust management is a hard problem to solve, and SCION takes a few important steps towards solving this problem. First of all the architecture limits the scope of trust to a smaller set of trustees by introducing ISDs, secondly it reduces the number of trust roots to a manageable number [11]. This makes key revocation, or certificate revocation respectively, much more feasible. There is no need for every single end host on the entire Internet to be informed individually. SCION also makes extensive use of trust transitivity offered by digital signatures.

Trust agility is the concept that the user can choose which roots of trust they relay upon and that they can revoke their trust, quickly and effectively, if an entity is compromised. This requires a simple and quick key revocation process, which SCION aims to provide this by effectively avoiding two scenarios:

- **Trust monopoly**: All the entities on the internet need to trust one root of trust, like in DNSSEC or BGP Sec. This scenario suffers from having a single point of failure, and revoking a key in this system is going to create an administrative nightmare that affects the whole infrastructure.
- **Trust oligopoly**: In this scenario, there is a multitude of equally trusted roots of trust. An example for this is the current TLS PKI system. This scenario suffers from the fact that it exposes many points of failure, and that each trust root can sign certificates for arbitrary entities. Revoking keys is made difficult by the sheer number of keys to manage. This trust model is only as strong as its weakest link.

This is achieved by introducing a hierarchy of trust. [11]. ASes use several different keys for different purposes and can replace the keys and employed algorithms autonomously. However, the used keys always require a signature by a trust root. This enables neighbouring ASes and end host in different ASes or ISDs to check the validity of the keys and by extensions the data processed by these keys. The keys used for this signing are encoded in the TRC and are thus managed and protected by the ISD core.

In SCION, trust is rooted in a low number of trust roots, which are encoded in each ISDs TRC. This TRC is only valid inside the ISD it applies to, thus limiting the scope of trust to one ISD. Since linked ISDs signed each other's TRCs trust is conveyed, by the transitive properties of trust, between ISDs. If an ISD revokes a trust root's key, all keys signed with it, become invalid at once. This change propagates quickly through the ISD own ASes as well as to neighbouring ISDs by the means of PCBs. From this, an interesting property emerges: As long as there is a path available to a given resource, the path can always be validated.

5 SCION Extensions

When SCION was first conceptualized, the idea was to incorporate all needed features in a holistic design. However, the authors acknowledged the need for SCION to be extensible, since not all features are vital to SCIONS proper operation. We will have a brief look at some of the more noticeable ones here.

Through source routing, SCION already allows an end host to route around ASes it does not trust [11]; however, this is insufficient protection if a sender wants to remain truly anonymous. Therefore, XY et al. propose the *High-speed Onion Routing at the Network-Level* [15], [16] or HORNET extension, which aims to add onion routing [17] to the protocol. The opaque fields and PCFS feature of SCION make it uniquely suited to onion routing, since an AS only needs to be able to read the opaque field it itself has created and does not depend on any knowledge about the preceding and following ASes in the path.

The SCION protocol already offers defences against DDoS attacks by giving ASes the ability to keep some down paths hidden until they are needed in an emergency [12]. To further harden SCION against DDoS attacks, Basescu et al. propose the *Scalable Internet Bandwidth Reservation Architecture* [18] or SIBRA extensions. The extension introduces defences against link-flooding attacks such as Coremalt [19] and Crossfire [20] attacks, which aim to degrade the performance of backbone links or the target itself by overwhelming them with what looks like legitimate traffic. SIBRA combats DDoS attacks by a combination of contractual agreements for bandwidth reservation and technical measures to enforce these reservations [18].

SCION is designed with easy adoption in mind and offers a number of attractive benefits to adopters. Design elements such as the use of existing ASes and isolating the inner structure of an AS from the SCION architecture are specifically targeted at easy adoption of SCION. For an AS to adopt SCION, it only needs to deploy border routes which are SCION capable, as well as deploying name, beacon, certificate, and path servers. All these can run on commodity hardware, while the rest of the AS can remain largely unchanged. Since core elements from BGP are adopted like ASes and beaconing, BGP routing policies can be fully expressed and even extended in SCION, further lowering the bar of entry to adopting SCION [13].

Since 2016 a real-world SCION test bed called ScionLab is operational [21] which includes several high-profile members such as Swisscom and Switch, as well as other financial institutions like SIX and the Swiss National Bank [22] and further academic institutions. In fact, as of 2020, the test bed serves over 600 entities and spans a global network around 40 ISDs.

6 Discussion

After we have looked at the components and processes which constitute the SCION architecture, in this section we discuss how SCION manages to provide the quality metrics defined in the introduction (see section 1) and look at further emergent properties of the architecture.

6.1 Availability

SCION incorporates multiple direct design decisions which work towards improving availability of the network, as well as other properties of the design which indirectly contribute towards that goal.

In SCION's down-path registration mechanism makes SCION inherently multipathed, since each AS may register multiple down-paths with the core path servers. This control over down paths also allows an AS to select down paths for their reliability, and may select paths in a way to avoid unreliable ASes. Further, the end host may take reliability into account during path construction as well. Finally, each packet carries its routing information in the packet header and the source may select a path on a per-packet basis, making use of the multipathed nature of SCION.

The high path freshness by guaranteed by SCION's regular beaconing process further works in favour of availability, since valid and working paths are propagated through an ISD every few seconds. Physical route failures are detected quickly and reconfigurations are propagated quickly, without the potential for temporary loops or any delays due to prolonged waiting times for route convergence.

Indirect contributors to availability are of course the improved security and isolation properties is SCION. Misconfigurations can no longer spread outside an ISD, nor can attacks. The split of data and control plain further improves availability by making sure that the data plane may continue to function, even when the control plane is disrupted.

6.2 Trust Management

An effort is made to move the trust model in SCION towards one which is more meaningful to humans, than the current ones at work in TLS PKI, DNSsec or BPGSec. This achieved first and for most by drastically reducing the cycle of trust by reducing the number of trust roots a user needs to rely upon through the introduction of ISDs. This in turn enables trust agility by making quick and effective key revocation feasible. Furthermore, ISDs are engineered to model and conform to existing trust boundaries derived from political and commercial real-world structures. At the same time, the single point of failure problem is avoided by introducing accountability into the management of trust roots through the implementation of ARPKI [23], [24].

6.3 Data Integrity and Accountability

While SCION leaves data integrity and data privacy of the actual payload data to other layers, host of cryptographic measure are employed to ensure the data it produces and consumes can not be tampered with. PCBs are signed each time they are forwarded, so a malicious AS can not alter any part of a received PCB, nor can it advertise links it has no rights to without detection. A misbehaving AS can always be attributed by its signature and can either circumvent by source routing or its keys revoked by the ISD core.

Since routing information is contained in each packet header, this needs to be protected as well. SCION protects each entry in the opaque field of each path-segment with a MAC, produced by a per AS key. This means a malicious as cannot alter the opaque fields generated by other ASes.

By implementing ARPKI the certificate authority and by extension the TRC become tamper prove as well, as an attacker always needs to compromise majority core ASes to be able to approve actions which alter the TRC.

6.4 Scalability and Efficiency

As proposed in the introduction scalability depends on how easy it is to add and remove entities from a structure and how far these changes must propagate within the structure. SCION manages to keep changes simple and local by introducing ISDs. For a hypothetical worldwide deployment, it is expected that there will eventually be around 6 to 10 [11] top-level ISDs, each subdivided into smaller subISDs. Consequently, adding and removing ISDs on any level is strictly contained to the new ISDs peers and its parent.

Adding and removing ASes from an ISD is contained similarly. As described in 4.1.2 an AS joins an ISD by purchasing connectivity from an AS which is already a member of the ISD the AS wishes to join. So, the only entities involved are one or multiple provider ASes and the ISD core, which needs to register the new paths in its path servers and sign the new ISD's keys.

A massive boon for efficiency is the fact, that SCION removes the necessity of routing tables in border routers, by storing forwarding information in the packet header. Current BGP routers use specialized memory architectures to store the ever larger routing tables and perform prefix matching at acceptable speed. This special hardware is not only expensive but also power hungry. When comparing BGP and SCION routers in a simulation, Chen et al. postulate an overall power saving of at least 16 %. They also find that the impact of larger packet headers due to the PCFS information is neg liable [25].

7 Related Work

Xin Hhang et al. lay to ground work in specifing SCION in their 2011 paper titled "SCION: Scalability, Control, and Isolation On Next-Generation Networks " [11]. This paper is later updated an referenced in a follow-up paper in 2015 where Barrera et al. who revisit SCION [12], while in their 2017 they give a detailed and update overeview in the Communiction of the ACM [13]. Multiple extension to the SCION protocol were proposed as follows. Onion routing was introduced through an extension discribed by Chen et al. [15], [16] and effective defences against DDoS attacks are discussed by Basescu et al. [18], Lee et al. [26] and Rothenberger et al. [27].

Since SCION heavily relies on multiple PKI systems therfore Basin et. all propose [23] and implement [24] an attack resilient PKI model. In order to simplify and better secure the PKI duties which come with operating a SCION IDS Matsumote et. al. introduce "CASTLE: CA Signing in a Touch-Less Environment" [28]

Ding et al. analyse five next-generation networking including SCION and compare them in 2016 study persented during in IEEE Access [29] and Know et al. present their findings from a real world test bed runing since 2016 ICNP 2020 [21]. A study by Giacomo et al. even suggests potential applications for SCION based networks in currently emerging internet satelite constalations.[30]

8 Conclusion

We have given an introduction to the SCION internet architecture in a form accessible to fellow interested professionals. We have laid out the challenges posed by the current and future scale of the global internet and defined a basic set of quality metrics to be fulfilled. We then proceeded in showing that current internet architecture is unable to provide these to a satisfactory level, and followed to state our case in support of the necessity for profound change. Subsequently, we explored the concepts of new internet architecture proposed by SCION and explained its operation, benefits, and security properties. Finally, we discussed why and how SCION is able to fulfil our defined quality metrics.

9 Indicies

References

[1] Y. Rekhter, S. Hares, and T. Li, *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271, Jan. 2006. DOI: `10.17487/RFC4271`. [Online]. Available: `https://rfc-editor.org/rfc/rfc4271.txt`.

[2] S. S. Wu, R. V. Sabett, D. S. Chokhani, D. W. S. Ford, and C. (R. Merrill, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, RFC 3647, Nov. 2003. DOI: `10.17487/RFC3647`. [Online]. Available: `https://rfc-editor.org/rfc/rfc3647.txt`.

[3] Y. Rekhter, S. Hares, and T. Li, *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271, Jan. 2006. DOI: `10.17487/RFC4271`. [Online]. Available: `https://rfc-editor.org/rfc/rfc4271.txt`.

[4] ——, *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271, Jan. 2006. DOI: `10.17487/RFC4271`. [Online]. Available: `https://rfc-editor.org/rfc/rfc4271.txt`.

[5] B. Barrett, "Why facebook, instagram, and WhatsApp all went down today," *Wired*, Apr. 10, 2021, Section: tags, ISSN: 1059-1028. [Online]. Available: `https://www.wired.com/story/why-facebook-instagram-whatsapp-went-down-outage/` (visited on 12/17/2021).

[6] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC 5280, May 2008. DOI: `10.17487/RFC5280`. [Online]. Available: `https://rfc-editor.org/rfc/rfc5280.txt`.

[7] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and D. C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, RFC 6960, Jun. 2013. DOI: `10.17487/RFC6960`. [Online]. Available: `https://rfc-editor.org/rfc/rfc6960.txt`.

[8] (Aug. 3, 2010). "The EFF SSL observatory," Electronic Frontier Foundation, [Online]. Available: `https://www.eff.org/observatory` (visited on 12/17/2021).

[9] R. P. Munroe. (). "Xkcd 927: Standards," xkcd, [Online]. Available: `https://xkcd.com/927/` (visited on 12/12/2021).

[10] (). "SCION internet architecture," [Online]. Available: `https://scion-architecture.net/` (visited on 12/11/2021).

[11] X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig, and D. G. Andersen, "SCION: Scalability, control, and isolation on next-generation networks," in *Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*, May 2011.

[12] D. Barrera, R. M. Reischuk, P. Szalachowski, and A. Perrig, "SCION five years later: Revisiting scalability, control, and isolation on next-generation networks," p. 21,

[13] D. Barrera, L. Chuat, A. Perrig, R. M. Reischuk, and P. Szalachowski, "The SCION internet architecture," *Communications of the ACM*, vol. 60, no. 6, pp. 56–65, May 24, 2017, ISSN: 0001-0782, 1557-7317. DOI: `10.1145/3085591`. [Online]. Available: `https://dl.acm.org/doi/10.1145/3085591` (visited on 10/18/2021).

[14] D. G. Andersen, H. Balakrishnan, N. Feamster, T. Koponen, D. Moon, and S. Shenker, "Accountable internet protocol (AIP)," p. 12,

[15] C. Chen, D. E. Asoni, D. Barrera, G. Danezis, and A. Perrig, "HORNET: High-speed onion routing at the network layer," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver Colorado USA: ACM, Oct. 12, 2015, pp. 1441–1454, ISBN: 978-1-4503-3832-5. DOI: 10.1145/2810103.2813628. [Online]. Available: https://dl.acm.org/doi/10.1145/2810103.2813628 (visited on 11/30/2021).

[16] D. E. Asoni, C. Chen, D. Barrera, and A. Perrig, "On building onion routing into future internet architectures," in *Open Problems in Network Security*, J. Camenisch and D. Kesdoğan, Eds., vol. 9591, Series Title: Lecture Notes in Computer Science, Cham: Springer International Publishing, 2016, pp. 71–81, ISBN: 978-3-319-39027-7 978-3-319-39028-4. DOI: 10.1007/978-3-319-39028-4_6. [Online]. Available: http://link.springer.com/10.1007/978-3-319-39028-4_6 (visited on 11/30/2021).

[17] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482–494, 1998. DOI: 10.1109/49.668972.

[18] C. Basescu, R. M. Reischuk, P. Szalachowski, A. Perrig, Y. Zhang, H.-C. Hsiao, A. Kubota, and J. Urakawa, "SIBRA: Scalable internet bandwidth reservation architecture," in *Proceedings 2016 Network and Distributed System Security Symposium*, San Diego, CA: Internet Society, 2016, ISBN: 978-1-891562-41-9. DOI: 10.14722/ndss.2016.23132. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2017/09/sibra-scalable-internet-bandwidth-reservation-architecture.pdf (visited on 11/30/2021).

[19] A. Studer and A. Perrig, "The coremelt attack," in *Computer Security – ESORICS 2009*, M. Backes and P. Ning, Eds., vol. 5789, Series Title: Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 37–52, ISBN: 978-3-642-04443-4 978-3-642-04444-1. DOI: 10.1007/978-3-642-04444-1_3. [Online]. Available: http://link.springer.com/10.1007/978-3-642-04444-1_3 (visited on 12/17/2021).

[20] Min Suk Kang, Soo Bum Lee, and V. D. Gligor, "The crossfire attack," in *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA: IEEE, May 2013, pp. 127–141, ISBN: 978-0-7695-4977-4 978-1-4673-6166-8. DOI: 10.1109/SP.2013.19. [Online]. Available: http://ieeexplore.ieee.org/document/6547106/ (visited on 12/17/2021).

[21] J. Kwon, J. A. García-Pardo, M. Legner, F. Wirz, M. Frei, D. Hausheer, and A. Perrig, "SCIONLAB: A next-generation internet testbed," in *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, ISSN: 2643-3303, Oct. 2020, pp. 1–12. DOI: 10.1109/ICNP49622.2020.9259355.

[22] "SNB and SIX launch the communication network secure swiss finance network," p. 1,

[23] D. Basin, C. Cremers, T. H.-J. Kim, A. Perrig, R. Sasse, and P. Szalachowski, "ARPKI: Attack resilient public-key infrastructure," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottsdale Arizona USA: ACM, Nov. 3, 2014, pp. 382–393, ISBN: 978-1-4503-2957-6. DOI: 10.1145/2660267.2660298. [Online]. Available: https://dl.acm.org/doi/10.1145/2660267.2660298 (visited on 11/30/2021).

[24] ——, "Design, analysis, and implementation of ARPKI: An attack-resilient public-key infrastructure," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 3, pp. 393–408, May 1, 2018, ISSN: 1545-5971. DOI: 10.1109/TDSC.2016.2601610. [Online]. Available: https://ieeexplore.ieee.org/document/7547899/ (visited on 11/30/2021).

[25] C. Chen, D. Barrera, and A. Perrig, “Modeling data-plane power consumption of future internet architectures,” in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, Pittsburgh, PA, USA: IEEE, Nov. 2016, pp. 149–158, ISBN: 978-1-5090-4607-2. DOI: 10.1109/CIC.2016.031. [Online]. Available: http://ieeexplore.ieee.org/document/7809702/ (visited on 12/09/2021).

[26] T. Lee, C. Pappas, A. Perrig, V. Gligor, and Y.-C. Hu, “The case for in-network replay suppression,” in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi United Arab Emirates: ACM, Apr. 2, 2017, pp. 862–873, ISBN: 978-1-4503-4944-4. DOI: 10.1145/3052973.3052988. [Online]. Available: https://dl.acm.org/doi/10.1145/3052973.3052988 (visited on 11/30/2021).

[27] B. Rothenberger, D. Roos, M. Legner, and A. Perrig, “PISKES: Pragmatic internet-scale key-establishment system,” in *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, Taipei Taiwan: ACM, Oct. 5, 2020, pp. 73–86, ISBN: 978-1-4503-6750-9. DOI: 10.1145/3320269.3384743. [Online]. Available: https://dl.acm.org/doi/10.1145/3320269.3384743 (visited on 11/30/2021).

[28] S. Matsumoto, S. Steffen, and A. Perrig, “CASTLE: CA signing in a touch-less environment,” in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, Los Angeles California USA: ACM, Dec. 5, 2016, pp. 546–557, ISBN: 978-1-4503-4771-6. DOI: 10.1145/2991079.2991115. [Online]. Available: https://dl.acm.org/doi/10.1145/2991079.2991115 (visited on 11/30/2021).

[29] W. Ding, Z. Yan, and R. H. Deng, “A survey on future internet security architectures,” *IEEE Access*, vol. 4, pp. 4374–4393, 2016, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2016.2596705.

[30] G. Giuliari, T. Klenze, M. Legner, D. Basin, A. Perrig, and A. Singla, “Internet backbones in space,” *ACM SIGCOMM Computer Communication Review*, vol. 50, no. 1, pp. 25–37, Mar. 23, 2020, ISSN: 0146-4833. DOI: 10.1145/3390251.3390256. [Online]. Available: https://dl.acm.org/doi/10.1145/3390251.3390256 (visited on 11/30/2021).

List of Figures

List of Tables