Zürcher Hochschule
für Angewandte Wissenschaften

Introduction to SCION

Farner Simon

Ergänzende Veranstalitung 1
ZHAW School of Engineering
Schweiz
December 12, 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

Todays 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 inpact of an 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 hourse or days at a time. As individuals we seldomly 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 enigneered with that goal in mind, nor does it provide this quality an practice. Further more, at least since the Snowden revelations, we also know that security, privacy and trust are in even more fragile state than the internets availability.

These shortcommings are deeply rooted in the arichtecture of the internet, since it has now grown far beyond the wildest assumptions at time of its insception in the 1970s. When the internet and its core protocols were designed nobody cloud imagine the eventual scale it would reach, also solving the technical challenge of connecting computers over long distances reliably took presedence over matters like security and efficiency. In fact getting it to 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 todays protocols are no longer up to the task of managiging 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* . A project which aims to provide a clean slate reengineering of the core interntet infrastructure, in order to solve some of the most pressing concerns which plague the modern global internet. This paper will outline inherent shortcommings of the current, mostly BPG based, internet architecture and examine how SCION proposes to solve said challanges. We will explore the concepts contained in the proposed solution as well, as comparing SCION to the BGP in multiple aspects. Our findigs will be present in a easy to read form for fellow professionals familiar with the fundamentals of networking, but unfamiliar with SCION, thus giving an introduction into the subjectmatter.

2 Problem Analysis

In this chapter we will analyse the current structure of the global internet architecture and point out it current flaws and challenges. We establish a set of quality metrics we expect from the global internet to meet our modern needs

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

- Internet Protocol (IP): Provides adressing of devices and enables forwarding of data packets.
- Border Gateway Protocol (BGP): Provides route discovery **rfc_bgp**
- Domain Name System (DNS): Provides resolution between domain names and ip addresses.
- TLS Public Key Infrastructure (PKI): Provides cryptographic binding between names and an entities public keys.

2.2 Quality Metrics

Now that we know what set of technologies we include in the discussion, it must also be definded 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 availablity in a vital cummications system we might look at the *plain old telephon systems* (POTS). Its availablilty is generally estimated to be around 99.999 % NEEDS REF.

If 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 techonlogical means, not generated by them. We expect that if any entity is reveiled to be untrustworthy or becomes compromised, we can revoke our trust quickly. We also expect that we can choose whom to trust with any out of scale reprecussions. The current solution to the trust problem is subject of the TLS PKI **tls_pki**, DNSSEC **dnssec** and BGP Sec **bgpsec**.

Once trust is established we would like to ensure that communictain paths can not be altered between two or more mutualy trested 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 Shortcommings 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 on a daly basis.

- (Distributed) Denial of Service Attacks (DoS)

- Disruptions or poisoning of DNS
- BGP route missconfiguration 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 degredation of service quality for larg 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 designe rigour applied by their creators, on the other hand are they no longer up to task of managing todays scale and complexity of the global internet and the modern threat landscape. This becomes evident by the comparetativey low availablity 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 most obvious causes for outages. However, these tend to be often localized to one or just a few sites, only ocassionaly causing world wide effects. In constrast, attacks on the BGP protocol like the route highjack carried out by the pakistani governement against YouTube in 2017 **youtbe_highjack** can often cause outage on a global scale. Misconfigurations in BGP often are similary disruptive and have wide ranging consequences. One rescent example is a 6 hour complete outage at Facebook on the xy. October 2021 **facebook_oups**.

Even during normal operations BGP can cause a distruption of service by temporary dead routes or routing loops, which can occoure during route convergence, which can take tens of minutes **route_convergence**.

Managing trust is notoriously difficult. There have been multiple attempts to implement certificate revocation, first with *certificate revocation list* (CRL) **rfc_crl** and then with *online certificate status protocol* (OCSP) **rfc_opsc** 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. Taking inspiration from human social behavior the natural thing to do may be to then drastically shrink the pool of trust roots one relys 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 **trusted_entities** trusted enties an and around 150 roots of trust in the current TLS PKI. For the onther, assessing them all relyably and continously is imense undertaking. Furthermore, removing a valid trust root which an individual user deems untrustworthy, my render a large number of resources on the internet untrusted and thus inacessible. This serves to illustrate that the current trust modle neither works, nor does it scale.

Finally the question of scaleablity ond efficency must be addressed. The current method how available routes are propagated in BGP potentially requires a route change to be propagated to every edge router of every AS on the internet. This leads to two problems: 1. Route convergence can take tens of minutes **route_convergence** 2. routing tables have become extremely large. Infact routing tables have become so larg that router manufacturer resort to purpos 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 noumerous BGP missconfiguration related outages and route highjacking attacks.

By now the need for a profounde change should have become evident. The current internet architecture does not or only partially provide the qualties its current scale and the surrounding threat landscape demand. Attempts to resolve these issues by evolution through grafting on solutions by protocol extensions or replacing current individual technolgies have largely failed, as the current adoption of IPv6 and DNSSEC clearly demonstrate. Allthough techonologies like TLS and BGP Sec have seen partial sucess, they still suffer from lack of unsolved issues outside their problem scope. From this it follows that a wholistic solution - revolution instead of evolition - is needed. SCION endevours to deliver this whole cloth reenigineering of the globalt internet architecture.

3 Method

This paper is purely based an survey of existing literature. It's 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 **scion_website**. We followed an itterative drill down approach, in each itteration skimming a handfull of papers and selecting some for indepth study. After skimming the 32 listed publications on the project website we selected a group of three overview papers covering insception and evolution SCION for indepth study [1]–[3]. During this indepth 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 clearifies or enhances excisting 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 an conceptional level of the SCION architecture.
4. The paper treats a techonolgy or mechanism addopted in SCION.
5. The paper is citet by the authors an important precursor or competitor to SCION.
6. The paper does not treat an implemetation of SCION on the code level.
7. The paper does not reference SCION as an implementation detail towards some other goal.

Additionally Google Schoolar **google_scholar**, the IEEE explorer **i3e_explorer** and Science Direct **science_direct** were all searched by the keywords "SCION internet architecture". All three searche engines combined turned up around 3000 results which needed to be dedouplicated and graded as for their relevance according to the above criteria. Unfortunatelty, but somewhate expectedly, this search did turn up some intressitng realted 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 chapter we peresent the results of our literature reseach 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.

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, repesents the smalest organisational unit. However, SCION introduces an additonal organisational unit called the Isolation Domain (ISD). The structure of an indivual ISD is ilustrated in 1a.

An ISD shares a common set of operational rules and share a set of trust roots. It is expected that ISDs will grow along social, political and econmical borders and structures [1]. Giving these technical implemtations a common legal and contractual framework and social context, from which enforcability and a meaningful (for humans) sense of trust can be derived. To emulate these realworld structures, SCION supports recursive ISDs which inherint trust roots and rules from their parent ISDs [1]. As an example one might imagine the tier-1 providers in a country forming the ISD core of a country level ISD, which is member of an ISD representing 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 the ISD, thus they may form a subISD inside the subISD of the country. One such example may be military and its associated organisations.

4.1.1 IDS Structure

As shown in ilustration 1a the main structure of an IDS is an undirected graph formed by a set of core ASes in the ISD core, client ASes and biderectional links between individual ASes. ASes may be connected by multiple redundant links. Although a link always carries biderctional traffic, there is an implied top down hirarchy of providers and consumers between the tiers in the graph. As in BGP a pair of ASes may enter an peering agreement, which is ilustrated is a dashed line. Links are also called path segments.

An ISD core is comprised of multiple core ASes which form fully connected clique and a logical. 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. The ISD core also provides links to other ISDs. The requirement to become 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 repicate the other core services listed above [1].

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

4.1.2 AS and ISD Componants

In the following we will explore the componantes which are required to run an SCION AS and by extension a ISD since an ISD usually replacates all or most core services for caching reasons.

SCION ASes look similar too their BGP cousins so fare as that they have internal routers 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 addhere to the common rules agreed upon inside the ISD, however each AS is free to choos its internal structure. Such as the intra domain routing protocol and adressing schema. Initially SCION was designed to employ *Accountable Internet Protocol* (AIP) **aip_2008**, [1] in all ASes, however this requirement was relaxed later in favour of interoperability and ease of adoption [2]. Because of the way SCION fowards packets, there is also no need for a uniform addressing schema between ASes (see **??**).

In addition each AS needs at least a beacon server, a certificate server and a path server. Beacon servers are responbsible for path discovery and are required for beaconing process described

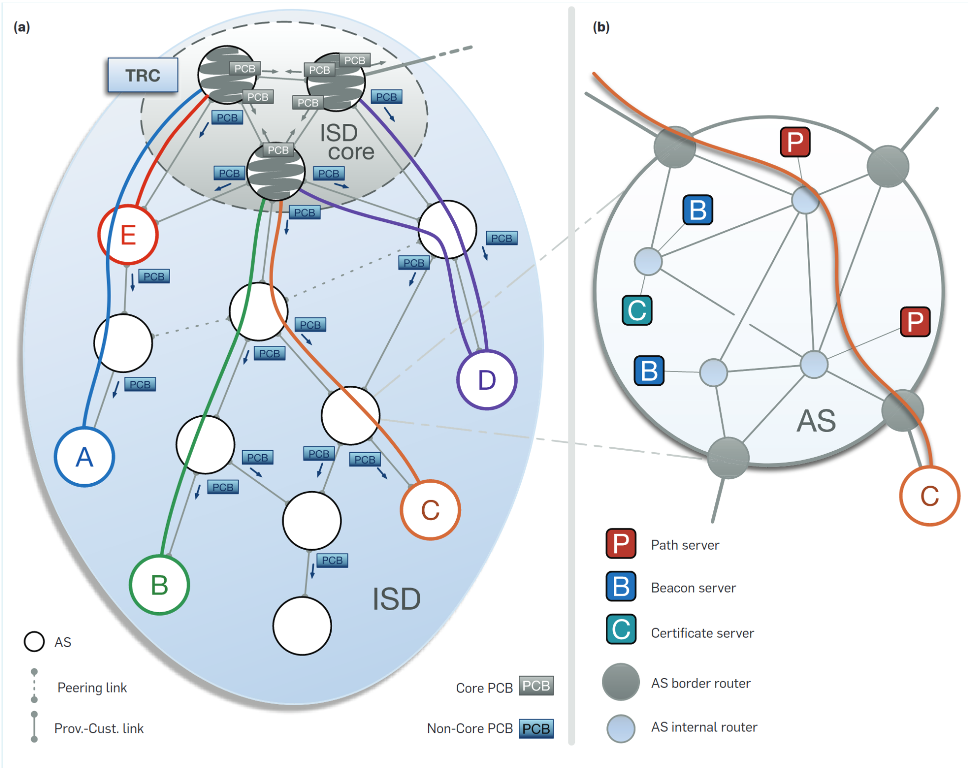

Figure 1: Internal structure of an ISD. Image taken from [3]

in section 4.2.1. Path server are repsonsible for caching and disimination of path information. They are involved in path resolution and assembly discussed in section 4.3.2. As SCION makes extensive us of certificates to validate paths and entities [1], certificate servers are deployed to cache and provide certificates in an AS.

A core AS differs from other ASes in serveral important aspects. Most importantly core ASes have border routers which are connected to cores ASes in neighbouring ISDs. 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 Configuratio* (TRC) is 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 whishing to join an ISD need to accept the TRC. Neighbouring ISDs acknowledge an ISDs TRC by signing it. This makes ASes communicting across ISD bordes able to trust signatures originating from an neighouring ISD. Each TRC also holds a number of policies on how the TRC is used and. Modifications to the TRC are only possible of multiple core ASes signe updated TRC, which prevents a rouge core AS from corupting 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 componants which make up an ISD, however the real world internet is not a static thing, so an ISD isn't either. To better manage complexity SCION is devided into a controll 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 fowarding. This division not only isolates complexity, but also isolates failures. 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 form BGP, the paths discovery mechanism is an other 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 paths 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 travle down the ISD graph as an policy constrained multipath flood. [1].

Initialy 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 incomming CP will first check the validity of the beacon by checking its signature. Then it goes on to process the PCB. First of all the version number of the TRC is checked and if necessary fetch the new TRC from the AS it received the PCB from. After adding its own path information to the PCB, the beacon server forwards the PCB to all its client ASes **??**.

Before forwarding the PCB the path server creates a record of the ingress inteface, egress interface, and available peers and then appends it to the PCB. These fields are called *Opaque Fields* and are each protected by a MAC. Important to note is that only there is no requirement for other ASes to be able to interpret this field, because during packet fowarding an AS only has to read only the 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 chaine from tampering [1]. In this way a PCB accumulates verifyable 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 endhosts 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 douplicate paths or might lead to intra-ISD beacons leaking into other ISDs.

PCBs traveling 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 the 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 segmemts 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 unique ability to control by which paths it whishes to be reached.

When selecting down-paths an AS tries to select as diverse paths as possible in order reach maximum redudancy. This makes SCION an ineherently multipathed system. Apart from path diversity, ASes can select for many different quality measure in their paths like low latency or anonymous forwarding capability along the whole path [1].

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

4.2.2 SCION Message Control Protocol

The control plane comes with its own control protocol the *SCION Message Control Protocol*. As its name allready suggests it operates quite similar to the allready established ICMP protocol and serves many of the same functions [2]. One noteworthy aspect of SCMP is that, in contrast to its cousine, it is integerity protect. For efficiency reasons a MAC generated by a per-AS symetric key is perefered over digital signatures. In the event a transit AS needs to send e SCMP message to a source AS, the per-AS key is generated on demand using the *Dynamically Recreatable Keys* (DRK) algorithm and common seceret 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 [2].

4.3 Data Plane

While the control plane deals with path discovery, the data plane deals with forwarding data packets. For this 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 descion for a given packet is stored in the packet itselfs. This is refered to as *Package Carried Forwarding State* (PCFS) and several interessting properties of SCION are derived from this. Each packet at least contains a path, since source and destination adresses are optional, if the path is unambigous in its contetxt. 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 completly eliminated.

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

The absence of routing tables simplyfies 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 accelration of cryptographic opertions through technologies like Intel AES-NI, forwarding descissions 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 validition is so efficient, it out performs DRAM look-ups a BGP router needs to performe to reach its routing decission.

4.3.2 Path Combination

Path combination is the process performed by an end host to obtain valid path before sending a packet. Up to three path-segments are combined into an end-to-end path. First of all 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 1a $A \to E$) 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 1a $B \rightarrow D$) The path can be constructed by chaining a up-segment with a down segment. The up- and down-segment intersect in a core AS.
- **AS shortcut** (as shown in figure 1a $B \rightarrow C$) 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 cut off and discarded.
- **Core path combination** (as shown in fuger 1a $A \rightarrow D$) 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 fuger 1a $A \rightarrow B$) The up-segment and the down segment are connected by a peering link, such that the peering link alows a shortcut to the destination. Analogous to the AS shortcut in this case the extranous 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 performe its own lookup and combination process. Of course this process is assisted by varous cashing mechanisms.

4.3.3 Source Routing

5 Securtiy Properties

5.1 Isolation of Attacks

SCION carves the global internet up into smaller selfcontained units through ISDs and even these can be devided up by the support of subISDs. This by itself allready provides a significant advantage, since all entities outside an ISD can not influence the path discovery process (see section **??**). The compromise of trust roots is isolted 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 a endhost. A malicous AS can only announce down-paths to reach that malicous as.

5.2 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 towords solving this problem. First of all the architecture limits the scope of trust to a smaler set of trustees by introducing ISDs, secondly it reduces the number of trust roots to a managable number. **??** This makes key revocatio, or certificate revocation respectively, much easier, since there is no need for every single endhost on the whole internet to be informed indivdually. SCION also makes extensive use of trust transitivity offered by digital signatures.

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

- **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 adminstrative 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 todays TLS PKI system. This scenario suffers from the fact that it exposes many points of failure and revoking keys is made dificult by the sheer amount of keys to manage.

This is achivied by introducing a hirarchy of trust. [1]. ASes use a number of 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 small 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 signe each others TRCs trust is conveyed, by the transitive properties of trust, between ISDs. If an ISD revokes a trust roots 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 a interessting property emerges: As long as there is a path available to a given resource, the path can always be validate.

6 SCION Extensions

When SCION was first conceptualised the idea was to incorporate all needed features in a holistic designe.

7 SCION Adoption

SCION is designed with easy adoption in mind and offeres a number of attractive benefits to adopters. Designe 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 adopotion 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 comodity hardware or on existing routers and 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 lower the bar of entry to adopting SCION [3]

Since 2016 a realworld SCION testbed called ScionLab is operational [4] which includes several high profile members such as Swisscom and Switch, as well as other financial instatution like SIX and the Swiss National Bank [5] and further acedemic institutions. Infact the as of 2020 the thes bed serves over 600 entities and spans a globalb network of 30 IDS.

8 Discussion

After we have looked at the componants 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.

8.1 Availablilty

SCION incorperates multiple direct designe descissions which work towards improving availablity of the network, as well as other properties of the designe which inderectly contribute towards that goal.

In SCIONs down-path registration mechanism makes SCION inherently multipathed, since each AS may register multiple down-paths with the core path servers. This controll over down paths also allows an AS to select down paths for their reliablity and may select paths in a way to avoid unreliable ASes. Further in the endhost may take relyability 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 an a per packet basis, making use of multipath nature of SCION.

The high path freshness by guaranteed by SCIONs 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 dataplane may continue to function, even when the control plaine is disrupted.

8.2 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 achived first and for most by drastically reducing the cyrcle 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 effectiv key revocation feasable. Further more, ISDs are engineered to model and conform to existing trust boundaries derived from political and comerial realworld structures. At the sametime the single point of failure problem is avoided by introducing accountability into the management of trust rootsthrough the implementation of ARPKI **rpki**.

8.3 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 of a received PCB, nor can it advertise links it has no rights to with out detection. A misbehaving AS can always be attributed by its signature and can either circumvented by source routing or its keys revoked by the ISD core.

Since routing information is contained in each packets 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 can not alter the opaque fields generated by other ASes.

By implementing ARPKI **arpki** the certificate authority and by extension the TRC become tamperprove as well, as an attacker always needs to compromise mayority core ASes in order to approve actions to alter the TRC.

8.4 Scalability and Efficiency

As propesed 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 world wide depolyment it is expeted that there will eventually be around 6 to 10 [1] top-level ISDs, each subdevided into smaller subISDs. Consequenlty 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 in a similar manner. As described in **??** an AS joins an ISD by purchasing connectivety from an AS which is allready member of the ISD the AS wishes to joint. To 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 signe the new ISD keys.

A hughe boon for efficiency is the fact, that SCION removes the neccessity of routing tables in border routers, by storing forwarding information in the packet header. Current BGP routers use specialiced memory architectures to store the ever larger routing tables and perform prefix matching an acceptable speed. This special hardware is not only expensive but also power hungry. When comparing BGP und SCION routers in a simuliton XY et al. postulate an overal power saving of at least 16 %. They also find that the impact larger packet headers due to the PCFS inforamtion is negliable **scion_power**.

9 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 " [1]. This paper is later updated an referenced in a follow-up paper in 2015 where Barrera et al. who revisit SCION [2], while in their 2017 they give a detailed and update overeview in the Communiction of the ACM [3]. Multiple extension to the SCION protocol were proposed as follows. Onion routing was introduced through an extension discribed by Chen et al. [6], [7] and effective defences against DDoS attacks are discussed by Basescu et al. [8], Lee et al. [9] and Rothenberger et al. [10].

Since SCION heavily relies on multiple PKI systems therfore Basin et. all propose [11] and implement [12] 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" [13]

Ding et al. analyse five next-generation networking including SCION and compare them in 2016 study persented during in IEEE Access [14] and Know et al. present their findings from a real world test bed runing since 2016 ICNP 2020 [4]. A study by Giacomo et al. even suggests potential applications for SCION based networks in currently emerging internet satelite constalations.[15]

10 Conclusion

We have given an introduction to the SCION internet architecture in a form accessible to fellow intresseted professionals. We have layed out the challenges posed by the current and future scale of the global internet and defined a basic set of quality metrics to be fullfiled. 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 necessety for profound change. Following that we explored the concepts of new internet arichtecture proposed by SCION and explained its operation, benefits and security properties. Finally we discussed why and how SCION is able to fullfill our defined quility metrics.

11 Indicies

References

[1] 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.

[2] 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,

[3] 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).

[4] 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.

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

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] 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).

[11] 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).

[12] ——, "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).

[13] 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).

[14] 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.

[15] 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