Zürcher Hochschule
für Angewandte Wissenschaften

Introduction to SCION

Farner Simon

Ergänzende Veranstalitung 1
ZHAW School of Engineering
Schweiz
November 30, 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 **1**

2 Problem Analysis **3**
2.1 The Global Interne . . . 3
2.2 Quality Metrics . . . 3
2.3 Shortcommings of thc Current Internet Infrastructure . . . 4

3 Method **6**

4 Results **7**
4.1 Isolation Domains . . . 7
4.1.1 IDS structure . . . 7
4.1.2 AS and IDS Componants . . . 7
4.2 Control Plane . . . 8
4.2.1 Path Discovery by Beaconing . . . 8
4.3 Data Plane . . . 8
4.3.1 Path Assembly . . . 8
4.3.2 Data Forwading . . . 8
4.4 Trust Management . . . 8
4.5 SCION Adoption . . . 8

5 Related Work **9**

6 Indicies **10**
Literature . . . 10
List of Figures . . . 12
List of Tables . . . 12

Chapter 1

Introduction

Todays world is not only unimaginable without technology, it is also grows ever more connected. From our basic utilities, to public transport, our personal devices right down to light bulbs, everything is connected to the internet. Since it's inception in the in the 1970s the internet has permiated through all aspects of our lives and thus is an indispensable part of what makes our modern and connectod society and industries possible. One could go as far as to say that the internet has become the backbone of our modern society. However with the ever greater scale of this global network, it has become brittle. A chain of well publicsed outages demonstrates this clearly. The outage at Facebook on **TODO** is only the most rescent which springs to mind.

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.

Inthis 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 plauge the modern global internet.

This paper will outline inherent shortcommings of the current 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 existing protocol.

The core protocols and services which make our modern connected world tick may be narrowed down to the following:

1. Internet Protocol (IP): Provides adressing of devices.
2. Border Gateway Protocol (BGP): Provides forwarding and path discovery between networks.
3. Domain Name System (DNS): Provides resolution between domain names and ip addresses.
4. Public Key Infrastructure (PKI): Provides cryptographic binding between names and entities.

Of course there are many more technologies involved in getting information from point A to point B, but these are the ones that make the global portion of the internet work. Any disruptions to these services, can cause major outages and other problems for larg parts of the global internet.

These protocols an 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 fo the internet at 99.9 %. Which might seem high at first, but actually amounts to an average downtime of xx seconds per day. This is shockingly low compared to other infrastructure systems like the plain old telephone system, with an availability of 99.9999 %.

The possible reasons why parts of the global internet or individual resources may be unreachable are manyfold however here are some major ones:

- Denial of servica attacks
- Disruptions in DNS
- BGP route high jacking
- BGP route missconfiguration
- Physical route failures

The compromise or coruption of ceritificate authority and with it the compromise of the roots of trust which they provide do not directly impact the availabilty of the internet, however it has adverse effects on qualities, and needs mentioning in this context as well.

Chapter 2

Problem Analysis

2.1 The Global Interne

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 make our modern connected world tick and thus constitute what we will call the global internet, may be narrowed down to the following:

- Internet Protocol (IP): Provides adressing of devices.
- Border Gateway Protocol (BGP): Provides forwarding and path discovery between networks.
- Domain Name System (DNS): Provides resolution between domain names and ip addresses.
- Public Key Infrastructure (PKI): Provides cryptographic binding between names and entities.

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 choos from. First and foremost we want to have availability - if a resource is unreachable, all bets are off. As a benchmark 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 trust is a social and political concept which can be only 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 choos whom to trust with any out of scale reprecussions The current solution to the trust problem is subject of the browser PKI and BGP Sec.

Once trust is established we would like to ensure that communictain 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 thc 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. These 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 DOS attacks and physical failures in the carrier medium are most obvious causes for outages. However, these tend to be ofter localized to one or just a few sites, only ocassionaly causing world wide effects. In constrast, attacks on or misconfigurations in BGP often have wide ranging consequences and can take large swaths of the interrnet down. Even short lived problems like temporary dead routes or loops during route convergence often affect thousands of users.

Managing trust is notoriously dificult. There have been multiple attempts to implement certificate revocation in the past and all of them failed. 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 once, the sheer number of available trust roots is immense. Firefox for example, at the time of wiriting, ships with 131 CA certificates includet NEEDS REF. Assessing them all relyably and continously is task. Furthermore, removing a trust root may render a large number of resources on the internet untrusted and thus inacessible. This also ilustrates that the current trust model does no scale.

Finally the question of scaleablity ond efficency must be addressed. The most glaring issue at the time is the exhaustion of IPv4 address space. IPv6 is a valiant effort to relieve this problem, which until now has not come to flurishion. This fact alone demonstrates how slowly core internet technologies evolve. Adding an new AS to the global internet not only requires each resource in that AS to be adressable by IP address it also requires that the new location of the AS to be propagated through the whole network to all the routers and to be added to their routing tables. As XY demostrates rout convergence in BGP can take up to XY seconds after a change, so changing, adding or removing routes is slow. Further is the process error prone, as demonstrated by noumerous BGP missconfiguration related outages. Prominant cases of BGP route high jacking further makes its lack of proper security clear.

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 DNS Sec clearly demonstrate. Allthough techonologies like TLS and DNS 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.

Chapter 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 unfamiliar with SCION and the details of routing protocols. We studied the main body work published by Perring et al. and surveyed a collection of connected papers. For the detailed description of these see Chapter 5.We present a condensed and simplfied form of the involved concept as an overview for the uninitiated.

Chapter 4

Results

4.1 Isolation Domains

SCION borrows basic ideas from the Border Gateway Protocol (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 4.1a. An ISD is comprised of multiple core ASes, form logical unit whos members share a common set of resources and mutualy trust each other. As their name states, ISDs are intended to be selfsuficient units, the internal state of which must not leak out into other ISDs. [1] While an arbitrary AS can be a member of an arbitrary ISD, or even multiple ISDs, it is expected that ISDs will form along shared comercial interests, legal juristiction or other political borders. [2].

4.1.1 IDS structure

As shown in ilustration 4.1a 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.

4.1.2 AS and IDS Componants

In the following we will explore the componantes which are required to run an SCION AS and by extension a IDS since a single core AS is sufficient to form an IDS.

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 enabled and must addhere to the common rules agreed upon inside de IDS, however each AS is free to choos its internal structure. 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 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 4.3.1. As SCION makes extensive us of certificates to validate paths and intities, certificate servers are deployed to cache and provide certificates in an AS.

A core AS differs from other ASes in serveral important aspects. First of all Core ASes have border routers which are connected to cores ASes in neighbouring. The beacon servers in the core

ASes also take part in inter IDS beaconing, thus their path servers also hold path information on how to reach neighbouring ASes. Further more the ISD core is responsible for maintaining the trust root configuration (TRC).

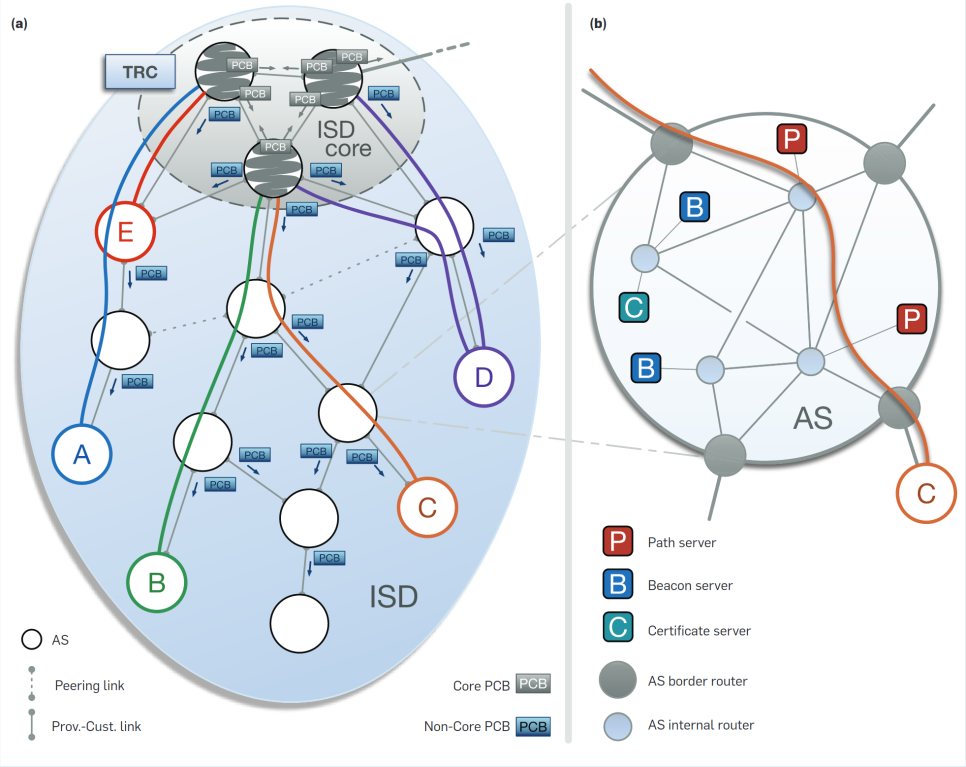

Figure 4.1: Internal structure of an ISD. From [2]

4.2 Control Plane

4.2.1 Path Discovery by Beaconing

4.3 Data Plane

4.3.1 Path Assembly

4.3.2 Data Forwading

4.4 Trust Management

4.5 SCION Adoption

Chapter 5

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 [3], while in their 2017 they give a detailed and update overeview in the Communiction of the ACM [2]. Multiple extension to the SCION protocol were proposed as follows. Onion routing was introduced through an extension discribed by Chen et al. [4], [5] and effective defences against DDoS attacks are discussed by Basescu et al. [6], Lee et al. [7] and Rothenberger et al. [8].

Since SCION heavily relies on multiple PKI systems therfore Basin et. all propose [9] and implement [10] 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” [11]

Ding et al. analyse five next-generation networking including SCION and compare them in 2016 study persented during in IEEE Access [12] and Know et al. present their findings from a real world test bed runing since 2016 ICNP 2020 [13]. A study by Giacomo et al. even suggests potential applications for SCION based networks in currently emerging internet satelite constalations.[14]

Chapter 6

Indicies

Bibliography

[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, 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).

[3] 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,

[4] 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).

[5] 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).

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] ——, "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).

[11] 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).

[12] 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.

[13] 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.

[14] 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

4.1 Internal structure of an ISD. From [2] 8

List of Tables