Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport DDPS

National Cyber Security Centre NCSC
Analysis and Prevention

18 March 2025

Technology considerations

SCION

1 Introduction

Since the mid-1960s, the internet has evolved from a packet-switched network originally developed for research purposes and not intended for commercial use into what we know today as a medium for all kinds of communication. Despite this evolution, the internet still relies on the foundational technologies that were developed at the time. While these have been refined over the years, they have never been fundamentally rethought to meet the changing demands placed on a globally available and reliable communications infrastructure. One of these foundational technologies is routing – that is, the way data (or data packets) are forwarded from a sender to one or more recipients in a packet-switched network.

This is where SCION comes in. SCION stands for Scalability, Control, and Isolation On Next-Generation Networks. But the word 'scion' also means 'descendant' or 'offspring'. That is no coincidence: SCION is not just a technology that promises more secure, reliable and controllable routing – and therefore safer data transmission online. It also represents an ambitious step toward a new internet architecture, positioning itself as the successor to today's way of transmitting data packets.

This technology brief gives a concise overview of the problems with today's internet architecture and how SCION aims to address them. For more in-depth information, see references [1] and [2], as well as many other resources available online.[1]

2 Problems

On the internet, routing protocols are responsible for routing IP packets, with a distinction made between internal and external protocols. Internal routing protocols handle routing within autonomous systems (ASes), which can be thought of as domains, while external routing protocols manage routing between domains. As the internet grew exponentially in the 1990s, the limitations of earlier protocols like the Gateway-to-Gateway Protocol (GGP), specified in RFC 823, became apparent. A more powerful, external routing protocol was needed, leading to the introduction of the Border Gateway Protocol (BGP). The version of BGP still in use today is specified in RFC 4271 and dates back to 2006, although its functionality has been expanded over time through additional RFCs.

[1] Many of these resources are available at https://www.scion.org and https://scion-architecture.net.

As an external routing protocol, BGP is primarily designed for efficient transmission of IP packets between domains, with less emphasis on security. Consequently, vulnerabilities in BGP are frequently identified and can be exploited for a variety of network-based attacks, including Distributed Denial of Service (DDoS) and BGP hijacking.[2] In both cases, a key underlying issue is that the data exchanged via BGP – i.e. inter-AS routing information – is not protected using cryptographic methods. This makes the data susceptible to tampering. Furthermore, BGP offers no means of influencing long-distance IP packet routing. This limits control over data transmission paths and reduces sovereignty in data communications.

To address the first issue, a security extension to BGP known as BGP Security (BGPsec) has been available since 2017, specified in RFCs 8205 to 8209. BGPsec offers a mechanism for validating routes using digital signatures. This ensures that route announcements are genuine and have been authorised by the responsible domains (ASes). However, implementing BGPsec requires a specialised global public key infrastructure (PKI); this is currently being set up as a Resource PKI (RPKI). Although the Federal Communications Commission (FCC) – the United States' regulatory authority responsible for the internet – is supporting the implementation of RPKI,[3] BGPsec will not be able to resolve all security issues related to routing, particularly during the incremental adoption phase.

3 SCION

Due to the limitations and associated vulnerabilities of BGP (as well as the BGPsec extension which was still in development at the time), researchers at ETH Zurich started designing an alternative in 2009. Their goal was to develop a system that offered not just stronger security but also the other qualities reflected in the SCION acronym – scalability, control and isolation. Consequently, SCION provides a greater range of features than either BGPsec or RPKI.

The SCION architecture is built around isolation domains (ISDs). Each ISD groups together one or more logically connected domains (ASes) that share a common trust root. Every ISD must have a certification authority (CA), which is responsible for issuing and managing digital certificates. In addition to managing certificates, each ISD plays a key role in providing information about available paths. This means that end systems can determine the route that their data packets will take before transmission. Similar to source routing in IP networks, it shifts some of the responsibility for routing from internet service providers (ISPs) to end systems and applications within an ISD. This marks a paradigm shift in how networks operate: it enables control over data transmission paths and allows these to be selected according to specific criteria, such as available bandwidth, latency and environmental and sustainability factors, like the CO_2 emissions of the routers used. Because transmission paths can be controlled, multiple paths can be used in parallel. This makes it possible to 'multipath' and switch paths quickly in the event of a path failure. SCION uses digital signatures not only to authenticate routing information (as BGPsec and RPKI do) but also to authenticate the sender information in data packets. This helps to defend against certain types of attack, including DDoS and amplification attacks. In addition to its core functions, SCION offers a variety of extra features, including connectivity with existing ISDs, firewall and gateway capabilities, support for building virtual private networks (VPNs) and bandwidth reservation. SCION-capable routers with verified software are also being developed. Alongside ETH Zurich, the development work involves a spin-off company[4] and various industrial partners, some of which are part of the SCION

[2] Already in May 1998, members of the hacker collective L0pht Heavy Industries warned of the risks posed by the lack of security mechanisms in BGP during a hearing before the US Senate (https://www.youtube.com/watch?v=VVJldn_MmMY).

[3] https://docs.fcc.gov/public/attachments/DOC-402579A1.pdf

[4] Anapaya Systems (https://www.anapaya.net)

Association.[5] Finally, the protocols used in SCION are being made available for international internet standardisation efforts.[6] This means that third-party providers will also be able to offer SCION-compliant products and services.

New networking approaches often struggle to gain widespread adoption. This is largely due to the many interdependencies involved and the different incentives of the various stakeholders. For example, network operators are unlikely to adopt a new approach unless there are enough applications using it. However, developers will only create such applications if the new approach is already widely available and in active use. Similar dependencies exist among all parties with an interest in SCION, which makes rolling it out a complex task. While SCION-enabled 'overlay' networks were initially the primary focus, SCION capabilities are now being developed and integrated directly into networks. Many ISPs now offer SCION-based services, and some sectors have started running ISDs as gated communities – such as the Secure Swiss Finance Network (SSFN) in the financial sector, or the Secure Swiss Health Network (SSHN) in healthcare. Although gateways are currently available to connect non-SCION-capable end devices, with various companies offering such solutions, 'native connection' via the operating system or dedicated application software is on the horizon.[7] Importantly, this does not have to be exclusive: SCION can be used alongside conventional BGP-based IPv4 or IPv6 networks to help maximise availability.

4 Conclusions and outlook

From a technological perspective, SCION offers major advantages over BGP and its security-related extensions (i.e. BGPsec and RPKI). These advantages extend beyond security in the narrow sense to include improvements in availability, reliability, control and sovereignty. In the context of intensifying geopolitical and economic tensions, technologies that can strengthen a country's digital sovereignty are becoming increasingly important. SCION's use of ISDs allows trust relationships to be managed locally. This eliminates the need for global trust frameworks such as web PKI. Furthermore, tests and measurements have shown that SCION provides security benefits and performs well in terms of speed and efficiency – a surprisingly positive outcome, given that improved security often comes at the cost of performance.

SCION also comes with some disadvantages. As with any new technology, the necessary expertise is not (yet) widely available and must first be developed. Over time, as SCION is standardised and incorporated into more products, this problem should become less significant. In this regard, activities in areas such as community building and standardisation are moving things in the right direction. There is always a risk that new security technologies raise unrealistic expectations – as if they could solve every security problem. Scion is no exception. While SCION can mitigate many (network-based) attacks, others will remain, typically those targeting higher layers of the protocol stack. These include attacks on web applications, such as SQL injection and cross-site scripting; weak authentication methods; data-driven attacks involving malware-infected Excel files; and various forms of phishing and social engineering. While SCION can help reduce some of these risks, for example by authenticating routing information and making attacks from certain IP addresses more difficult, it cannot eliminate them entirely. Therefore, SCION will need to be complemented by other security technologies, mechanisms, and services to ensure an adequate level of protection.

---

[5] https://www.scion.org

[6] The research group responsible for this is called the Path Aware Networking Research Group (PANRG); its documents are available at https://datatracker.ietf.org/rg/panrg/.

[7] This option is currently being tested within the SCION Education, Research, and Academic (SCIERA) network, with a quarter of a million users.

Abbreviations

AS	Autonomous System
BGP	Border Gateway Protocol
BGPsec	BGP Security
CA	Certification Authority
DNS	Domain Name System
DNSSEC	DNS Security
ETH	Swiss Federal Institute of Technology (*Eidgenössische Technische Hochschule*)
FCC	Federal Communications Commission
GGP	Gateway-to-Gateway Protocol
IETF	Internet Engineering Task Force
ISD	Isolation Domain
ISP	Internet Service Provider
PANRG	Path Aware Networking Research Group
PKI	Public Key Infrastructure
RFC	Request for Comments
RPKI	Resource PKI
SCIERA	SCION Education, Research, and Academic
SCION	Scalability, Control, and Isolation On Next-Generation Networks
SSHN	Secure Swiss Health Network
SSFN	Secure Swiss Finance Network

References

[1] Adrian Perrig, et al., SCION: A Secure Internet Architecture, Springer, 2017
[2] Laurent Chuat, et al., The Complete Guide to SCION: From Design Principles to Formal Verification, Springer, 2022