SCION ASSOCIATION

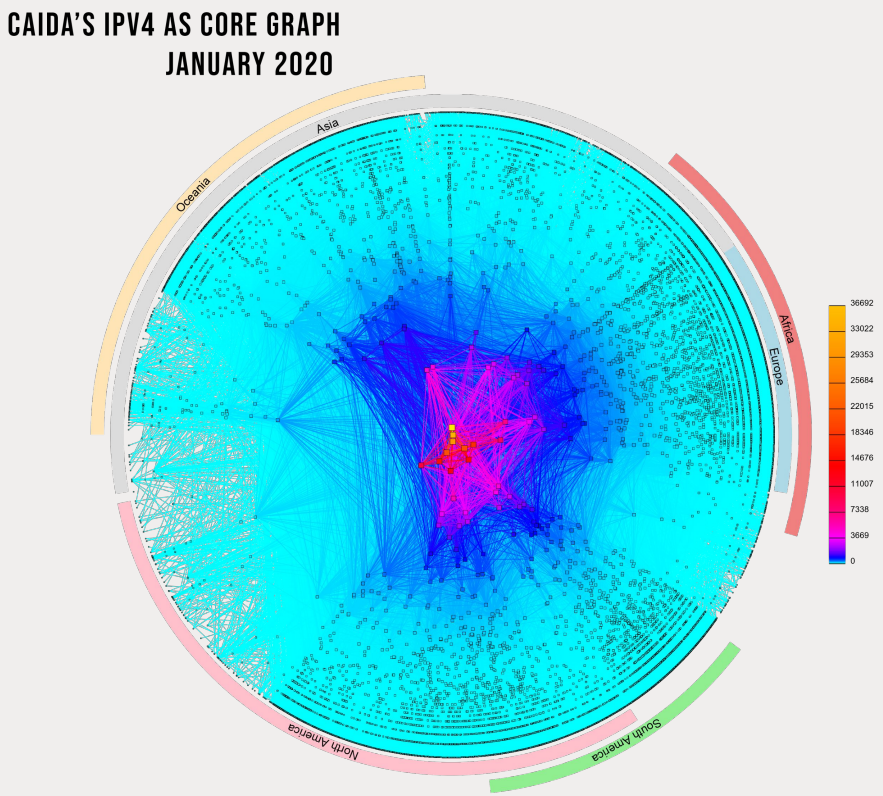
SCION: SECURE PATH-AWARE INTERNET ROUTING

SCION Association
info@scion.org

THE GLOBAL ROUTING SYSTEM

as of 1 June 2024

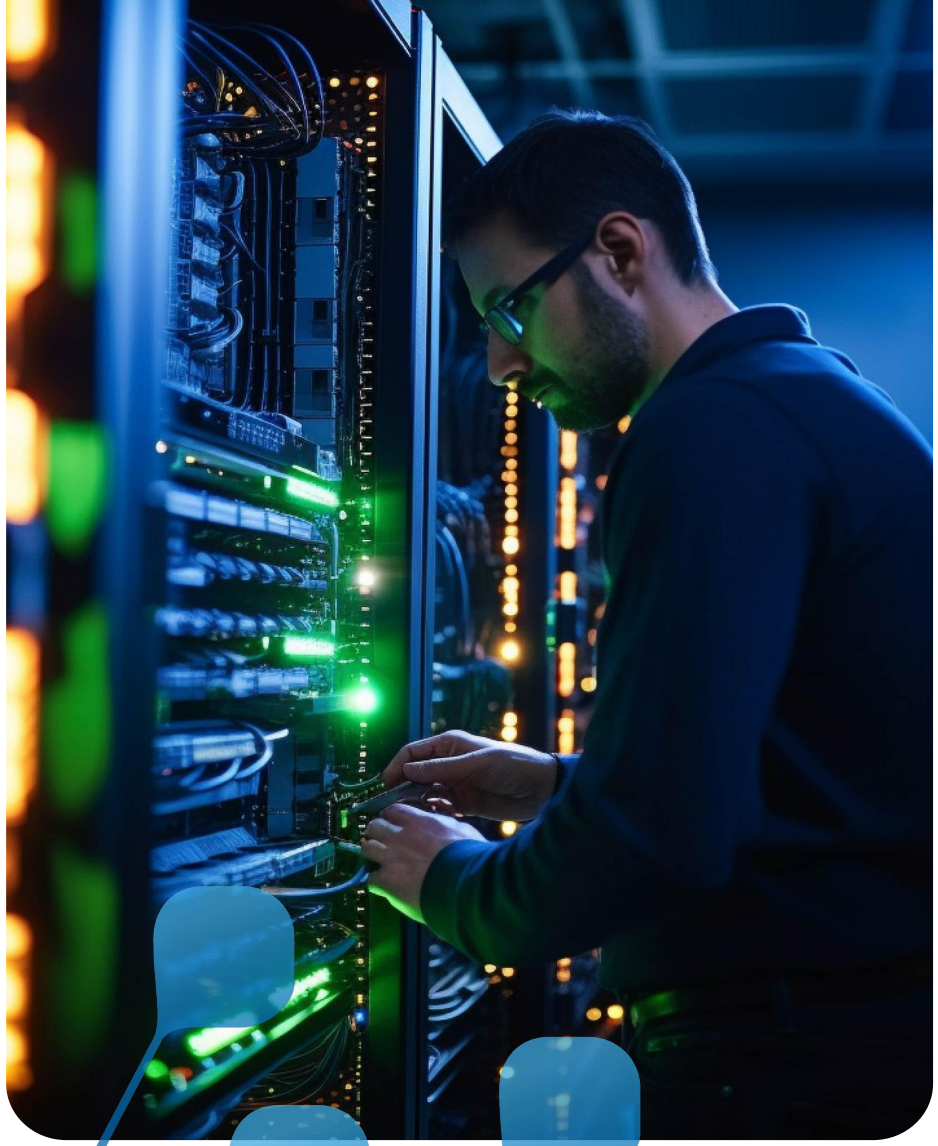
- 76,123 networks known as Autonomous Systems connected to the Internet, each using a unique Autonomous System Number (ASN) for identification
- 971,761 advertised IP prefixes (routes)
- Many possible paths across the Internet



THE ROUTING PROBLEM

Border Gateway Protocol (BGP): the Internet routing protocol

- The Border Gateway Protocol (BGP) used by the Internet routing system is inherently based on unverified trust between networks
- No built-in validation that route advertisements are legitimate
- Any network can announce any ASN or IP prefix
- Any network can claim to be another network
- Sending and receiving networks cannot decide the path that intermediate routers direct their traffic across the Internet



WHY IS THIS A PROBLEM?

Some information @ a glance

EVENT	EXPLANATION	REPERCUSSIONS	EXAMPLE
ROUTE LEAK	Usually accidental but sometimes malicious redirection of traffic through an unintended path. A network operator with multiple links announces to an upstream provider that has a route to a destination through another link.	Traffic is delayed or never delivered, with the intermediate network(s) carries unintended traffic. Can be used for MITM including traffic inspection and/or modification.	In Jun 2019, Verizon accepted incorrect routes from DQE Communications that diverted traffic destined for Cloudflare, Facebook & Amazon through small ISP.
ROUTE OR PREFIX HIJACKING	A network operator or attacker impersonates another network operator by falsely announcing ownership of IP prefixes and/or ASNs. Re-routes traffic by offering a shorter or more specific path for malicious or censorship reasons.	Traffic is forwarded to the wrong destination. Can be used for Denial-of-Service attacks, traffic interception or network masquerading.	Feb 2022 – KLAYswap Cryptocurrency hijack Apr 2018 - Amazon Route 53 hijack Feb 2008 - YouTube hijack
DATA SOVEREIGNTY BREACHES	BGP routing can, and often does, send traffic across geopolitical boundaries.	Can breach national and supra-national (e.g. GDPR) data protection legislation.	May 2023 – Australian healthcare data transferred through another country.

ROUTING PROBLEMS 101

Data sovereignty

Different countries have different regulations regarding transfer of sensitive data across geopolitical borders.

Routing can send traffic through different jurisdictions, thereby making regulatory compliance complex.

HOW IS THIS BEING ADDRESSED?

Some info @ a glance

EVENT	EXPLANATION	LIMITATIONS
RPKI & ROV Resource Public Key Infrastructure & Route Origin Validation	ROAs (Route Origin Authorisations) provide cryptographic assertions of IP prefix ownership and which ASNs are allowed to originate them. Routers can validate ROAs and generate appropriate route filters.	Requires widespread deployment to be effective (less than 50% of IP prefixes are signed in 2024) Few network operators currently use ROV (5%). Only does origin validation and does not validate paths through the Internet.
BGPSEC BGP Security	Builds on RPKI to provide cryptographic assertions that every router (hop) en-route to a destination has authorized the advertisement of that route. Prevents unauthorised insertion of ASNs into a path to circumvent RPKI.	Needs to be explicitly supported by all routers along a path to achieve full benefits. Computationally intensive and introduces significant delays in route convergence. Explicit path selection is not possible. Almost no deployment.
ASPA Autonomous System Provider Authorization	ASPA objects are similar to ROAs, but allow ASNs to authorize other ASNs to carry their traffic through the Internet. Works out-of-band so doesn't need to be deployed on all routers.	Developmental stop-gap technology and not yet an Internet standard. Does not provide assurances that traffic will actually follow validated paths.
SCION	Inter-domain routing architecture offering secure path awareness and selection.	Needs to be supported by border routers.

WHAT IS SCION?

SCION is an inter-domain path-aware architecture

INTER-DOMAIN MULTIPATH ROUTING:

- Fast path failover (can switch to backup path in ~RTT)
- Multi-operator

PATH CONTROL:

- Source endpoints can select AS path (included in packet header)

PATHS ARE AUTHENTICATED AT DISCOVERY AND VERIFIED AT FORWARDING:

- Higher assurance that packets will follow certain path
- Hijacking prevention
- Geofencing

Internet-based secure and reliable communication for critical infrastructure ecosystems (e.g. financial services, power utilities, emergency services, government, ...)

HOW IT WORKS

SCION core components in a nutshell

TRUST MODEL

- ISDs: logical groupings of ASes sharing common trust policy
- Each ISD administered by Core ASes via a voting mechanism
- Trust Root Configuration: X.509 certificates + ISD information
- TRC negotiated by Core ASes according to the trust policy
- Not reliant on third-party CAs

CONTROL PLANE – PATH CONSTRUCTION

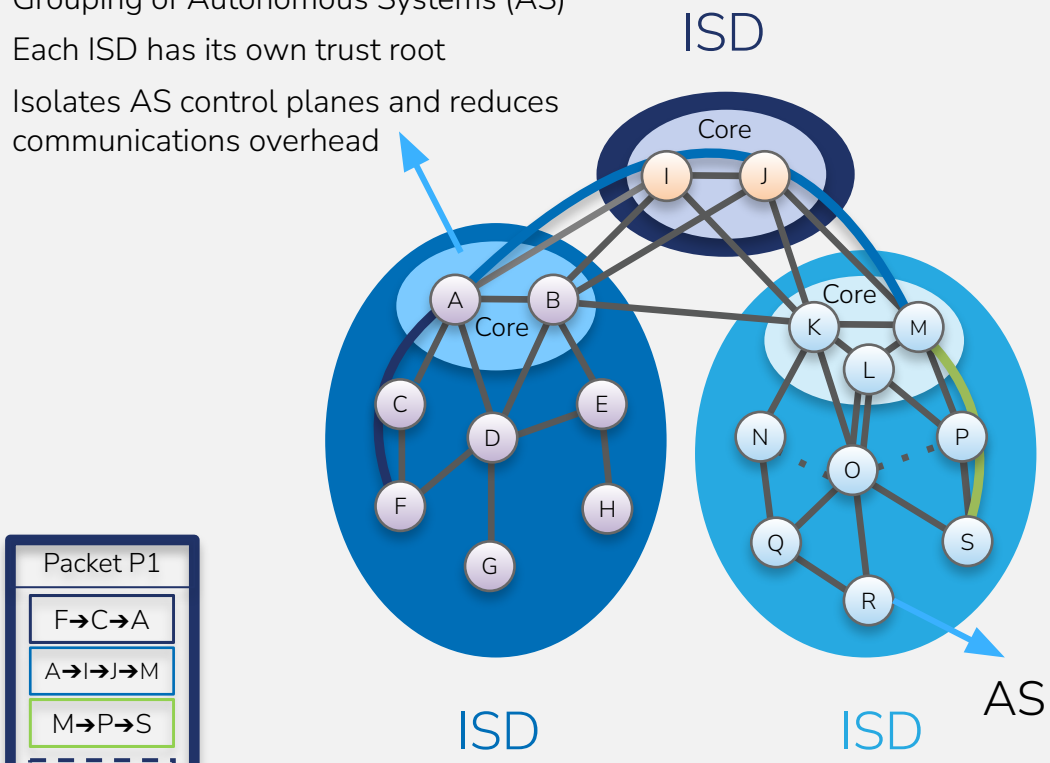
- Beacon server uses path-segment construction beacons (PCBs) to build path segments and routing paths
- Path server stores paths to AS discovered during beaconing
- Endpoints combine path segments to form end-to-end paths
- PKI authenticates path information

DATA PLANE - PACKET FORWARDING

- Combine path segments into end-to-end path (ISD-AS level)
- SCION packets contain end-to-end ISD-AS path
- Border routers forward SCION packets to next SCION router or end destination based on end-to-end path

Isolation Domain (ISD): the building block of SCION

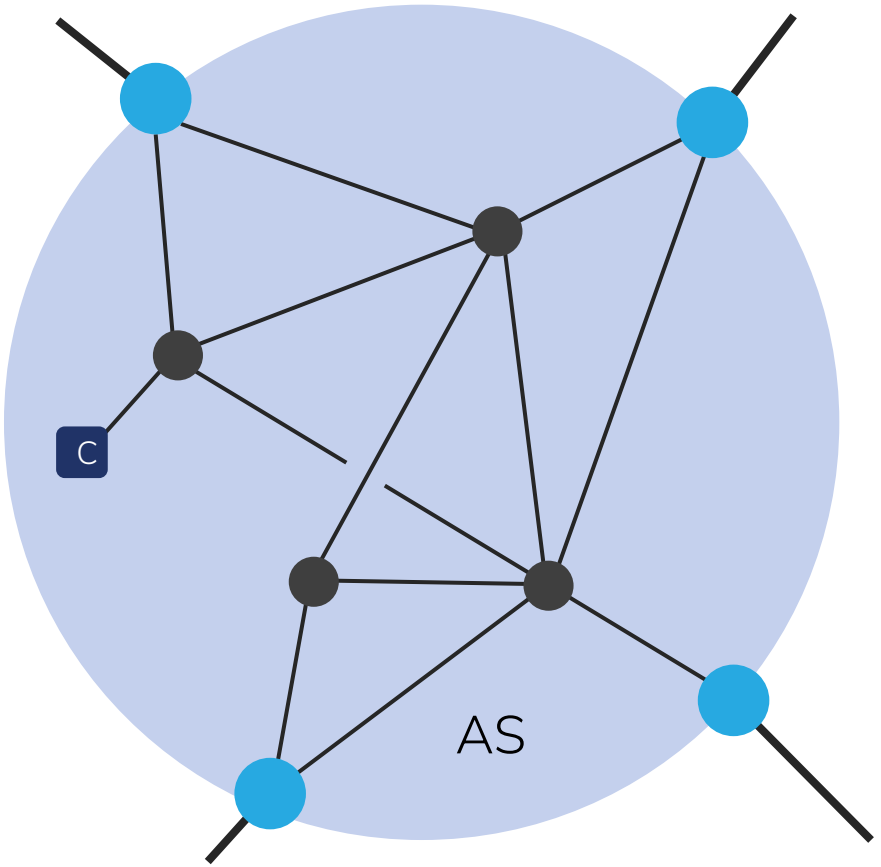
- Grouping of Autonomous Systems (AS)
- Each ISD has its own trust root
- Isolates AS control planes and reduces communications overhead



Packet from AS F to AS S

DEPLOYMENT MODEL

SCION AS



- SCION routers are set up at the borders of an AS
- Border routers peer with other SCION-enabled networks and collect customer traffic
- Control services discover and map network paths
- No change to the internal network infrastructure of a network operator needed.
- Endpoints run a SCION stack
- Legacy endpoints can use SCION gateways

C Control Services Border router Internal router

SCION CONTROL PLANE

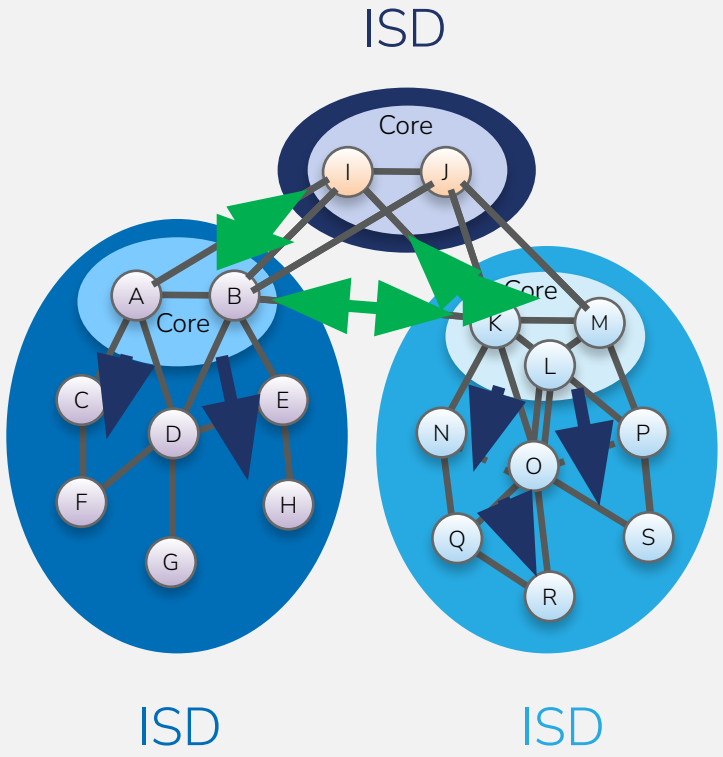
A look at how it works

Control plane mechanisms:

- Grouping ASes into ISDs - isolates AS control planes and reduces communications overhead
- AS-level routing - establishes paths on AS basis instead of on prefix basis

Beaconing:

- Path-segment Construction Beacons (PCBs) messages are used to build path segments and routing paths
- Core beaconing algorithm is used between all Core ASes
- Intra-ISD beaconing algorithm used between Core and Leaf ASes
- Endpoints look up path segments and combine them to form end-to-end paths.



Simulations on CAIDA AS topology (2k core ASes, 7k ASes in single ISD, 12k ASes total) suggest similar Core beaconing messaging overhead to BGPsec, and 1-2 orders of magnitude better for Intra-ISD beaconing.

SCION SETUP

CONTROL SERVICES (PER AS)

- **Beacon server** – generate, receive and propagate path-segment construction beacons (PCBs) to construct path segments and routing paths.
- **Path server** – store mappings of AS to path discovered during beaconing
- **Certificate server** – cache copies of TRCs retrieved from ISD core, AS certificates and key management for inter-AS communication
- **Border routers** – SCION packet forwarding to next SCION border router or destination host within the AS

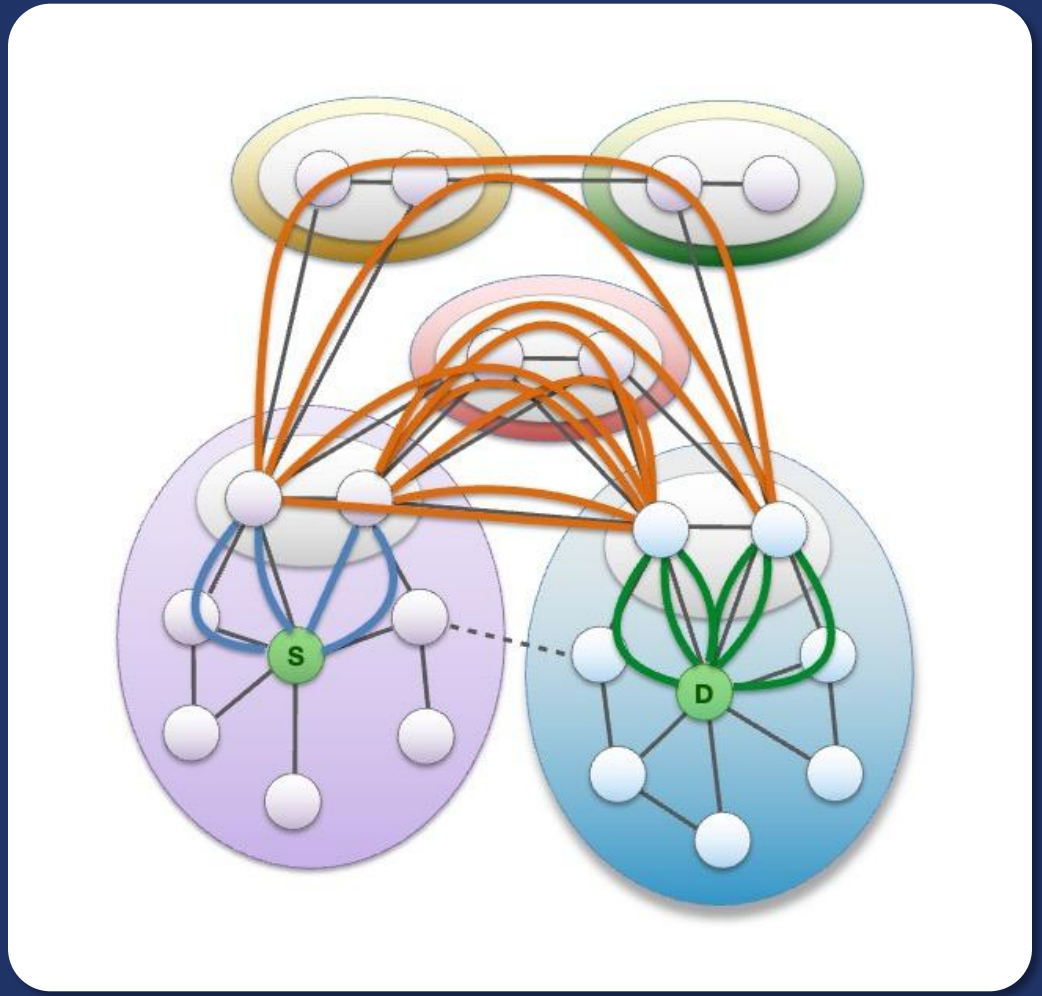
SIMPLER, CHEAPER ROUTERS

- SCION border routers only forward traffic and do not need to undertake control plane operations
- SCION border routers do not need to maintain inter-domain forwarding tables so do not require large and expensive TCAMs.
- One AES operation per packet for Message Authentication Code verification
- Paths can be used as soon as they are disseminated.

SCION BENEFITS: FAST MULTI-PATH DISCOVERY & FAILOVER

Advantages over regular Internet

- BGP generally selects routes based on ‘lowest cost’ regardless of whether these are in practice the most optimal or they meet particular requirements.
- With SCION, Leaf ASes only receive and do not forward any beacons. Only Core ASes initiate beacons.
- Beaconing does not rely on iterative convergence nor forwarding table updates, allowing rapid path exploration within ISDs.
- The control services discover path segments and assemble these into available paths.
- Tests show path failover to be within 1-2 seconds.
- Applications can choose paths based on optimal characteristics or other parameters, and can also use multiple paths simultaneously.



SCION BENEFITS: PATH VALIDATION

Experimental extensions

PROPERTY	APPROACH	COMPONENT
PATH AUTHORIZATION (HOP-BY-HOP)	Information at each hop is authenticated with a MAC (Message Authentication Code), checked by border routers at forwarding. Each AS only forwards traffic on paths that are explicitly authorized by the AS.	Standard SCION
PROOF OF FORWARDING	EPIC adds short per-packet MACs at each SCION hop. Source authentication and path validation are enabled by the additional use of efficiently derivable symmetric keys.	EPIC extension, L3 [1]
TRUST-ENHANCED NETWORKING	Packet headers are extended with policies telling border routers which intra-AS path to forward the packet, so that endpoints can select routers/ASes with specific path policies. Inter-domain paths are this way mapped to policy-compliant intra-domains paths. Per-AS attestation done by a third part.	FABIRD extension [2]

1. Legner, Markus, et al. "EPIC: every packet is checked in the data plane of a Path-Aware Internet." 29th USENIX Security Symposium (USENIX Security 2020).
2. Krähenbühl, C., Wyss, M., Basin, D., Lenders, V., Perrig, A. and Strohmeier, M., 2023. FABRID: Flexible Attestation-Based Routing for Inter-Domain Networks. (USENIX Security '23)

COMMERCIAL & OPEN-SOURCE IMPLEMENTATIONS

If you're interested in deploying SCION, there are currently two options:

ANAPAYA

Commercial

Open Source

Other implementations under development: P4, Rust, OpenWRT

SCION Association formed by deployers and early adopters to support open source development, standardization, and community involvement.

INTERNET ENGINEERING TASK FORCE

- Standardisation is important for interoperability and to encourage other implementations
- SCION components and functionality currently being documented through PANRG (an IRTF Working Group)
- Discussions with other IETF Working Groups
- Independent Submission Stream
- Hackathon @ IETF 118: Control Plane RPC over HTTP/3

Current Internet Drafts:

- SCION Overview draft-dekater-panrg-scion-overview
- SCION Components draft-rustignoli-panrg-scion-components
- SCION PKI draft-dekater-scion-pki
- SCION Control Plane draft-dekater-scion-controlplane
- SCION Data Plane draft-dekater-scion-dataplane

PANRG
Internet-Draft
Intended status: Informational
Expires: 10 March 2024

C. de Kater
N. Rustignoli
SCION Association
A. Perrig
ETH Zuerich
7 September 2023

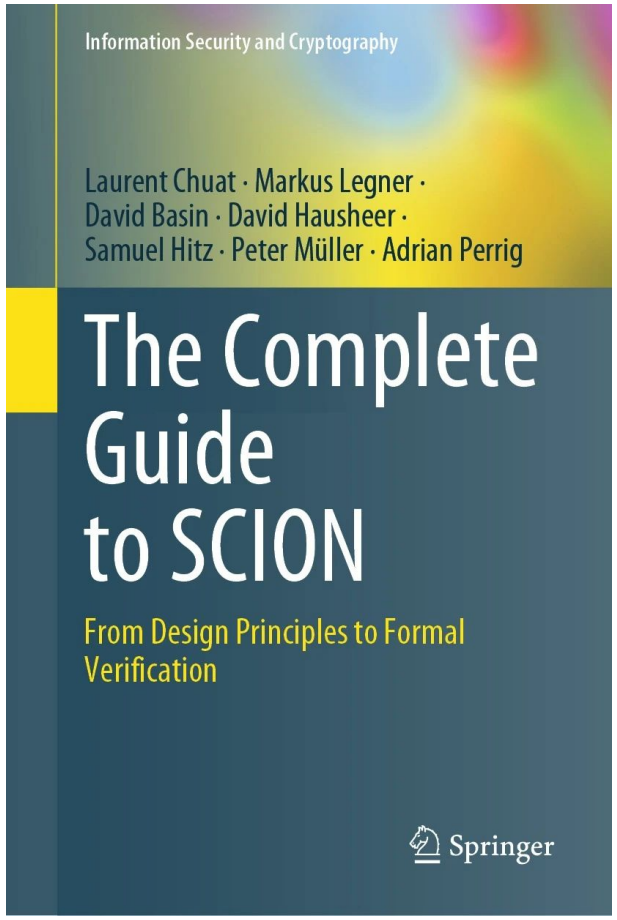
SCION Overview
draft-dekater-panrg-scion-overview-04

Abstract

The Internet has been successful beyond even the most optimistic expectations and is intertwined with many aspects of our society. But although the world-wide communication system guarantees global reachability, the Internet has not primarily been built with security and high availability in mind. The next-generation inter-network architecture SCION (Scalability, Control, and Isolation On Next-generation networks) aims to address these issues. SCION was

SCION TODAY

A growing ecosystem



The Complete Guide to SCION
Springer Verlag, 2022

THANK YOU!

More information:

- SCION Association: https://www.scion.org
- Reference & Developer Docs: https://docs.scion.org/
- Research: https://scion-architecture.net
- Vendor: https://www.anapaya.net/resources
- Latest Release: https://github.com/scionproto/scion/releases/