Internet Draft Updates

PANRG - IETF 120
July 25th, 2024

Nicola Rustignoli (nic@scion.org)
Kevin Meynell (kme@scion.org)

draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

Background: the SCION Internet Architecture

- Path-aware *inter-domain* Internet architecture, focusing on
  - Availability
  - Routing Security
  - Routing security (path authorization)

- In production use by dozens ISPs, serving the Swiss inter-banking network SSFN & an education network, being rolled out for a healthcare network and tested for a utility network.

- Core specification in 3 drafts (below)

Updates Since IETF 118

At IETF 118 PANRG we had a discussion about deployment experiences by early adopters

We also discussed where the SCION work fits within IETF/IRTF

- We'd like to document protocol specification of existing deployment ISE
- Research aspects / open questions of SCION should be kept in a RG (e.g. PANRG)
- In the long-term early adopter spec and RG work could be base for future IETF work

What happened since then:

- ISE submission
- IPR disclosure
- Updates to the drafts
- Open questions (later today)

Drafts Overview

Core SCION specification

Open questions
Research, lessons learned from deployment, long-term protocol evolution (later today)

Component	Document status	Internet Draft	Next Steps
PKI		draft-dekater-scion-pki-06	Waiting further review feedback
Control Plane	Submitted to ISE	draft-dekater-scion-controlplane-05	Addressing reviews
Data Plane		draft-dekater-scion-dataplane-02	Addressing reviews
Overview	Parts Incorporated into specifications I-Ds	draft-dekater-panrg-scion-overview-06	Not intended for publication
Component analysis	Expired	draft-rustignoli-panrg-scion-components-03	Not intended for publication
Deployment considerations	Table of Contents produced	draft-meynell-panrg-scion-deployment-00	Looking for inputs and contributors
Research questions	Table of Contents produced	draft-meynell-panrg-scion-research-questions-01	
DRKey	- Expired	draft-garciapardo-panrg-drkey	Submitted last update in 2022 by ETH. Pick draft again if there is interest?

draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

IPR Disclosures

Anapaya Systems AG submitted 3 IPR disclosures regarding SCION, including licensing information. We are not aware of any other IPR.

Patent	Control Plane	Data-plane	PKI	Component	Overview	IPR Disclosure
SCION-IP Gateway: The patent describes a system to discover and select remote SCION-IP gateways (SIGs) and optimize SCION path selection based on a variety of metrics to a remote SIG. (No license required)				x	x	https://datatracker.ietf.org/ipr/6392/
Optimizing internet traffic over a source-selected path routing network: The patent describes a system to embed a SCION Internet in the BGP-based Internet as a single BGP AS. Furthermore, it describes how this embedding can be used to optimize network traffic based on source-based path selection. (RAND)				x Section 3.1.		https://datatracker.ietf.org/ipr/6393/
Highly available autonomous systems: The patent describes an implementation of a highly available SCION AS control-plane relying on sharding, gossiping, and eventual consistency. (No License Required)	x	x	x	x	x	https://datatracker.ietf.org/ipr/6391/

Draft Updates - Overview

- Introduction
- New sections and clarifications
- Editorial
  - References, removed forward references (e.g. SCMP)
  - BCP14 keywords
- Security considerations
- IANA section: no IANA actions, added reference to currently allocated SCION numbers (https://docs.anapaya.net/en/latest/resources/isd-as-assignments/)

Control & Data Plane Updates

Section	draft-dekater-scion-controlplane	draft-dekater-scion-dataplane
Configuration required to run an AS • Clarify links, interfaces, neighbour adjacencies (incl. underlay addresses) must be configured out of band • Clarify current implementation uses IP/UDP as lower layer protocol	2.2.4. Configuration	1.3.3. Configuration
Dependencies on time synchronization • Clock skew of single digit minutes is generally tolerable • Relevant for PCBs/segment validation, as they are timestamped. Their validity is expressed in multiples of 337.5s, or 1/256 of a day • PCBs may be propagated at regular interval, with some delay	2.3.3. Effects of Clock Inaccuracy	4.2.2.3. Effects of Clock Inaccuracy

draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

Control Plane Updates

- Clarify requirement to validate Path Construction Beacons, especially regarding time (2.2.3. PCB Validity)
- Scalability next slides
- Specification of the Control Service gRPC API in protobuf (Appendix)
  - Updated to use HTTP/3 following this IETF118 hackathon project
- Service addresses, used for control plane communication (Appendix)

Control Plane Scalability - Updates

New section 2.4. Path Discovery Time and Scalability

- Explain trade-offs in terms of resource overhead (PCBs, validating signatures) and amount of paths discovered
- Clarify implication of *best PCBs set size*. To avoid exponential growth of PCBs, ASes limit the number of propagated PCBs per interface to 50 (intra-ISD) and 5 per destination AS (inter-ISD)
  - Intra-ISD beacons per AS grow linearly with # of neighbours
  - Inter-ISD beacons per AS grow linearly with # of core ASes
- In case of cold start, paths are discovered at worst after n propagation times (where n is the longest path)
  - Optional *fast recovery* mechanism can reduce this

Data Plane Updates

- Clarifications on MAC computation
  - Introduced AES-CMAC as a default algorithm to be supported by all vendors. Clarified requirements for alternatives.
    (4.1.1.3. Default Hop Field MAC Algorithm, 4.1.1.4. Alternative Hop Field MAC Algorithms)
  - 4.1.1.2. Layout of the Input Data for the MAC Calculation

- Introduced dedicated service addresses for discovery and control service (2.2.2. Address Header)

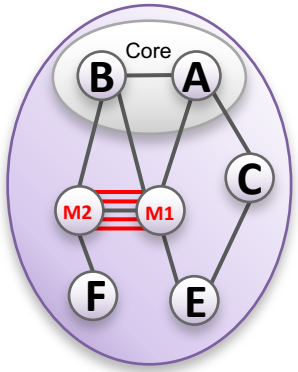
Security Considerations

- “Vanilla” SCION, with its core components, provides:
  - Path authorization
  - Hijack traffic prevention (e.g. path splicing, attract other AS traffic, inject malicious AS in beacons, spoof AS, ...)
- Experimental extensions can cover more threat scenarios (not part of current drafts)
- We clarify attacks, defenses in security considerations

Security Considerations – Control Plane

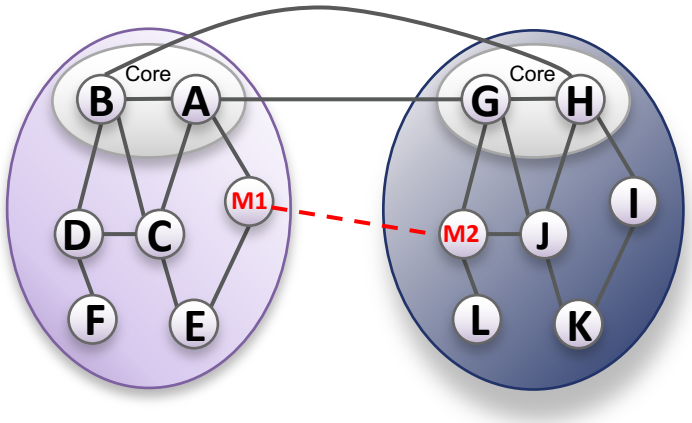
- Beaconing in an ISD depends on Core ASes
  - Path discovery stops if *all* core ASes are compromised
  - Data plane keeps forwarding until path segments expire
- Two colluding ASes might attempt to manipulate the path selection process (section 5.2.4):

Announcing a large number of path segments to attract traffic:



- Only downstream ASes are affected
- Can be detected counting paths

Wormhole attack: creating a “tunnel” shortcut (even across ISDs) to attract traffic:

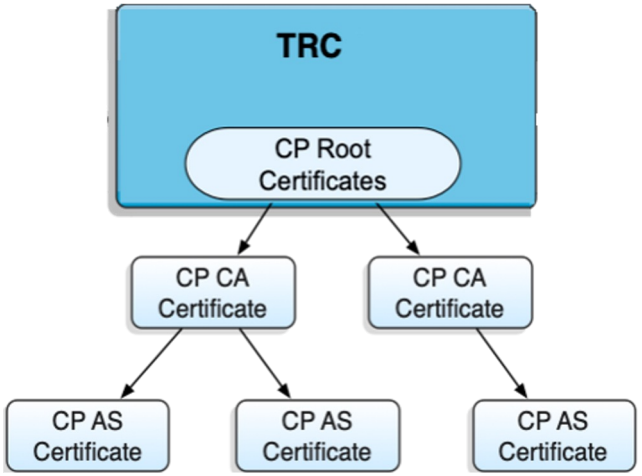


- Intrinsically difficult to prevent
- Might be detected with latency measurements

draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

Security Considerations – PKI

- ISD have a “self assigned” root of trust (TRC)
  - Voting and updates protects them from compromise (PKI section 5.1.2)
- Beaconing requires a valid AS certificate
  - Prevents AS spoofing (see control plane 5.2.2)
  - Short lived
  - Reliance on certificates (PKI section 5.1), especially on intermediate CAs (PKI section 5.2)
- A malicious ISD may be created if:
  - Other ASes to accept a new ISD root of trust
  - Open questions on the ISD creation process (deployment draft)

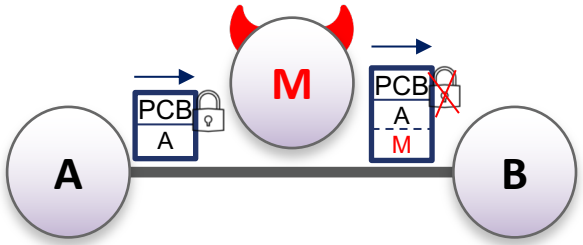


draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

Security Considerations – Path Hijacking

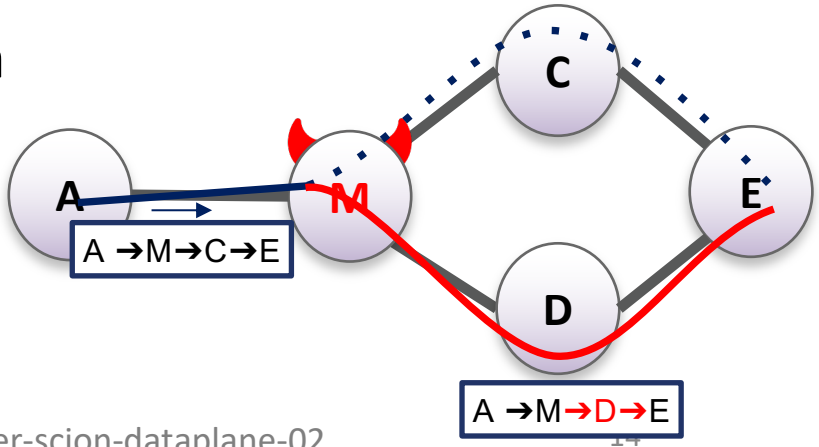
In Control Plane: A malicious AS M cannot hijack traffic between neighbors A and B to divert traffic through itself

- On control plane: M cannot inject itself into path by altering path discovery (PCBs) – Next ISD-AS field is signed and hijacking is detected by B



In data plane

- An on-path attacker M may rewrite remaining part of path header with another *authorized* path.
  Could be detected by endpoints by adopting a data integrity protection system (like IPSEC).



draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

Security Considerations – Data Plane

SCION's Data plane provides path authorization via chained MACs.

- The forwarding key used for MACs is shared among routers within the AS.
  - If it gets compromised, path authorization may be violated (5.1.1 Forwarding key compromise)
- MAC forging unlikely (5.1.2 Forging MAC)
- Path segments cannot be spliced to craft an unauthorized path by a malicious endpoint.
  - Prevented by segment identifiers/accumulator and path segment timestamps.
  - However, collisions may briefly happen with current 16 bit field length.

draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

Security Considerations – DoS

- Data Plane: use of path reversal limits possibility of reflected volumetric DoS
  - Endpoints might switch to alternate path if link BW exhausted due to volumetric DoS
  - Higher-layer DoS not covered by SCION
  - Path-awareness enables more fine-grained filtering
- Control plane:
  - Deployment requires filtering and replication of control services to avoid DoS
  - Recommended filtering of path lookup endpoints and rate limiting

NASR

- Similar use cases
- SCION has a strong inter-domain focus. It could use NASR intra-domain
- SCION PKI introduces a unique trust model
- Secure Path-awareness is specific to SCION
  - Multipath
  - Diminishes need for proof of transit (in terms of security properties). Proof of transit can be an additional “auditing” tool on top of path authorization
  - Proof of transit is not offered by core SCION components (experimental extension)

draft-dekater-scion-pki-06 & draft-dekater-scion-controlplane-05 & draft-dekater-scion-dataplane-02

Thank You For Your Attention!

Questions & Remarks?

nic@scion.org