Background: the SCION Internet Architecture

- Path-aware *inter-domain* Internet architecture, focusing on
  - Availability (even in presence of adversaries)
  - Security (routing)
  - Scalability

- In production use by 7 ISPs, trial deployment by 5 ISPs, serving the Swiss inter-banking network [SSFN](http://example.com) & an education network, being tested for the Swiss health network.

- For a general overview about SCION, see: [draft-dekater-panrg-scion-overview](http://example.com)
SCION Core Components in a Nutshell

Data Plane - *Packet Forwarding*
- Combine path segments into end-to-end path (ISD-AS level)
- Packets contain end-to-end ISD-AS path
- Forward packet based on e2e path, agnostic of end-host address

Control Plane – *Inter-Domain Routing*
- Discover valid inter-domain paths
- Construct and disseminate path segments
- Routing is based on <ISD>-<AS> tuple as “locator”
- Intra-AS communication reuses existing data plane and routing (e.g., IPv6/IPv4)

Control Plane PKI (CP-PKI) - *Authentication*
- Authenticate path information
- Used by control plane
- Basis for unique ISD trust model

Isolation Domain (ISD):
- Grouping of Autonomous Systems (AS)
  - Each ISD has its own trust root
  - For routing protocol scalability

draft-dekater-scion-controlplane & draft-dekater-scion-dataplane
IETF 18 Prague:

- Joined the Hackathon last weekend
- Have a SCION vendor and user here today

Presented and discussed at the PANRG Interim Meeting on 8 September 2022
Control Plane – Inter-Domain Routing

- **Exploration (beaconing)**
  SCION control plane discovers valid paths through “beaconing”

- **Registration**
  ASes select path segments and make them available to other ASes

- **Resolution (lookup and combination)**
  Source endpoint creates an e2e path and adds it to the packet header
CP - Path Exploration

- Core ASes periodically send Path Construction Beacons (PCBs)
  - Inter-ISD “core” beacons are flooded (with loop prevention mechanism)
  - Intra-ISD beacons travel top-down (parent to child)
- Per propagation period, each AS
  - further propagates selected PCBs to neighbors
- PCBs accumulate cryptographically protected path- and forwarding information per traversed AS
- Key content of one PCB:
  - Initiation timestamp/Expiration time/ID
  - List of all ASes on the path so far
  - Signed routing information per AS
  - Possibility of peering links

draft-dekater-scion-controlplane & draft-dekater-scion-dataplane
CP - Path Registration

• Each AS periodically stores/registers selected PCBs as **path segments** *(up-path or down-path)*
  • Each AS can freely choose selection algorithm and criteria
  • Reversion of path segment direction is possible
• **Up-path** segments
  • How the AS wants to reach its core AS(es)
  • Stored at the AS’s local control service
• **Down-path** segments
  • How the AS wants to be reached by other ASes
  • Registered with the control services of the relevant core ASes

draft-dekater-scion-controlplane & draft-dekater-scion-dataplane
CP/DP - Path Resolution

Source endpoint creates e2e path by
• looking up path-segments to destination AS (control plane)
• combining path-segments into e2e path (data plane)

Requires lookup of max. 3 path segments:
• **Up**-path segment
  • To reach core AS in source ISD
  • Responsible: control service of source AS
• **Core**-path segment
  • To reach core AS in destination ISD
  • Responsible: control service of core AS in source ISD
• **Down**-path segment
  • To reach destination AS
  • Responsible: control service of core AS in destination ISD

Reduce latency by:
• Caching returned path segments
• Sending requests for path segments in parallel
Data Plane - Overview

- SCION data plane forwards inter-domain packets between ASes
- Forwarding is based on end-to-end path information contained in the packet header
  - Path information consists of a sequence of hop fields – 1 hop field per on-path AS
  - Each hop field includes ingress- and egress interface IDs for the corresponding AS
  - Hop fields are authenticated with a Message Authentication Code (MAC) to prevent forgery:
    - ASes use their own secret key to authenticate the hop field
    - The MAC is checked by routers during forwarding
    - ASes only forward authorized traffic

SCION routers are deployed at the AS edge. Required steps to forward packets:
- Access the next hop field in the packet header
- Verify the authenticity of the hop field’s MAC
- Forward packet to the next AS on the path
  → No need to inspect destination addresses and forwarding tables

Intra-domain routing based on existing mechanisms

draft-dekater-scion-controlplane & draft-dekater-scion-dataplane
SCION forwarding is based on end-to-end path information contained in the packet header. The SCION packet header consists of a

- **Common header** - defines the
  - length of header & payload
  - type of SCION path
  - type & length of endpoint address of source and destination

- **Address header** – defines the
  - ISD-, AS-, and endpoint addresses of source and destination

- **Path header** – contains the
  - full AS-level forwarding path

- **Extensions header** (optional)
  - Hop-by-Hop and End-to-End options, similar to IPv6 extensions

[Diagram of SCION header structure]

*draft-dekater-scion-controlplane & draft-dekater-scion-dataplane*
SCION Path - Path Header Overview

The **SCION** path type is the standard path type in SCION. The path header of the SCION path type consists of:

- **One path meta header**
  - Indicates the currently valid segment info field and AS hop field while the packet is traversing the network
  - Defines the number of hop fields per segment

- **Up to 3 info fields**
  - Each info field contains basic information about corresponding path segment
  - Number of info fields == the number of path segments in the path

- **Up to 64 hop fields**
  - Each hop field represents a hop through an AS on the path
  - Hop field information is authenticated with Message Authentication Code (MAC) to prevent forgery
An endpoint creates E2E paths in the data plane, by combining path segments looked up in the control plane

- Each E2E path can contain at most one of each type of segment (up-, core-, and down-segment)
- The SCION path header is created by extracting required info and hop fields from the corresponding path segments
DP - Possible Path-Segment Combinations

Allowed path-segment combinations:

- Communication through core Ases
  - Core-segment combination (1a, 1b, 1c, 1d)
  - Immediate combination (2a, 2b)
- Communication via a peering shortcut (3a and 3b)
- Communication via an AS shortcut (4a and 4b)
- On-path communication (5)
Data Plane – Advantages SCION Design Choice

- It provides **control & transparency** over forwarding paths to **endpoints**
- It offers **inter-domain multi-path**
- It enables path authorization
- It simplifies the **packet-processing** at routers
  - Just access the next hop field in the packet header
  - No longest-prefix matching on IP addresses
- **Intra-domain routing** protocols and infrastructure is **reused**
Security Considerations*

- **PCBs are signed** in an onion fashion in order to avoid path hijacks/splicing. Every AS can verify all routing messages by following the certificate chain.

- **Hop-by-hop path authorisation**: Information on each hop is authenticated with a MAC, checked by routers at forwarding. Each AS only forwards traffic on paths that it has explicitly authorized.

- **Lack of global kill-switches**: Roots of trust are ISD-scoped, thanks to the use of own PKI (CP-PKI [draft-dekater-scion-pki](#)).

*Section not available in the drafts yet, will come soon.*

[draft-dekater-scion-controlplane](#) & [draft-dekater-scion-dataplane](#)
Summary & Next Steps

Summary:

• SCION is a future Internet architecture with **productive deployment**
  • Its **control plane PKI** builds the basis for a **unique trust model** per ISD
  • Its **control plane** provides **path-aware, inter-domain routing**
  • Its **data plane** forwards data packets based on **end-to-end path information** contained in the packet header

• IETF Internet Drafts are available for all three main SCION components (PKI, CP, DP)
  • Feedback is welcome
  • To be done: IANA section, Security considerations

Next Steps (within the IETF):

• To be discussed at the end of today’s session

Thank You For Your Attention!

Questions & Remarks?