Path Validation in SCION

Side meeting - IETF 118 Prague

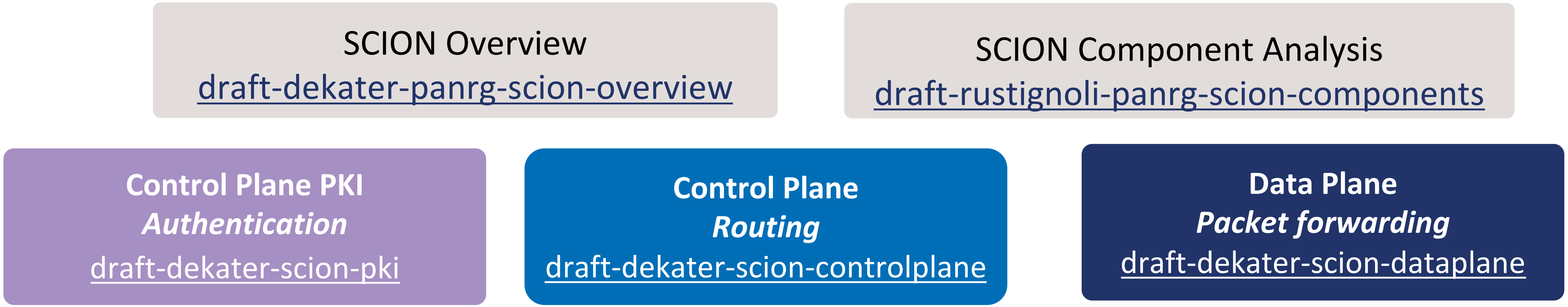
7.11.2023

Nicola Rustignoli, SCION Association (nic@scion.org)

draft-dekater-panrg-scion-overview

Motivation and background

- SCION is a path-aware inter-domain architecture that provides:
  - Path authorization
  - High assurance that packet follows desired path
  - Proof-of-transit (as an extension)
- Existing work focuses on intra-domain path validation



SCION Overview
draft-dekater-panrg-scion-overview

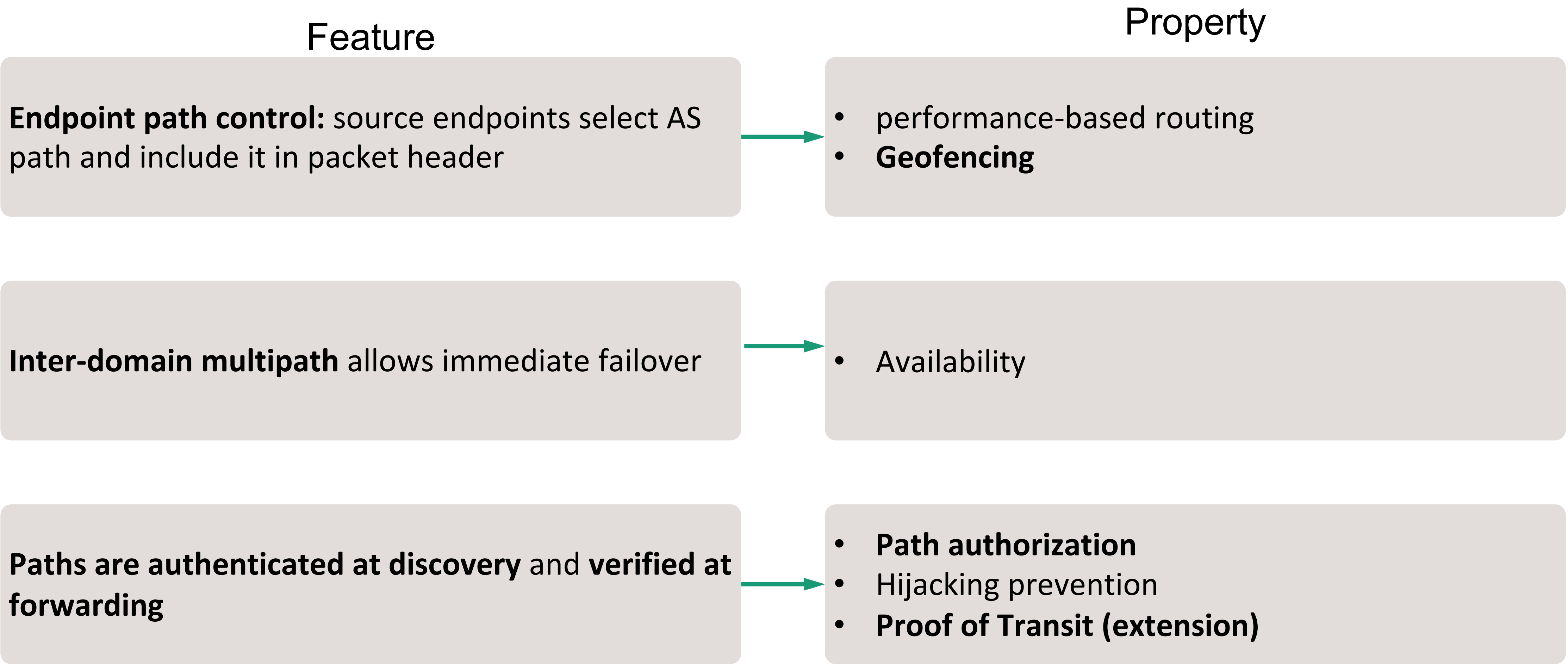
SCION Component Analysis
draft-rustignoli-panrg-scion-components

Control Plane PKI
Authentication
draft-dekater-scion-pki

Control Plane
Routing
draft-dekater-scion-controlplane

Data Plane
Packet forwarding
draft-dekater-scion-dataplane

Background: the SCION *inter-domain* routing architecture



Feature	Property
Endpoint path control: source endpoints select AS path and include it in packet header	• performance-based routing • **Geofencing**
Inter-domain multipath allows immediate failover	• Availability
Paths are authenticated at discovery and **verified at forwarding**	• **Path authorization** • Hijacking prevention • **Proof of Transit (extension)**

SCION: Approach

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)

SCION: some use cases & adopters

- Internet-based enterprise communication for critical infrastructure
    - Connect multiple organizations, branches with performance-based routing, path control and inter-domain multipath (e.g. finance, power, blue lights, government, …)
- Geofencing: keeping traffic in a trusted area of the network

Some adopters:

- Swiss inter-banking network SSFN, Swiss healthcare network
- Swiss Internet Exchange
- Global education network
- Sui validator network
- Others being tested

Path validation: use cases in combination with inter-domain path-aware networking?

Why **is path validation** especially interesting for path-aware architectures?

- **Geofencing** (use only paths with routers in a given area, based on geolocation, jurisdiction, …)
- **Trust-enhanced networking:** Route based on attested router policies (e.g. vendor, patch level, time synchronization support such as PTP, ...)
- **Path stability** can be assured over time

Conclusion

- Path validation provides interesting use cases in combination with inter-domain path-aware networking (geofencing, trust-enhanced networking)
- We see a gap in inter-domain path validation
  - SCION is inter-domain only, therefore It can potentially reuse or build on top of other intra-domain path-validation techniques
  - Further work is required in this area (e.g. intra-AS attestation based on RATS)
- Proof of transit can be an additional "auditing" tool on top of path authorization

Questions?

Nicola Rustignoli, SCION Association (nic@scion.org)