SCION

Joeri de Ruiter

SIDN LABS

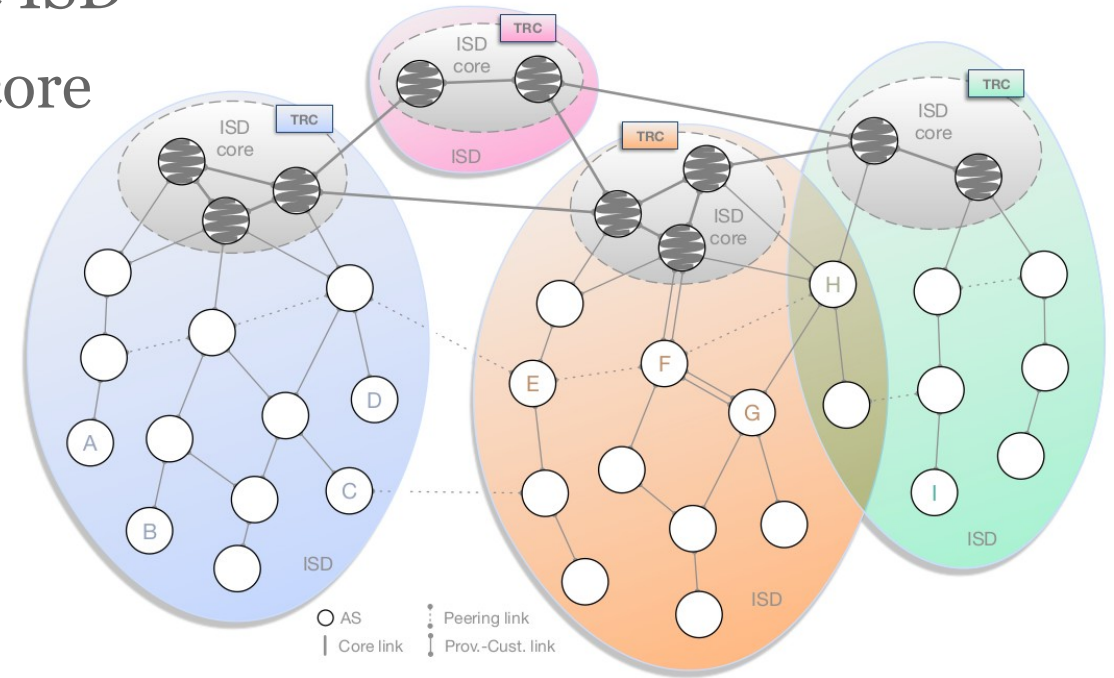
SCION

- Scalability, Control, and Isolation On Next-generation Networks
- New internet architecture
- Research at Network Security Group, ETH Zurich
- Scalability and security through Isolation Domains (ISDs)
  - Group of autonomous systems
  - E.g. per country or jurisdiction
- Routes authenticated both in control and data plane

SIDN LABS

Isolation Domains

- PKI organised per ISD
- ISD core: ASes managing the ISD
- Core AS: AS part of the ISD core
- Hierarchical control plane
  - Inter-ISD control plane
  - Intra-ISD control plane



Source: The SCION Internet Architecture: An Internet Architecture for the 21st Century, Barrera et al., 2017

Network paths

- Control plane – finding end-to-end paths
  - Path exploration
  - Path registration
- Data plane – sending packets
  - Path lookup
  - Path combination

SIDN LABS

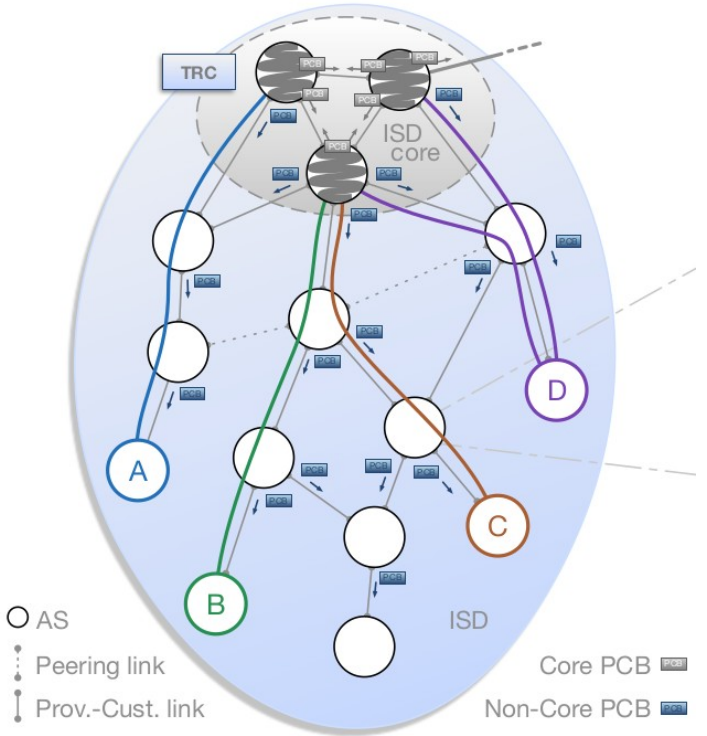
Control plane: path exploration

- Inter-ISD
  - Performed by core ASes
  - Flooding similar as with BGP
  - Less ASes involved (only core)
- Intra-ISD
  - Downstream multi-path flooding

SIDN LABS

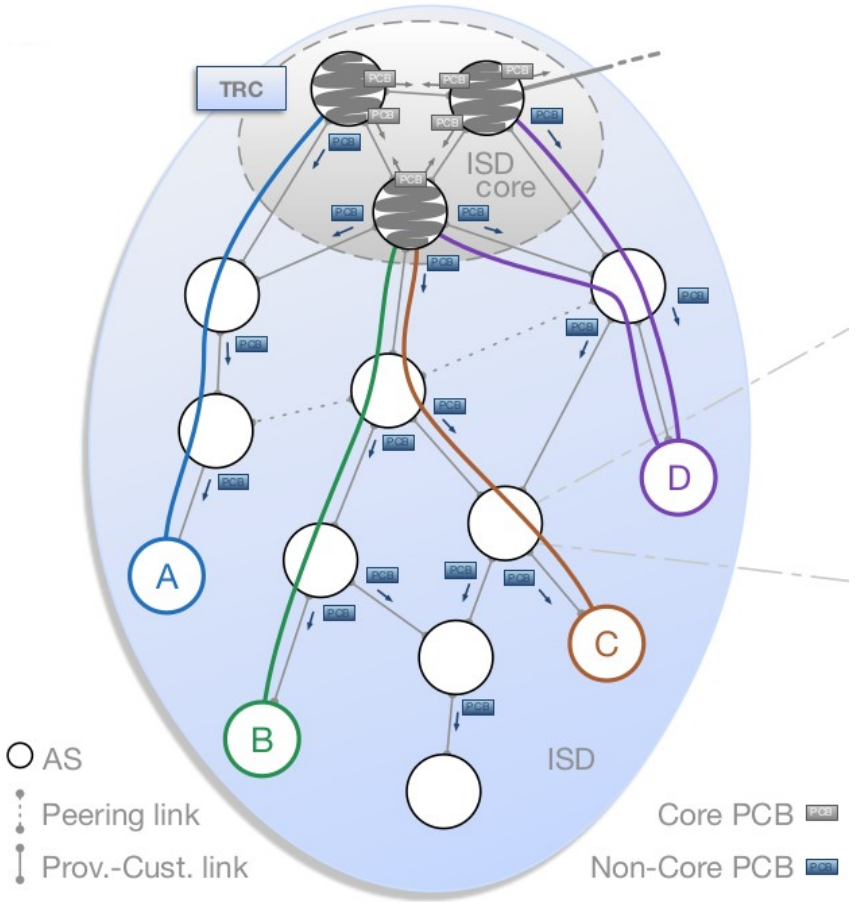
Intra-ISD path exploration and registration

- Path Construction Beacons (PCBs) sent downstream using multi-path flooding
  - Initialised by core ASes
  - Extended and forwarded by receiving ASes
  - Add incoming and outgoing interface and optional peerings
- Eventually all nodes know how ISD core can be reached
- Path registration
  - Preferred down-segments (path from core to AS) with path server in the core
  - Preferred up-segments registered with local path server in AS



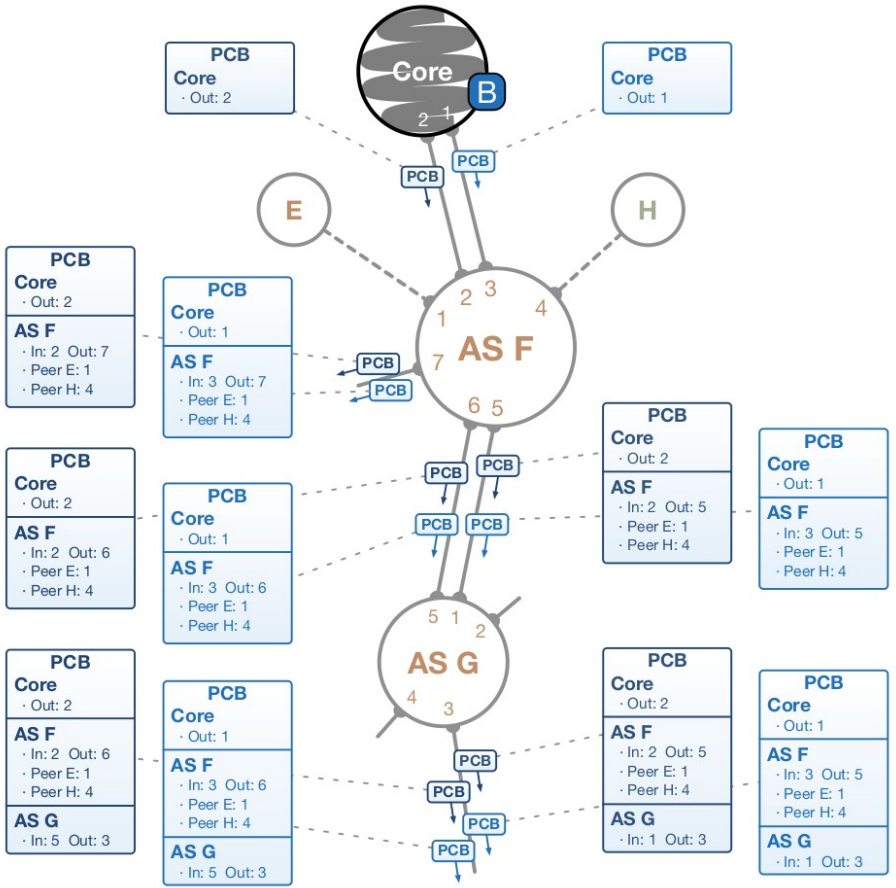
Source: The SCION Internet Architecture: An Internet Architecture for the 21st Century, Barrera et al., 2017

Intra-ISD path exploration and registration



Source: The SCION Internet Architecture: An Internet Architecture for the 21st Century, Barrera et al., 2017

Intra-ISD path discovery and registration

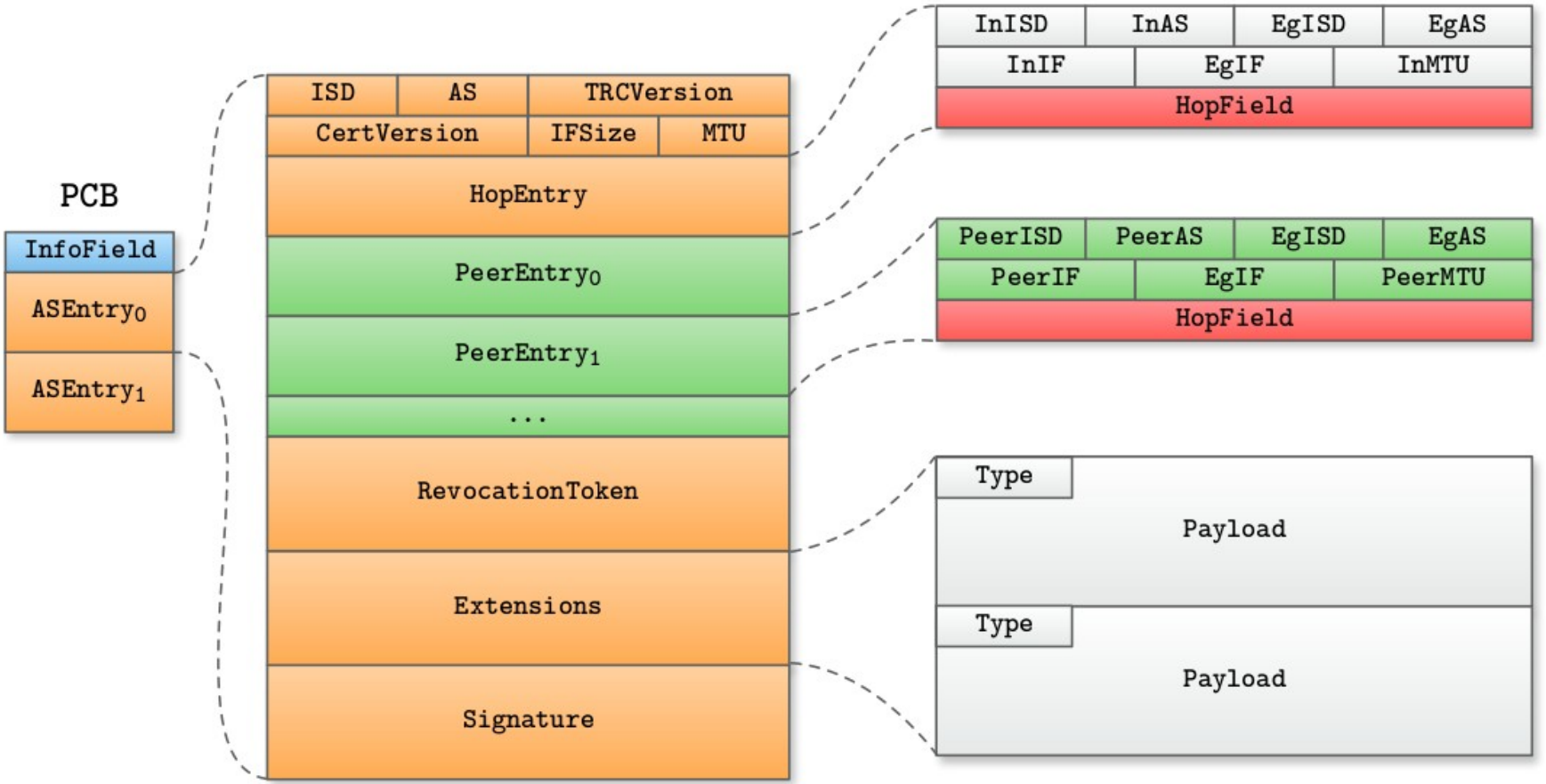


Source: The SCION Internet Architecture: An Internet Architecture for the 21st Century, Barrera et al., 2017

Path Construction Beacons

- Path Construction Beacons are signed by every AS along the path
- Hop fields (HF) included that can be used to later select paths
  - Contain MAC computed using hop field key
  - Only processed locally

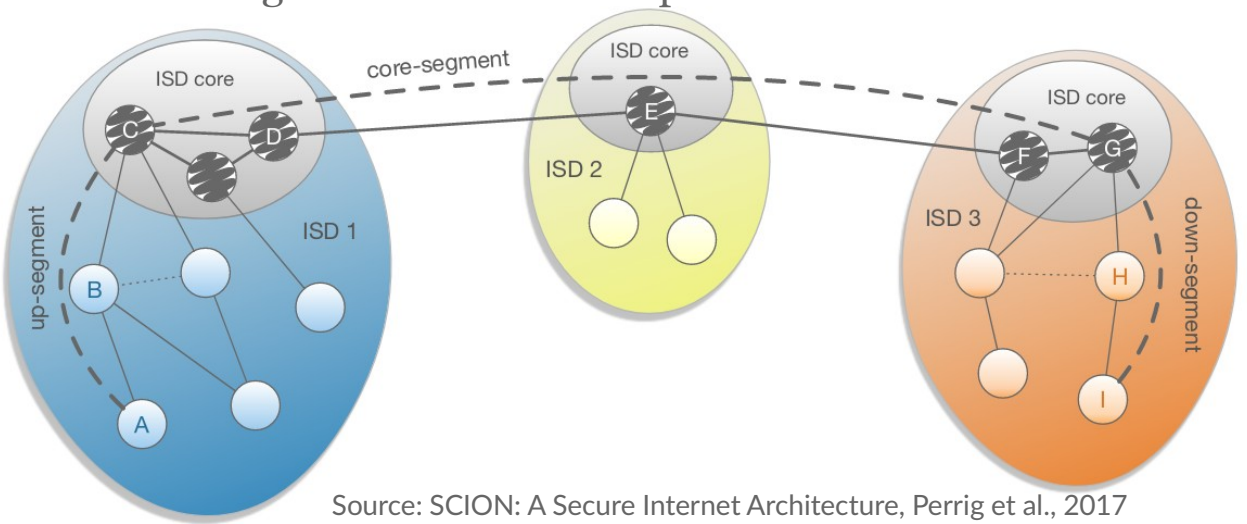
Path Construction Beacons



Source: SCION: A Secure Internet Architecture, Perrig et al., 2017

Data plane: path lookup and combination

- Path construction performed by end hosts
- Request route to (ISD, AS) from local path server
- Local path server replies with
  - Up-path segments to local ISD core
  - Down-path segment in remote ISD from core to destination AS
  - Core-path segments needed to connect up-path and down-path segments
- End hosts pick and combine segments to determine path



Source: SCION: A Secure Internet Architecture, Perrig et al., 2017

Data plane: path lookup and combination

- Path server caches path segments
- If path to AS in remote ISD is not present in cache:
  - Request core- and down-path segments from local core AS
  - Core AS requests down-path segments from core AS in remote ISD
  - Up-, core- and down-segments returned to end host

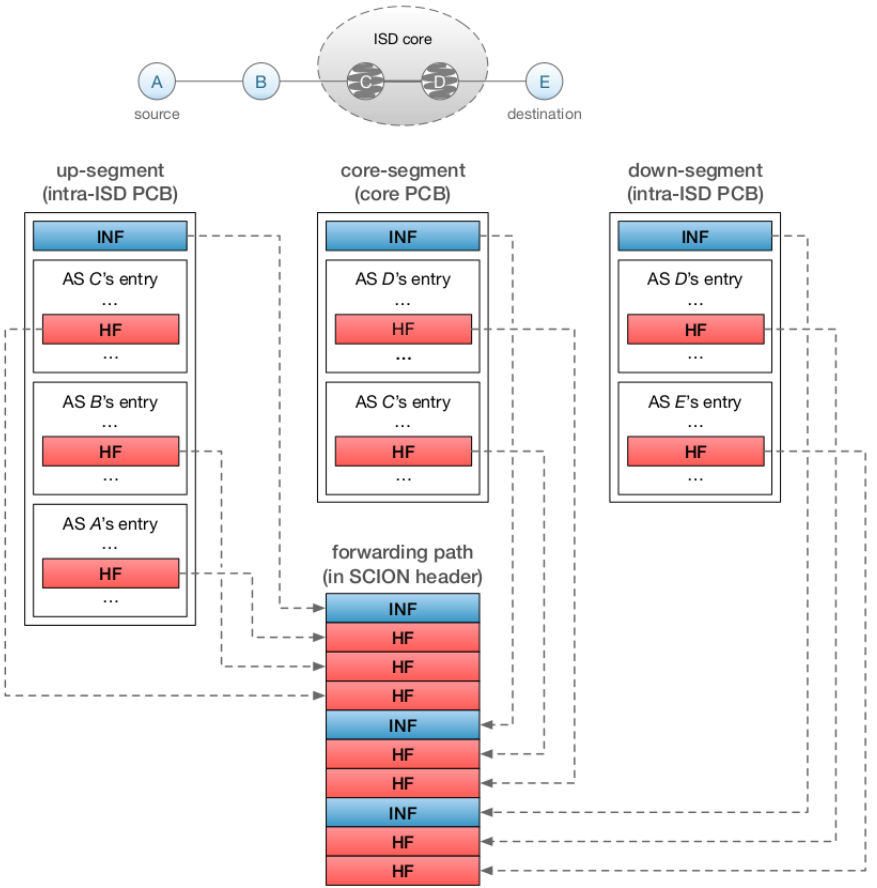
SIDN LABS

Routing

- Path information included in packet headers
  - Corresponding hop-field included
  - No forwarding information necessary at routers
  - Packet-carried forwarding state (PCFS)
- Sender selects the path
  - Possible to use multiple paths
- Recipient address no longer used to route between autonomous systems
  - Only used by the destination AS
  - Local delivery is responsibility of destination AS

SIDN LABS

Routing



Source: SCION: A Secure Internet Architecture, Perrig et al., 2017

Routing

- Possible paths determined by
  - Up-stream AS, by deciding which PCBs to forward to where
  - Local AS, by registering down-path segments with ISD core
  - Local AS, by offering path segments to clients
  - Clients, by combining path segments offered by local path server

SIDN LABS

Security

- Trust within ISD
  - Compromise is kept local → root key can only be used to compute certificates for local ISD
- PKI Control-plane
  - Comparable to RPKI
  - Short-lived certificates for ASes
- PKI Name-resolution
  - Comparable to DNSSEC
  - Typically ISD will delegate name resolution to TLDs
- PKI End-entity
  - Comparable to TLS
  - Certificates need to be signed by multiple CAs and registered at publicly verifiable log server

SIDN LABS

Features and extensions

- Hidden paths
- Redundancy through multi-path
- EPIC: Every Packet Is Checked
  - Level 1: unique MAC per packet
  - Level 2: Per-hop source authentication
- COLIBRI
  - Admission control (source authentication)
  - Resource allocation
  - Traffic policing
  - Traffic monitoring

SCION in practice

- Open source implementation available
- Can be combined with existing Internet (e.g. through gateways)
- SCIONLab: international research network
  - Open for everyone to connect to
- Used in practice by banks, government and hospitals
- At SIDN Labs
  - Permanent infrastructure node (AS) connected to SCIONLab
  - Implementation of SCION on open networking hardware

Follow us


SIDN.nl


@SIDN


SIDN

Thanks for your attention!

joeri.deruiter@sidn.nl
www.sidnlabs.nl