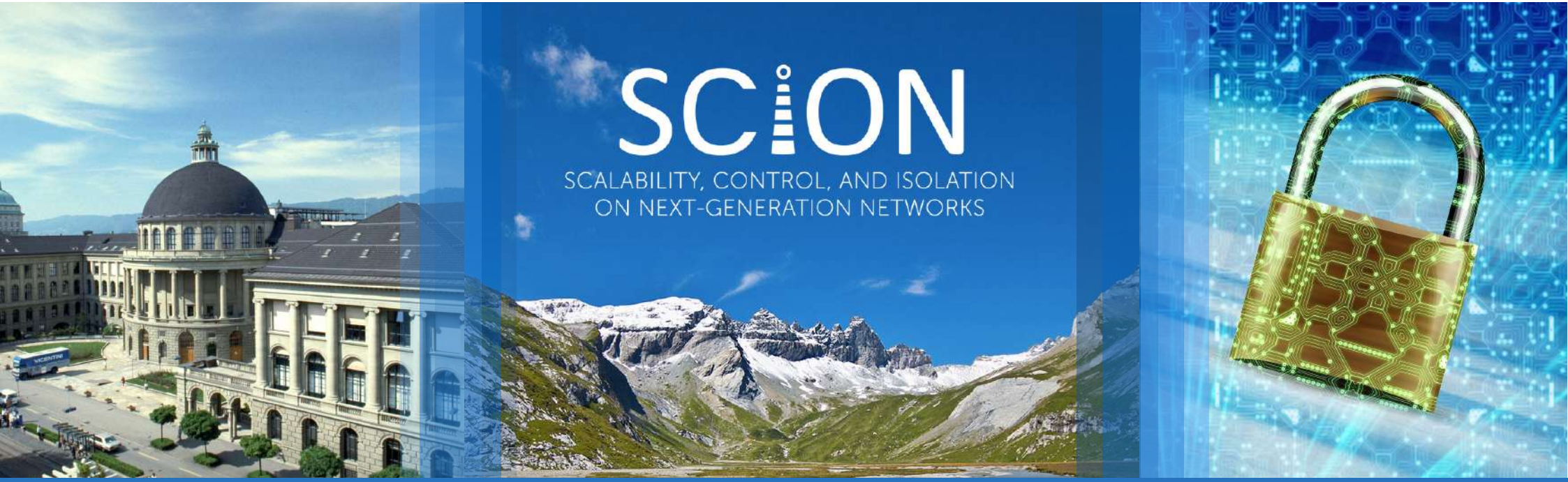


Experiencing a new Internet Architecture

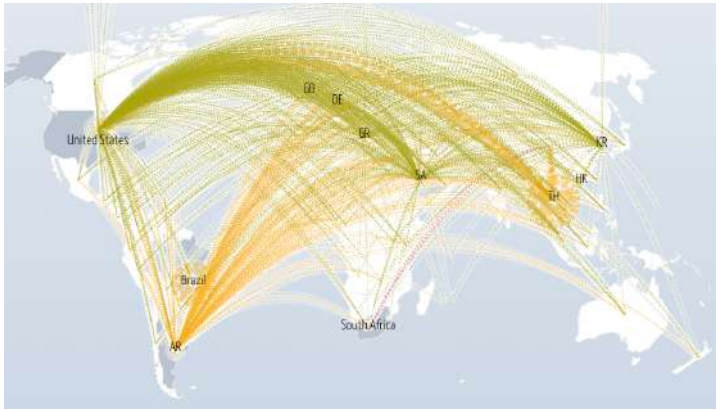
Adrian Perrig, Network Security Group

ETH zürich

SCION

The Internet is on Fire!

- Lack of sovereignty
- Frequent outages
  - https://downdetector.com
- Constant DDoS attacks
  - https://www.digitalattackmap.com
- Frequent routing attacks
  - https://bgpstream.com
- Lack of communication guarantees
- Expensive maintenance



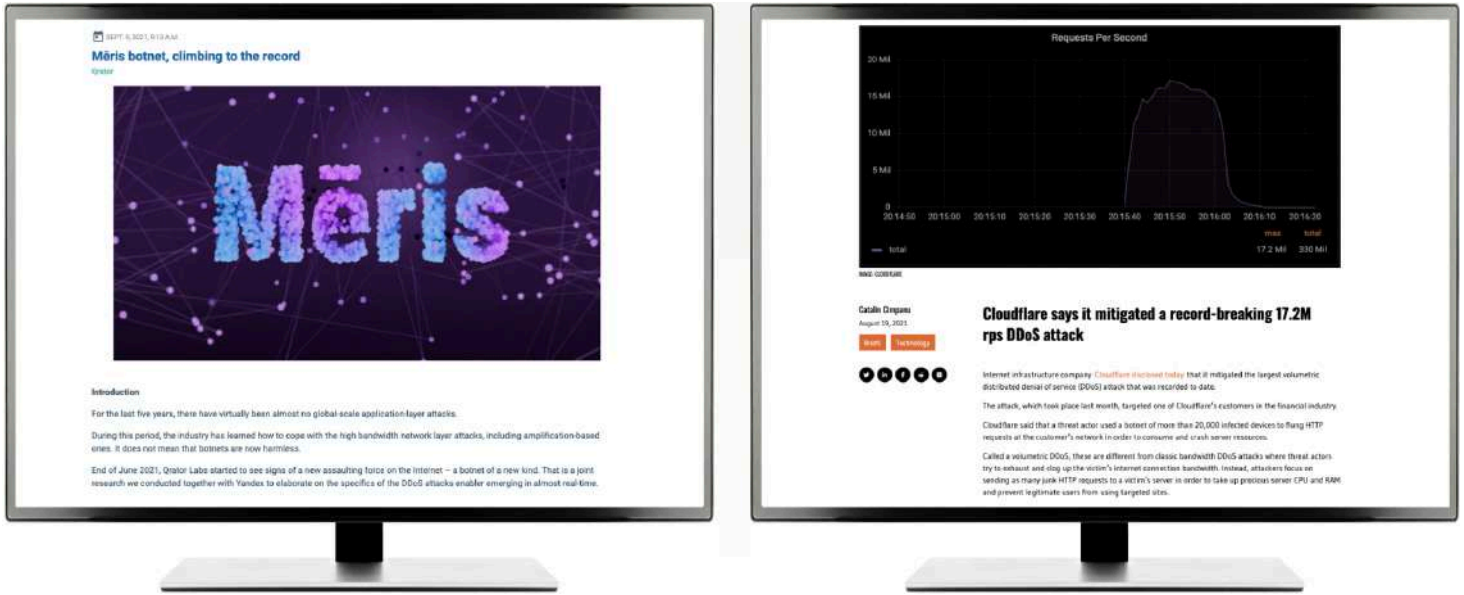
ETH zürich

SCION

Ransom DDoS Attacks on the Rise

Network security attacks continue to be relevant:

- Ransom DDoS attacks on the Rise: recent Meris botnet capable to send over 300 Tbps!
- Routing attacks through BGP hijacking occur daily

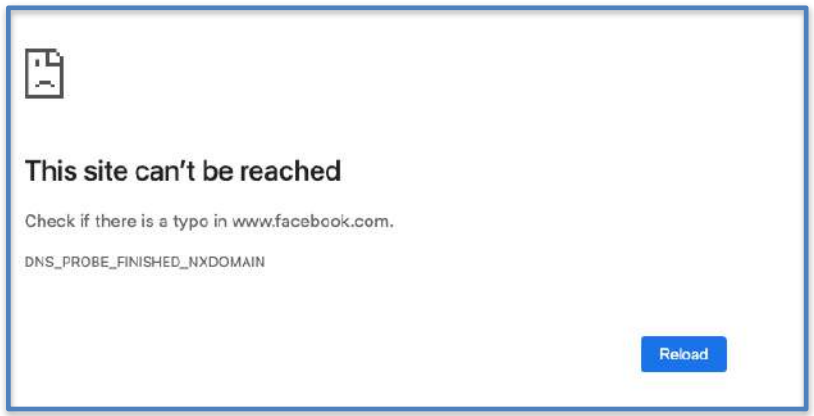


ETH zürich

SCION

Facebook Outage (4 Oct 2021)

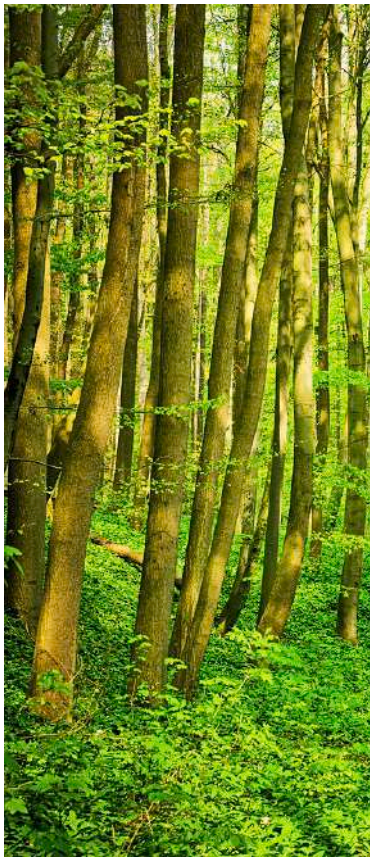
- Over 6 hour global downtime of Facebook, Instagram, WhatsApp
- BGP management system detected an issue and withdrew routes to entire Facebook DNS infrastructure
- Circular dependencies resulted in cascading failures
  - Administrators could not reach data center any more and could not log in to fix the problem
  - Door locks used the Internet to verify credentials, so personnel could not enter building any more



Inspirations for a New Beginning

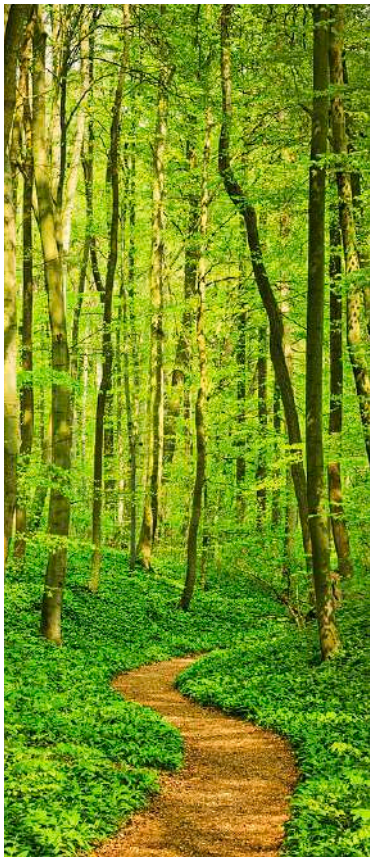
- Many exciting next-generation Internet projects over the past 25 years
- General Future Internet Architectures (FIA)
  - XIA: enhance flexibility to accommodate future needs
  - MobilityFirst: empower rapid mobility
  - Nebula (ICING, SERVAL): support cloud computing
  - NIMROD: improved scale and flexibility
  - NewArch (FARA, NIRA, XCP)
  - RINA: clean API abstractions simplify architecture
- Content-centric FIAs: NDN, CCNx, PSIRP, SAIL / NETINF
- Routing security: BGPSEC, S-BGP, soBGP, psBGP, SPV, PGBGP, H-NPBR
- Path control: MIRO, Deflection, Path splicing, Pathlet, I3
- Inter-domain routing proposals: ChoiceNet, HLP, HAIR, RBF, AIP, POMO, ANA, ...
- Intra-domain / datacenter protocols: SDN, HALO, ...

Discoveries on our Journey

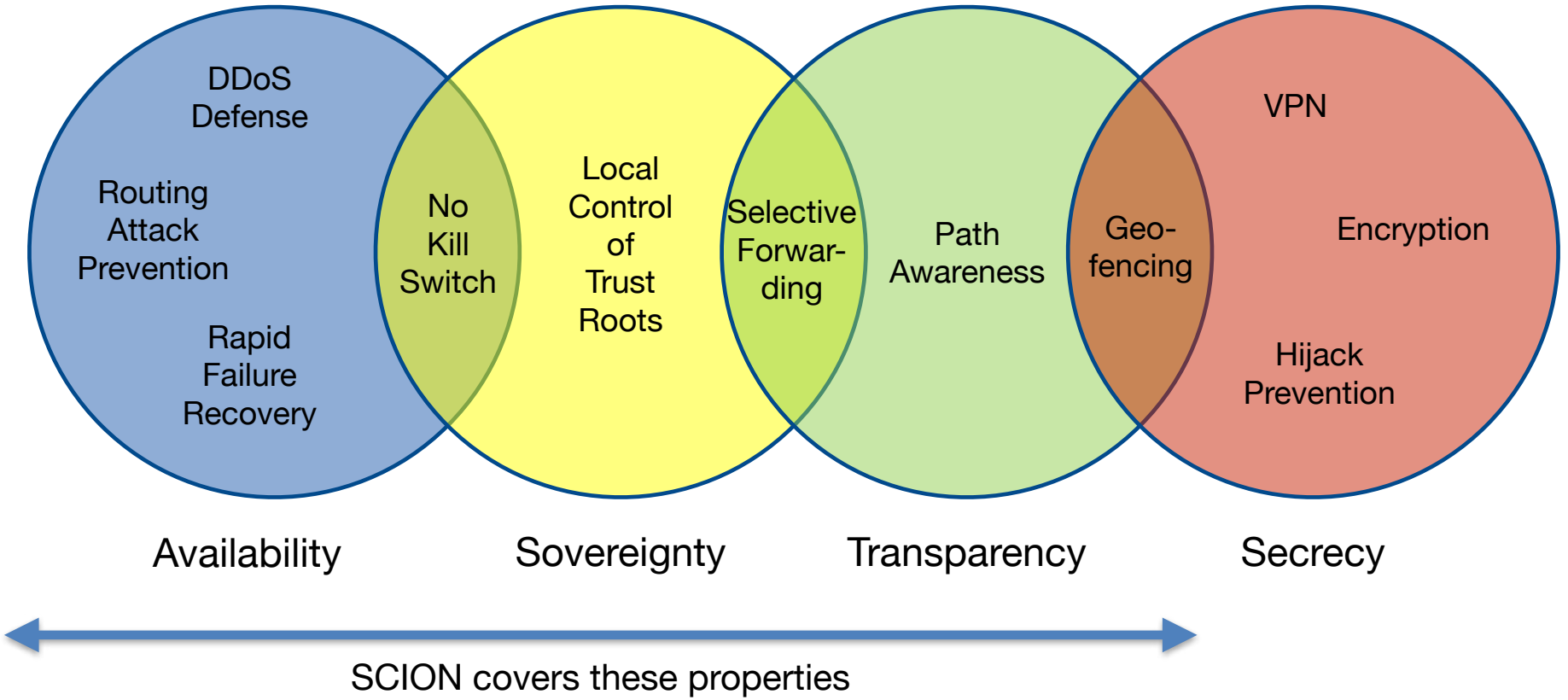


- During our journey, we have encountered many interesting discoveries
- Several discoveries suggest new approaches for inter-domain networking

The real voyage of discovery consists not in seeking new landscapes, but in having new eyes. Marcel Proust



Important Properties: Availability, Sovereignty, Transparency, Secrecy

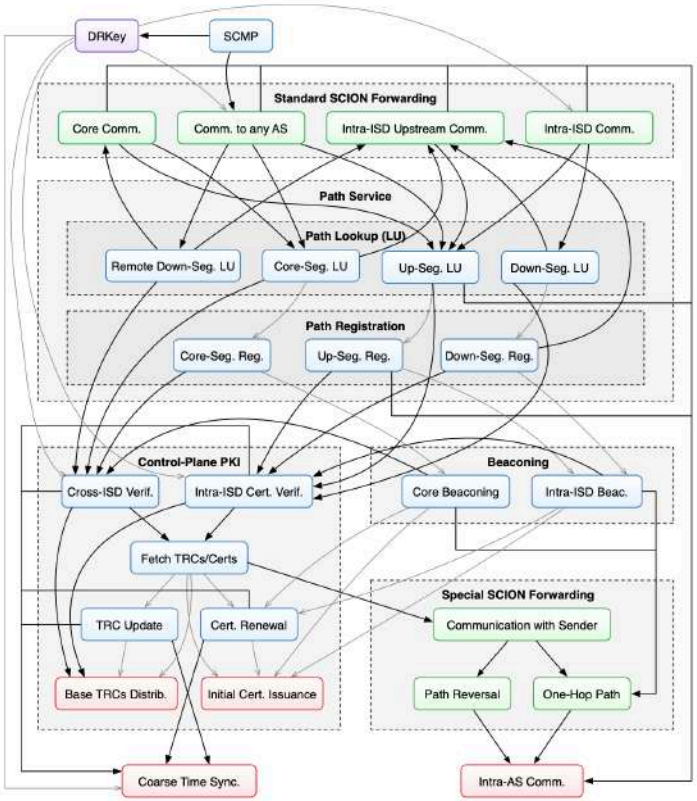


SCION Architecture Principles

- Stateless packet forwarding (no inconsistent forwarding state)
- “Instant convergence” routing
- Path-aware networking
- Multi-path communication
- Sovereignty and transparency for trust roots
- High security through design and formal verification

Dependency Analysis

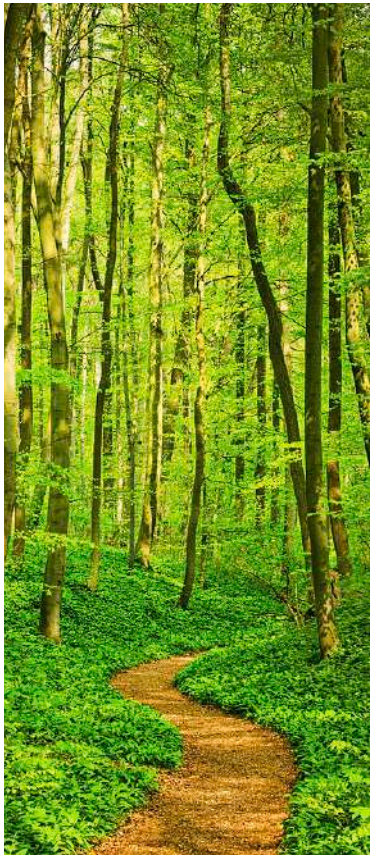
- Absence of circular dependencies is important for reliability
- Design of SCION ensures no circular dependencies exist



ETH zürich

Insight: Formal Security Verification Necessary

- To achieve strong assurance for a large-scale distributed system, formal security verification is necessary
- Performing formal verification from the beginning avoids “difficult-to-verify” components
  - Many design aspects of SCION facilitate formal verification
- Collaboration with David Basin’s and Peter Müller’s teams in the VerifiedSCION project

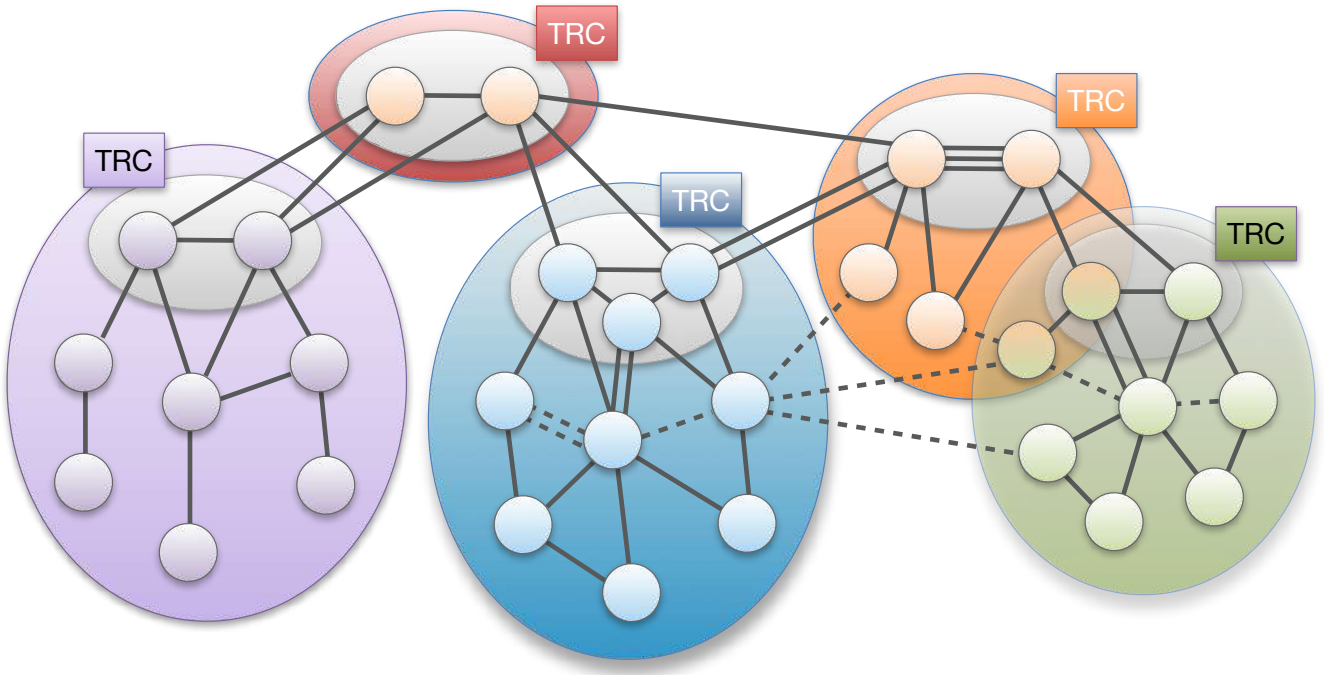


ETH zürich

VerifiedSCION

Approach for Scalability: Isolation Domain (ISD)

- Isolation Domain (ISD): grouping of Autonomous Systems (AS)
- ISD core: ASes that manage the ISD and provide global connectivity
- Core AS: AS that is part of ISD core



SCION Overview in One Slide

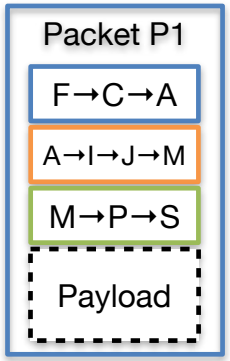
Path-based Network Architecture

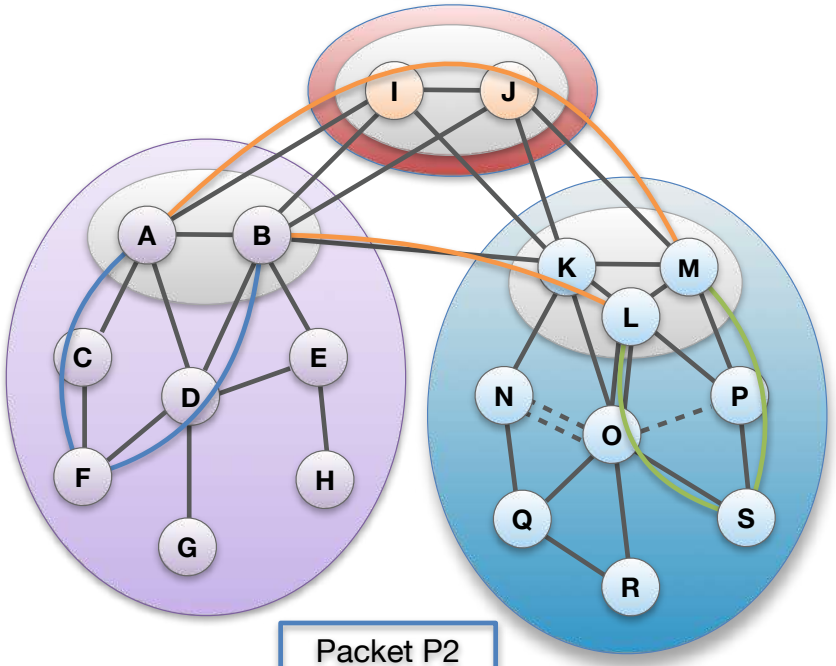
Control Plane - Routing

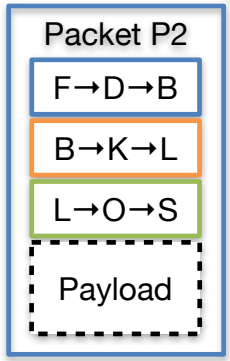
- Constructs and Disseminates Path Segments

Data Plane - Packet forwarding

- Combine Path Segments to Path
- Packets contain Path
- Routers forward packets based on Path
  - Simple routers, stateless operation



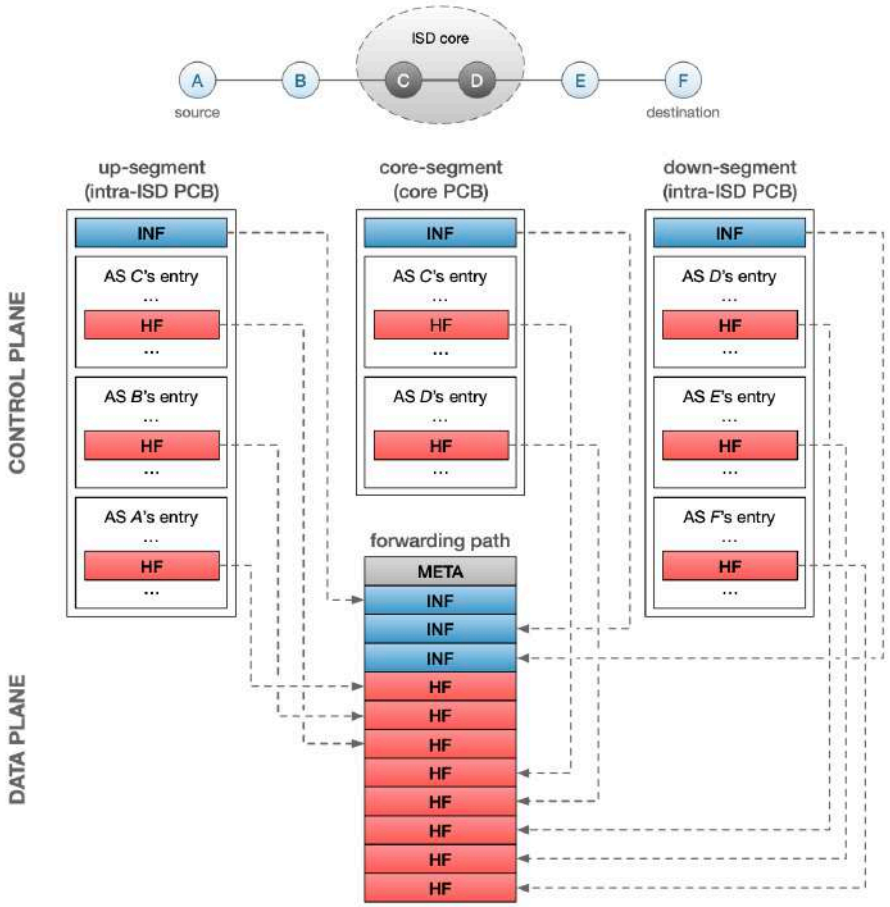




SCION

SCION Control and Data Plane

- Three main functions of the control plane
  1. Path exploration → path segments
  2. Path dissemination → senders requests segments
  3. Certificate dissemination/renewal
     → needed for segment verification
- Path segments contain forwarding and meta information. Meta information can include geographical location of routers, MTU, bandwidth, link latency…
- Senders extract the forwarding information from the path segments to form complete end-to-end paths
- Forwarding information is encoded in the packet header. Routers only verify the authenticity of the information
  → two AES operations replace longest-prefix match

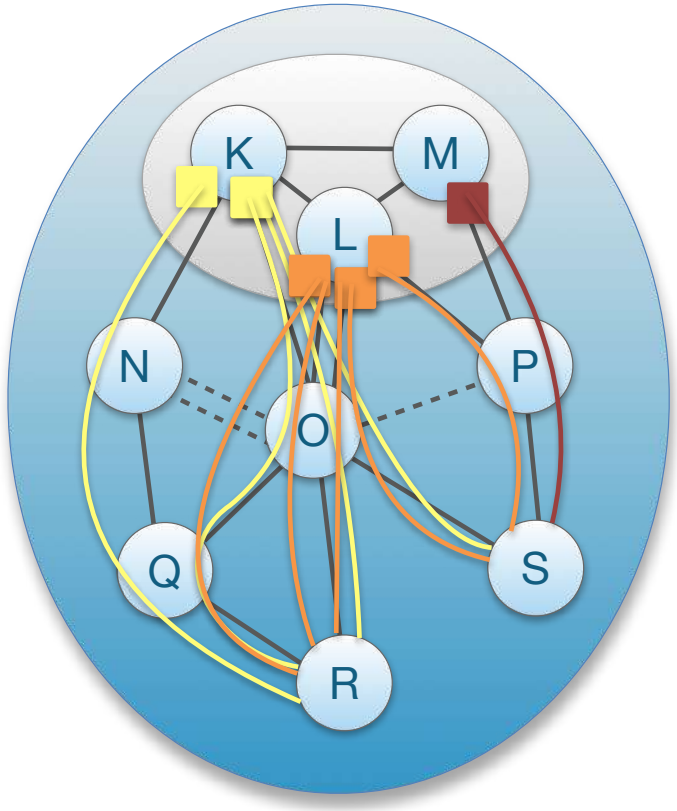


ETH zürich

SCION

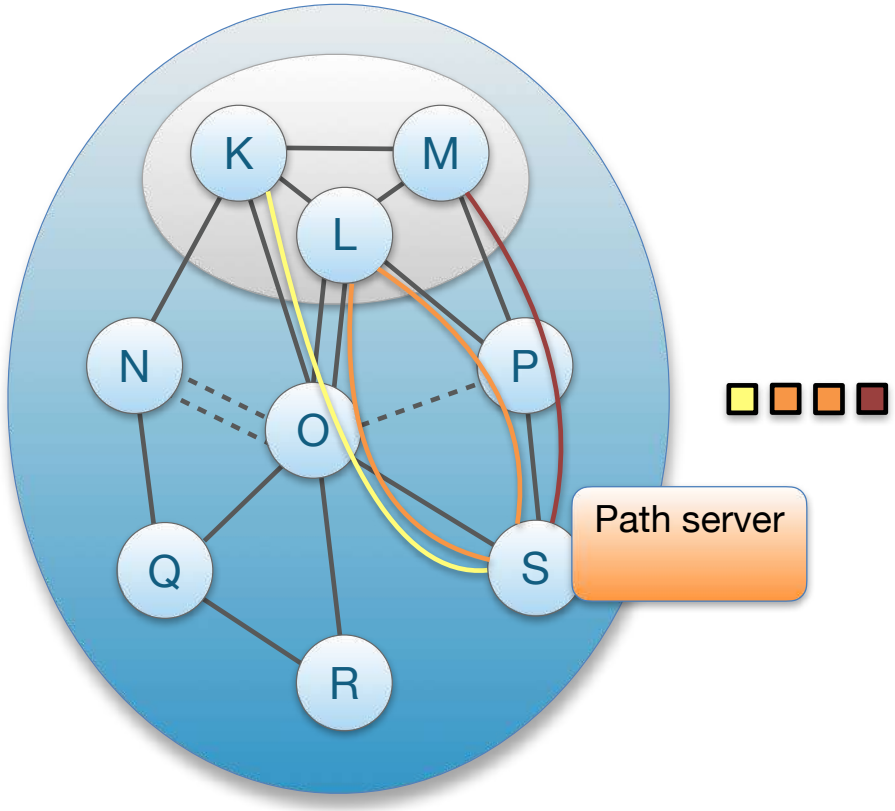
Intra-ISD Path Exploration: Beaconing

- Core ASes K, L, M initiate Path-segment Construction Beacons (PCBs), or "beacons"
- PCBs traverse ISD as a flood to reach downstream ASes
- Each AS receives multiple PCBs representing path segments to a core AS



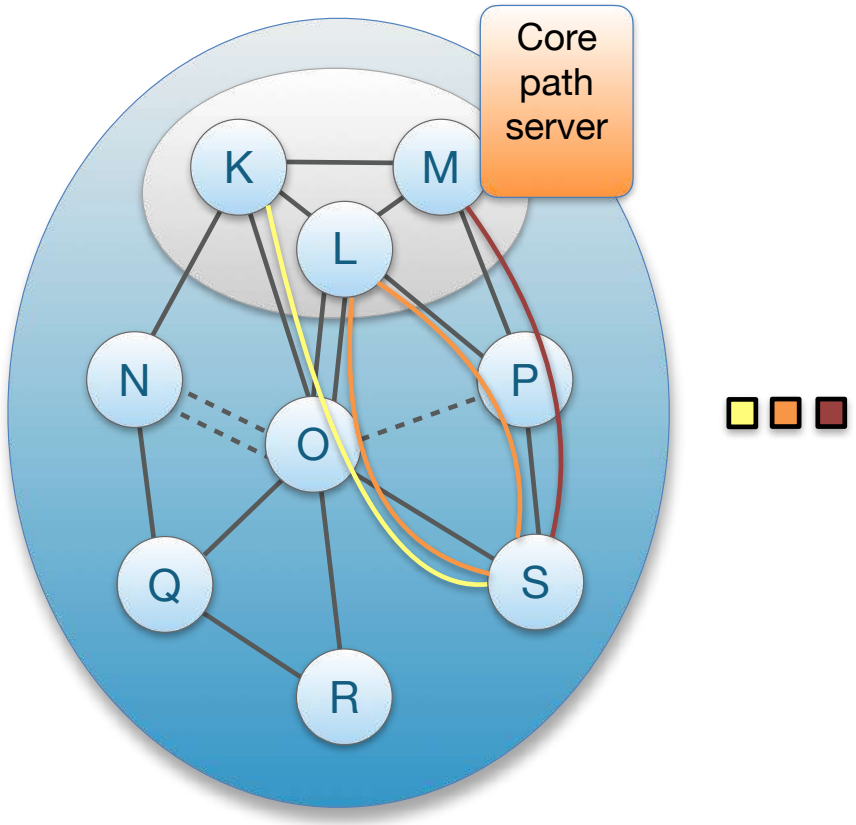
Up-Path Segment Registration

- AS selects path segments to announce as up-path segments for local hosts
- Up-path segments are registered at local path servers



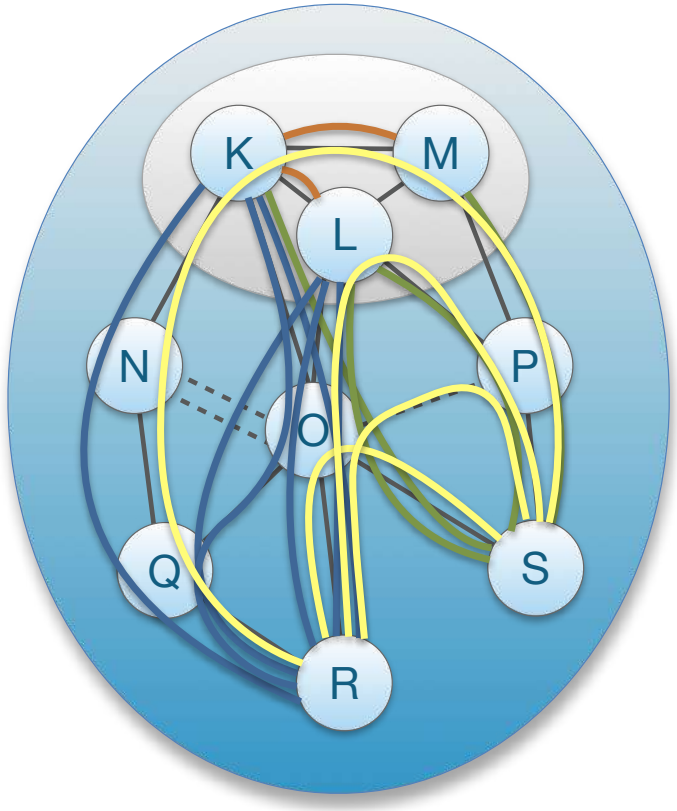
Down-Path Segment Registration

- AS selects path segments to announce as down-path segments for others to use to communicate with AS
- Down-path segments are uploaded to core path server in core AS



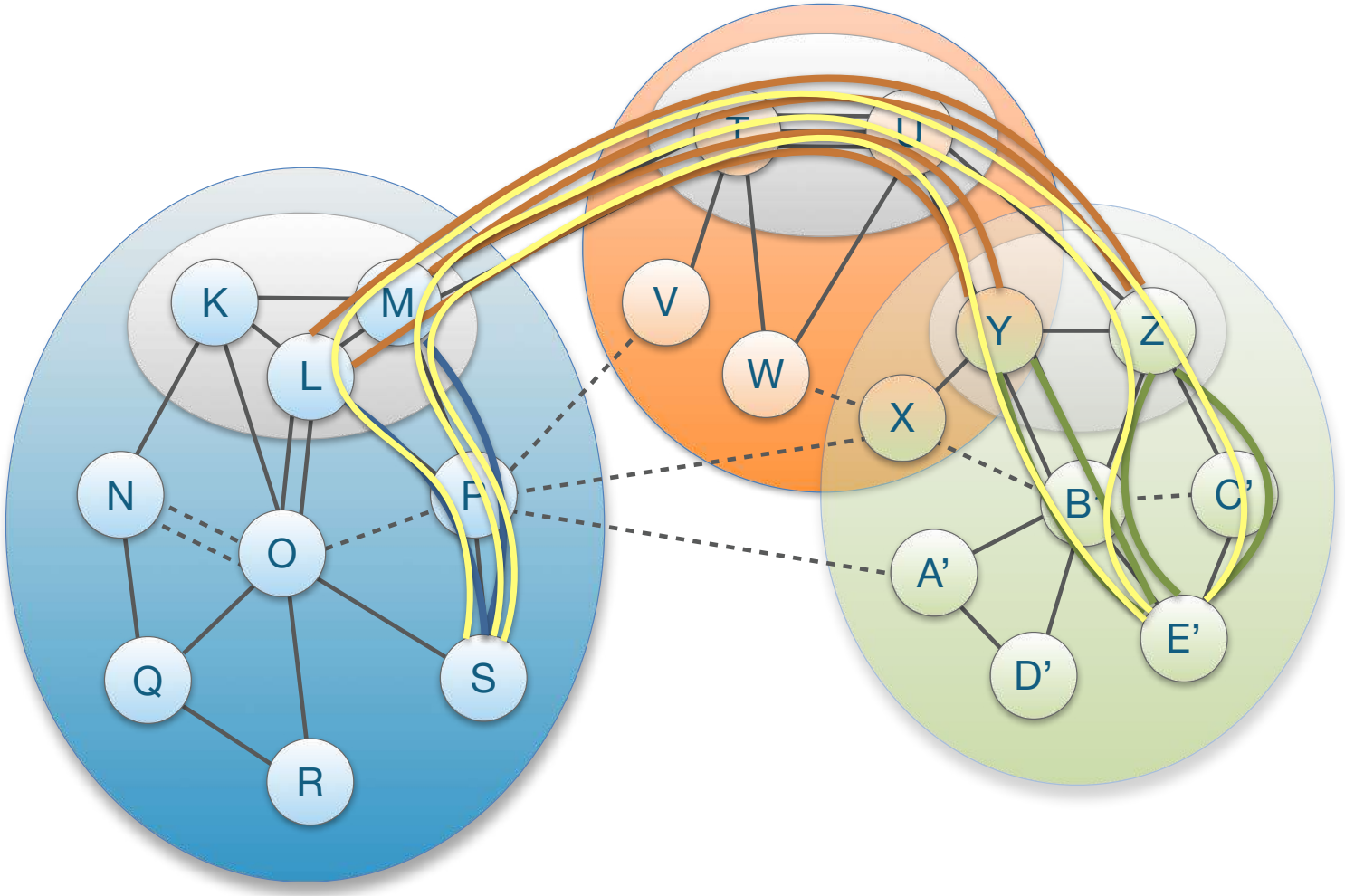
Communication within ISD

- Client obtains path segments
  - Up-path segments to local ISD core ASes (blue)
  - Down-path segments to destination (green)
  - Core-path segments as needed to connect up-path and down-path segments (orange)
- Client combines path segments to obtain end-to-end paths (yellow)



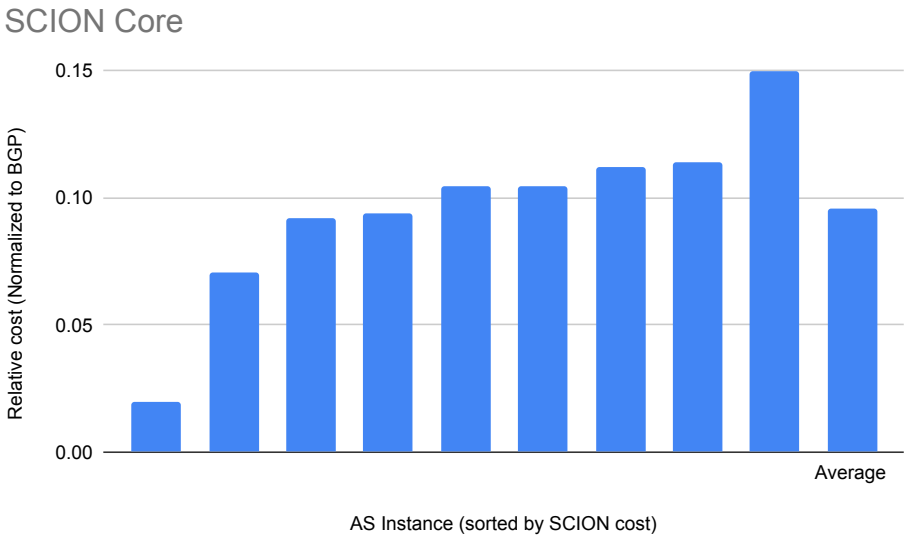
Communication to Remote ISD

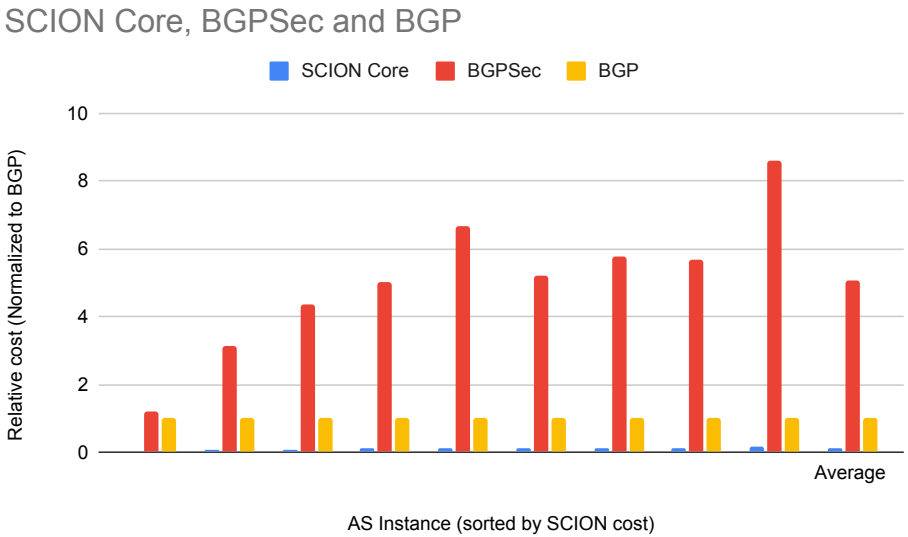
- Host contacts local path server requesting <ISD, AS>
- If path segments are not cached, local path server will contact core path server
- If core path server does not have path segments cached, it will contact remote core path server
- Finally, host receives up-, core-, and down-segments



ETH zürich

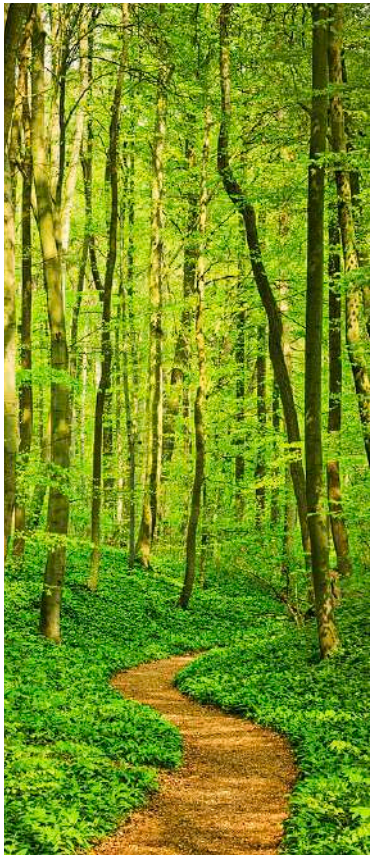
Scalability of SCION Core Beaconing





Scalability Study Results

- On a per-path basis, SCION overhead about 200 times lower than BGP, and about 1000 times lower than BGPsec
- Time-to-connectivity in SCION is over 3 orders of magnitude faster than BGP
  - The iterative convergence approach in BGP takes minutes to converge with fully updated forwarding tables (in case of small changes), sometimes even hours in case of large-scale outages



SCION Drawbacks

Initial Latency Inflation

- ❖ Additional latency to obtain paths
- ✓ BUT amortized by caching & path reuse

Bandwidth Overhead

- ❖ Due to paths in the packets
- ❖ About 80 additional bytes
- ✓ Enables path control, simpler data plane, etc

Increased Complexity in Key Mgmt.

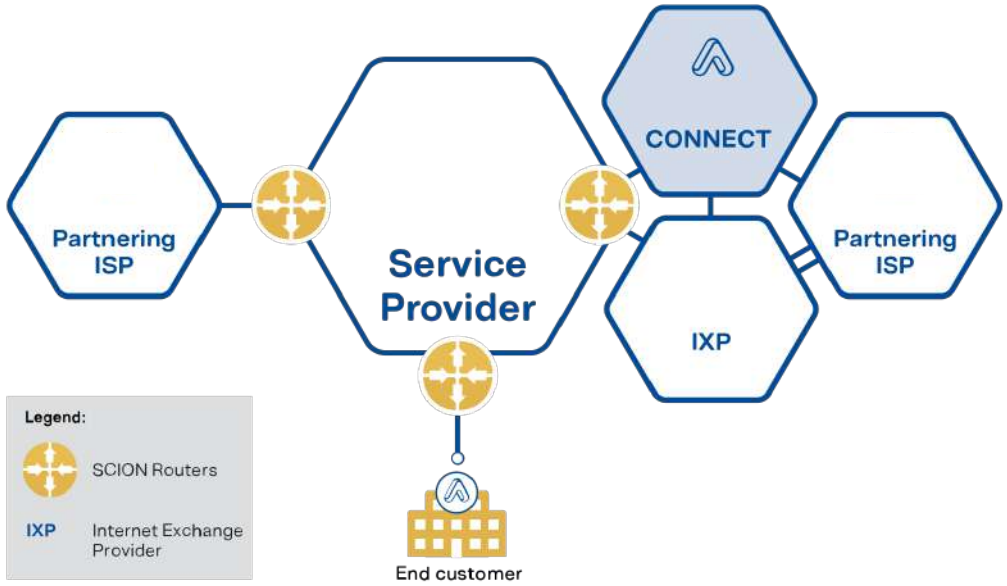
- ❖ New certificates (e.g., TRC Certificates)
- ✓ High security design

Initial Set-up Cost

- ❖ Training network operators
- ❖ Installing new infrastructures
- ✓ Offers methods to facilitate deployment

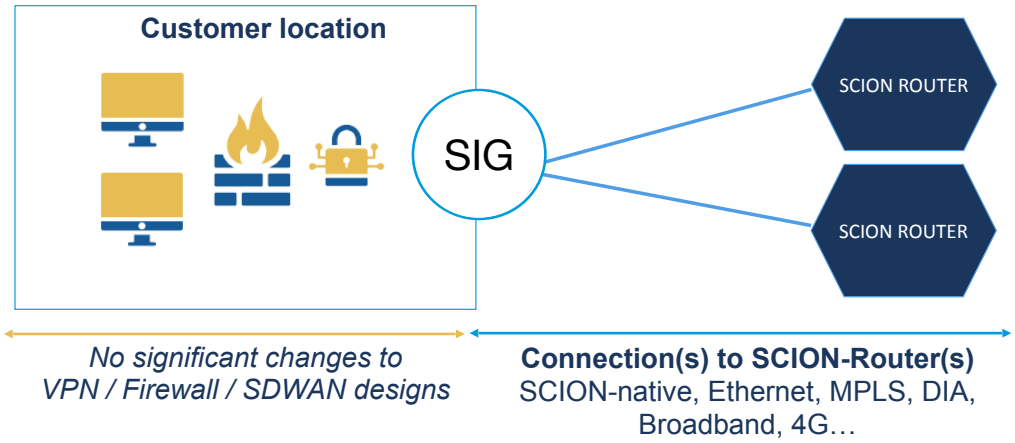
How to Deploy SCION: ISP

- CORE Routers are set up at the borders of an ISP
  - to peer with other SCION-enabled networks
  - to collect customer accesses
- No change to the internal network infrastructure of an ISP needed!



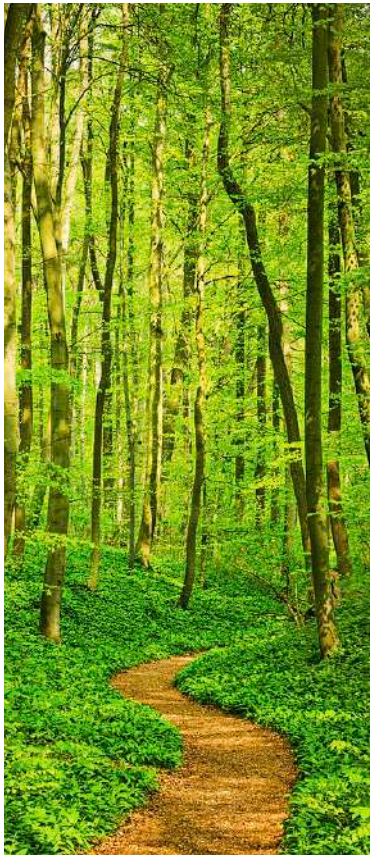
How to Deploy SCION: End Domain

- SCION IP Gateway (SIG) enables seamless integration of SCION capabilities in end-domain networks
- No upgrades of end hosts or applications needed



Insight: Incremental Deployment Possible

- Incremental deployment of a new Internet architecture is possible, operating side-by-side with BGP
- For ISPs, new architecture can be deployed with minimal effort
- For end domains, SCION-IP Gateway (SIG) offers immediate benefits without updating any end hosts
- Important: no reliance on BGP for inter-domain operation ("BGP-free")
  - Overlay / insecure underlay should be avoided not to inherit vulnerabilities
- Re-use of intra-domain network architecture for local communication



SCION Production Network

- Led by Anapaya Systems 

- **BGP-free global communication**
  - Fault independent from BGP protocol

- Deployment with international ISPs
  - Goal: First **global public secure** communication network
- Construction of SCION network backbone at select locations to bootstrap adoption
- Current deployment
  - ISPs: Swisscom, Sunrise, SWITCH, + others joining soon
  - IXPs: SwissIX offers SCION peering, + others joining soon
  - Bank deployment: 4 major Swiss banks, some in production use

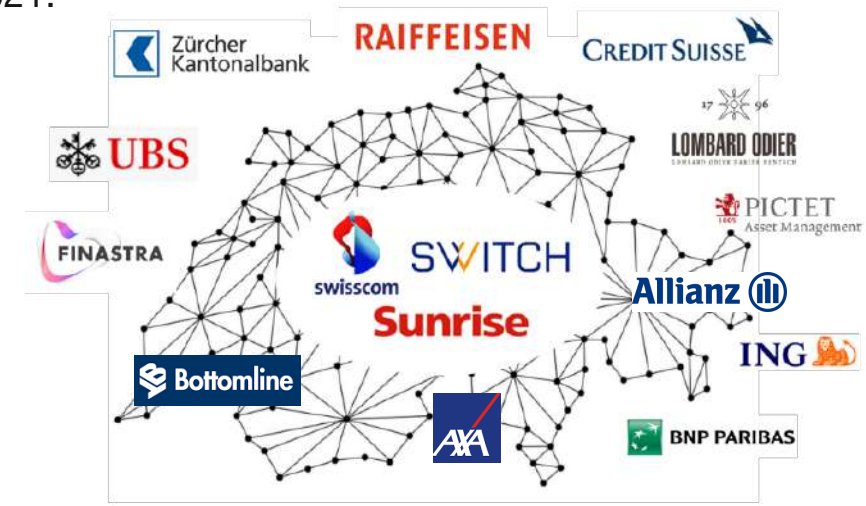
Secure Swiss Finance Network (SSFN)

The Swiss Interbanking Clearing system in numbers:

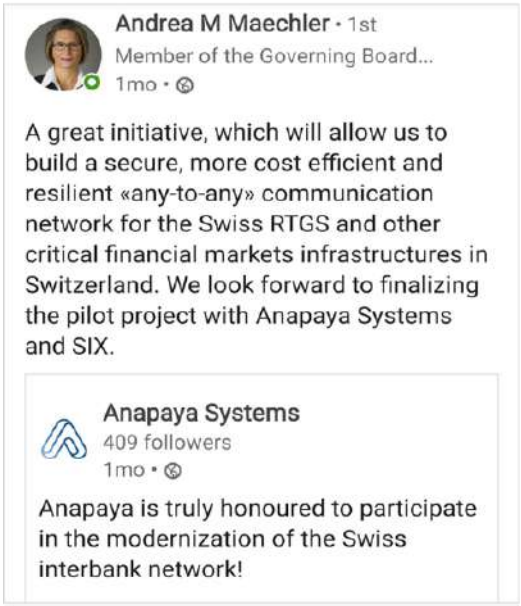
- 321 participants, including 280 banks, 14 insurance companies and 12 securities firms
- 2.9 million transaction representing 178 billion CHF per day

SSFN: Secure Swiss Finance Network

The new secure, reliable, community-based and sovereign network announced in July 2021:



Logos are illustrative



Technologies to Drive Deployment

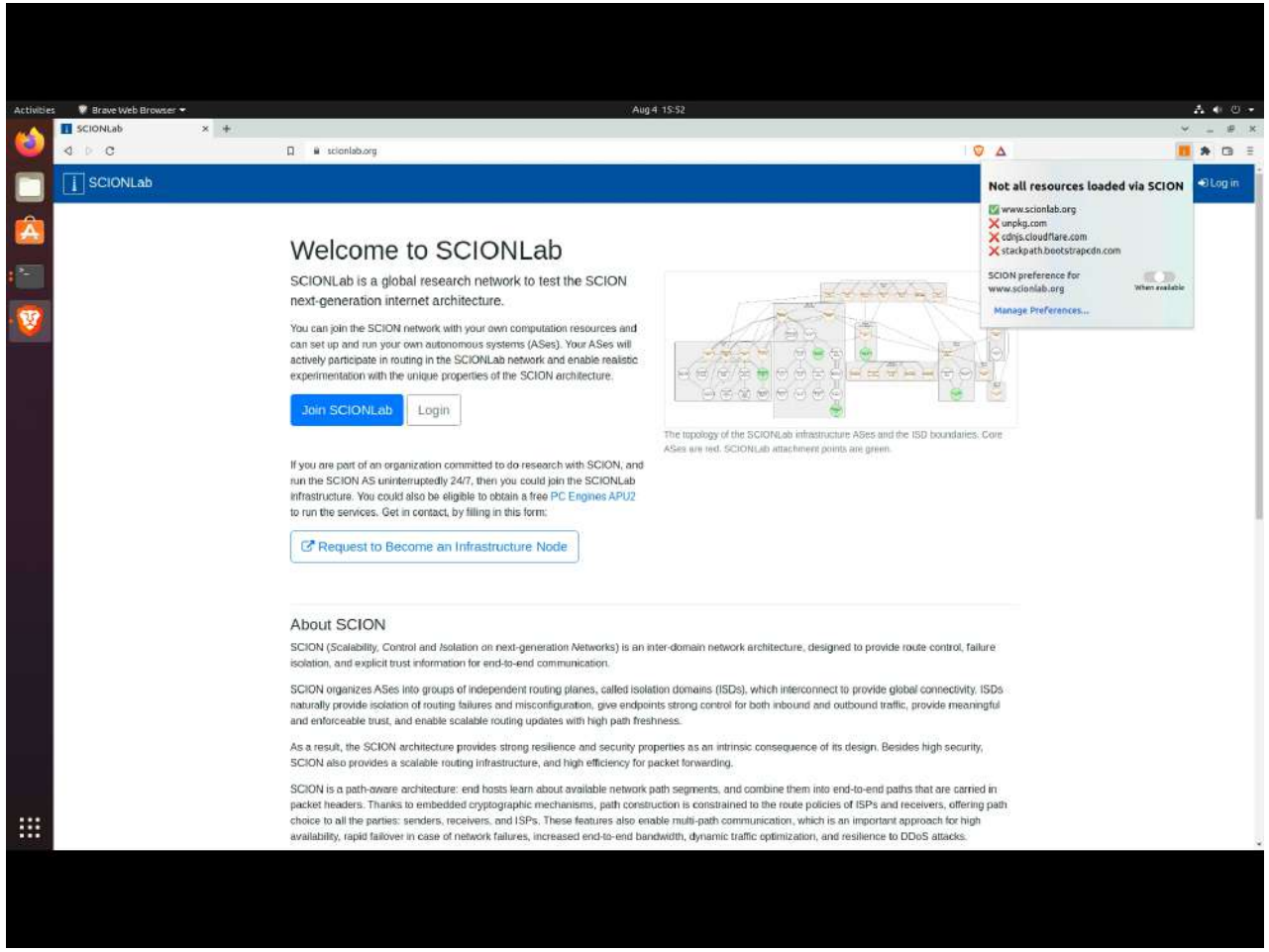
- Changes required: change required, no change required

- SCION-IP Gateway (SIG) deployed at local AS
  - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- Secure home office: Carrier-Grade SIG deployed at ISP
  - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- In-application deployment will take advantage of SCION if present in local AS
  - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- “Happy eyeballs” standard with SCION support
  - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)
- Secure Backbone AS (SBAS) approach
  - ISP (src, dst), Leaf AS (src, dst), OS (src, dst), App (src, dst)

brave SCION

- Collaboration with Brave browser team to build native SCION communication into browser
- Without OS support, SCION-enabled browser can directly fetch web pages over the SCION network if host is within SCION-enabled network
- Compelling advantages
  - Download speed optimization
  - Specific optimizations possible: low carbon footprint paths, low delay, high bandwidth, low jitter, low loss, …
- 60M enabled devices would help spur SCION adoption

brave Demo



ETH zürich

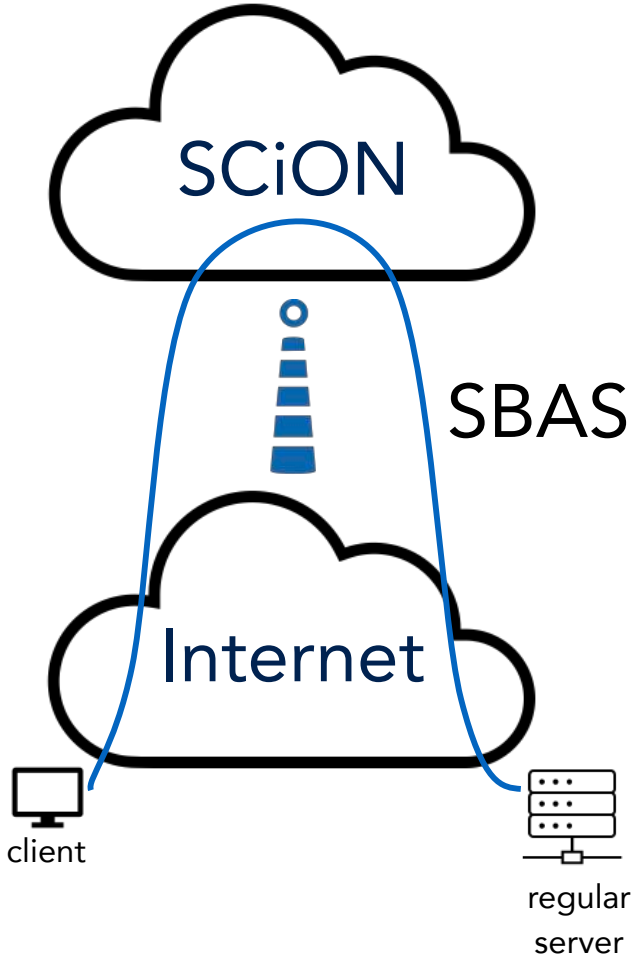
SCION

Secure Backbone AS (SBAS) Project

SBAS optimizes **regular** Internet traffic, using the SCiON backbone

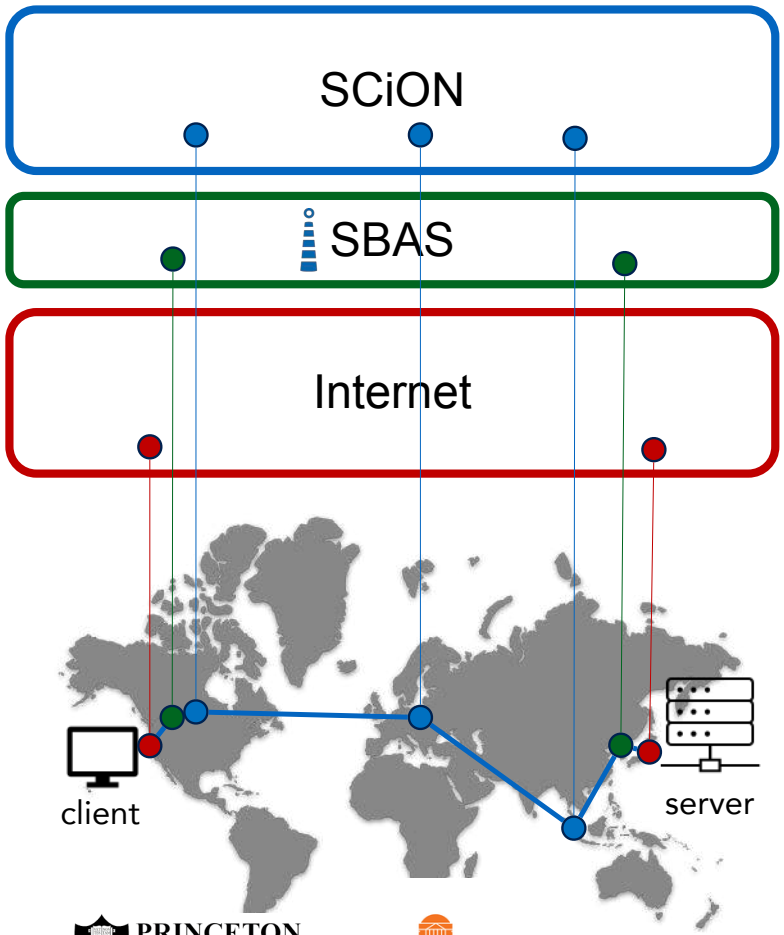
- Optimizing latency, CO_2, security
- Transparent to Internet hosts
- Promising system to get traffic onto the SCiON network

Key point: no upgrade to source or destination!



ETH zürich PRINCETON UNIVERSITY UNIVERSITY of VIRGINIA SCiON

Secure Backbone AS (SBAS) Project



Hijack-resilient enterprise network
For security-conscious enterprise customers

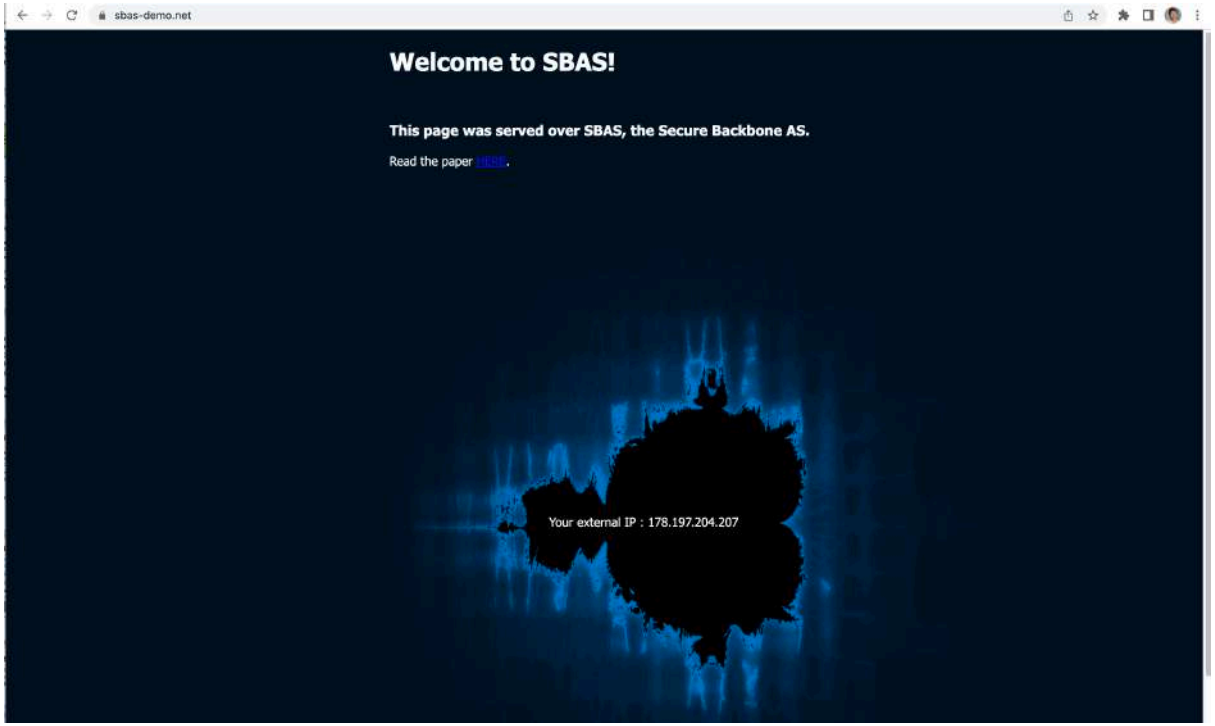
Green Internet
Improved carbon efficiency for private customers

Gaming Internet
A latency-optimized home connection for private customers

ETH zürich PRINCETON UNIVERSITY UNIVERSITY of VIRGINIA SCION

SBAS Demo is Live

- https://www.sbas-demo.net
- https://sbas.netsec.ethz.ch

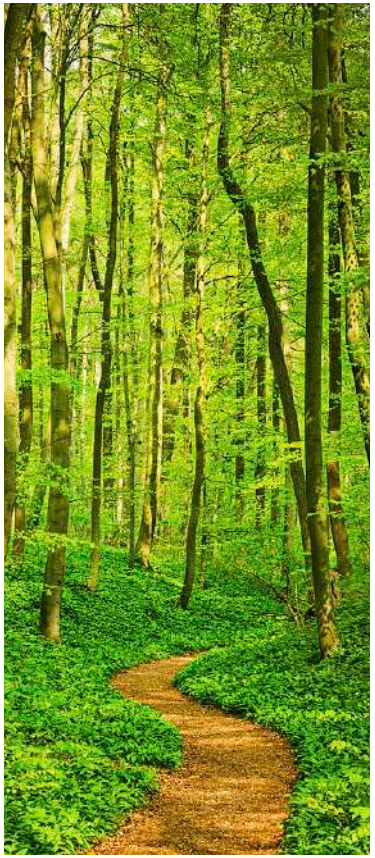


ETH zürich

SCION

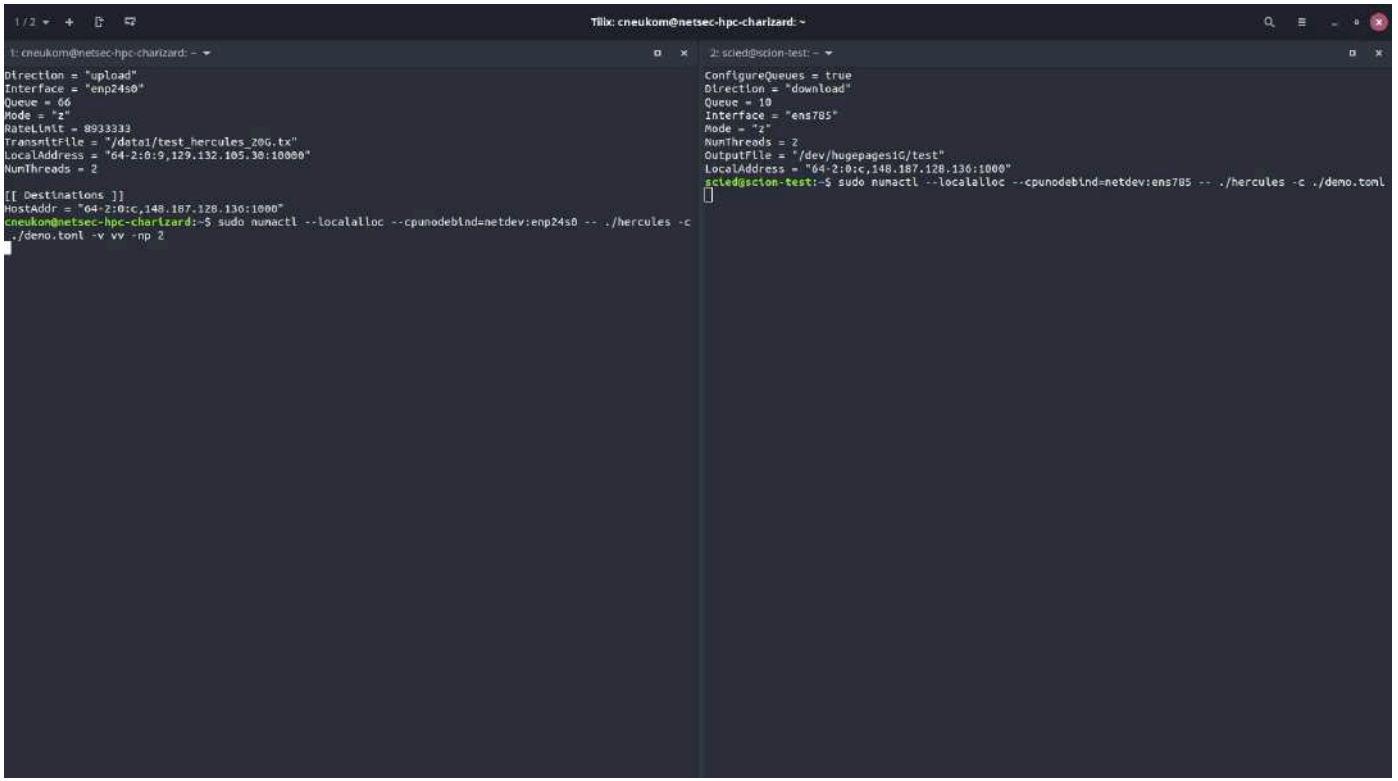
Insight: Incremental Deployment Possible

- Incremental deployment of a new Internet architecture is possible, operating side-by-side with BGP
- For ISPs, new architecture can be deployed with minimal effort
- For end domains, SCION-IP Gateway (SIG) offers immediate benefits without updating any end hosts
- Important: no reliance on BGP for inter-domain operation ("BGP-free")
  - Overlay / insecure underlay should be avoided not to inherit vulnerabilities
- Re-use of intra-domain network architecture for local communication



Demo: Sending 20Gbytes ETH to CSCS

- Single path metrics
  - Duration: 14.6 s
  - Avg: 11 Gbps
  - Max: 16.4 Gbps

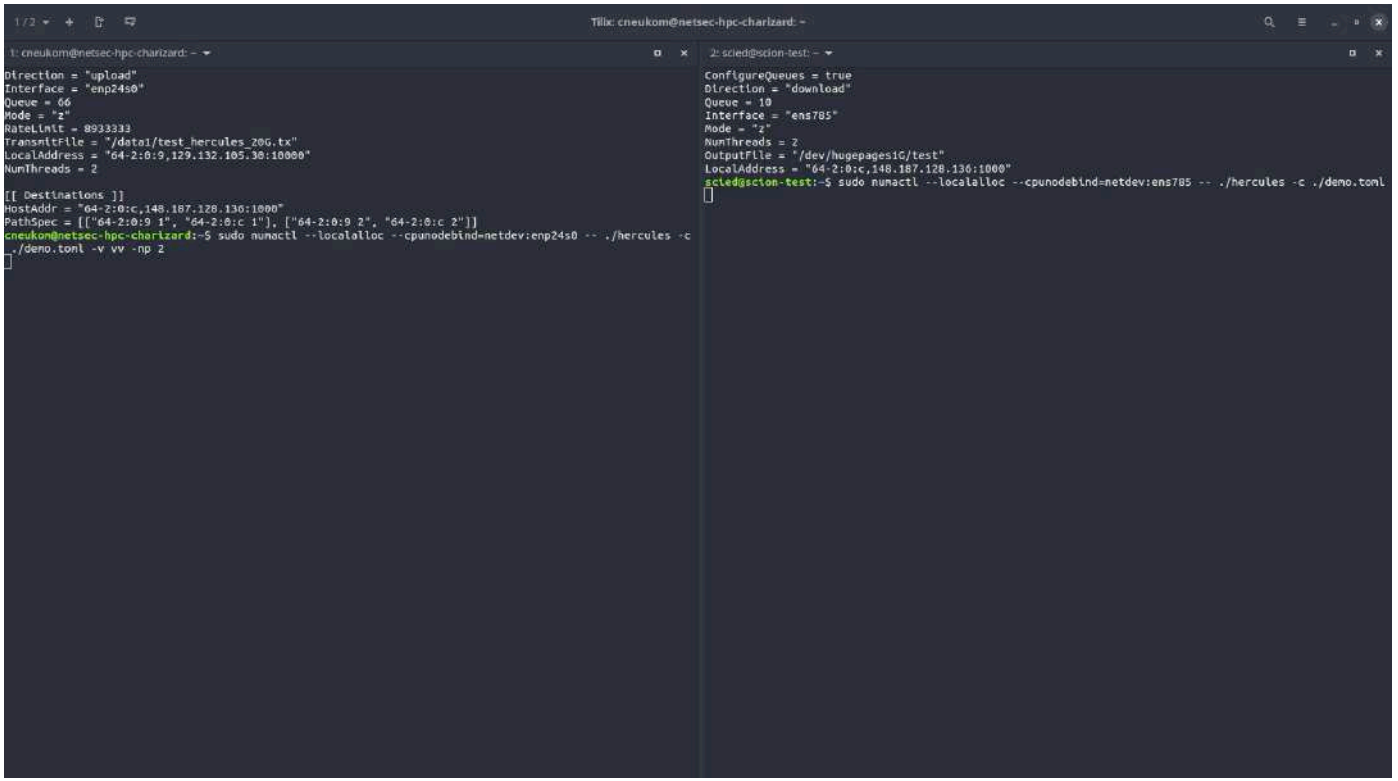


ETH zürich

SCION

Demo: Sending 20Gbytes ETH to CSCS

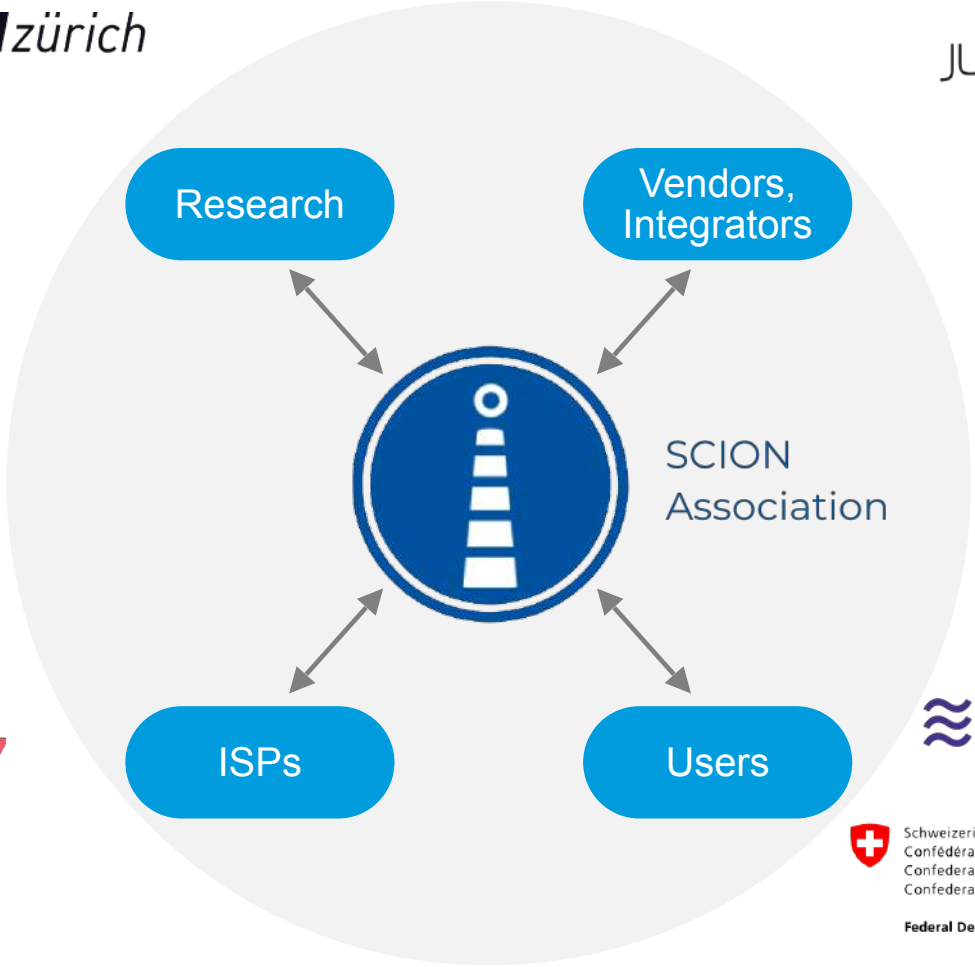
- 2-paths used, as both ETH and CSCS have 2 SCION connections to SWITCH
  - Duration: 8.1 s
  - Avg: 20 Gbps
  - Max: 30 Gbps



ETH zürich

SCION

SCION Association



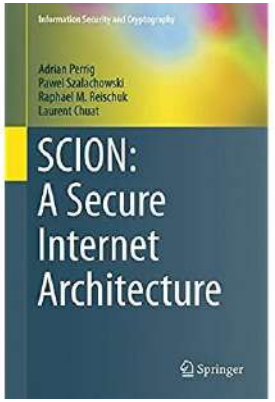
Startups

Bank

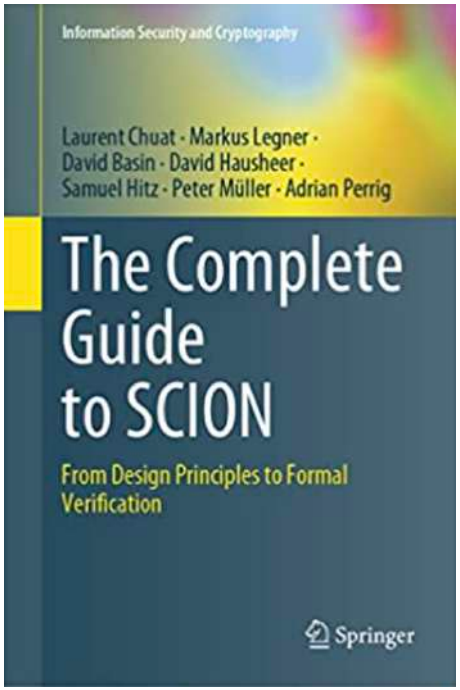
SCION Extensions

Online Resources

- https://www.scion-architecture.net
  - Book, papers, videos, tutorials
- https://www.scionlab.org
  - SCIONLab testbed infrastructure
- https://www.anapaya.net
  - SCION commercialization
- https://github.com/scionproto/scion
  - Source code
- SCION Association: https://www.scion.org



2017



2022

SCION Summary

- SCION: Next-generation Internet you can use today!
- High-performance
  - Path-aware network enables application-specific optimizations to provide enhanced efficiency
  - Multi-path communication enables simultaneous use of multiple paths, increasing available bandwidth
- Secure, high assurance, high availability
  - Per-packet authentication verification possible on routers
  - Formal verification of protocols and code
  - Immune against routing attacks, e.g., BGP prefix hijacking

SCION Team