SCION

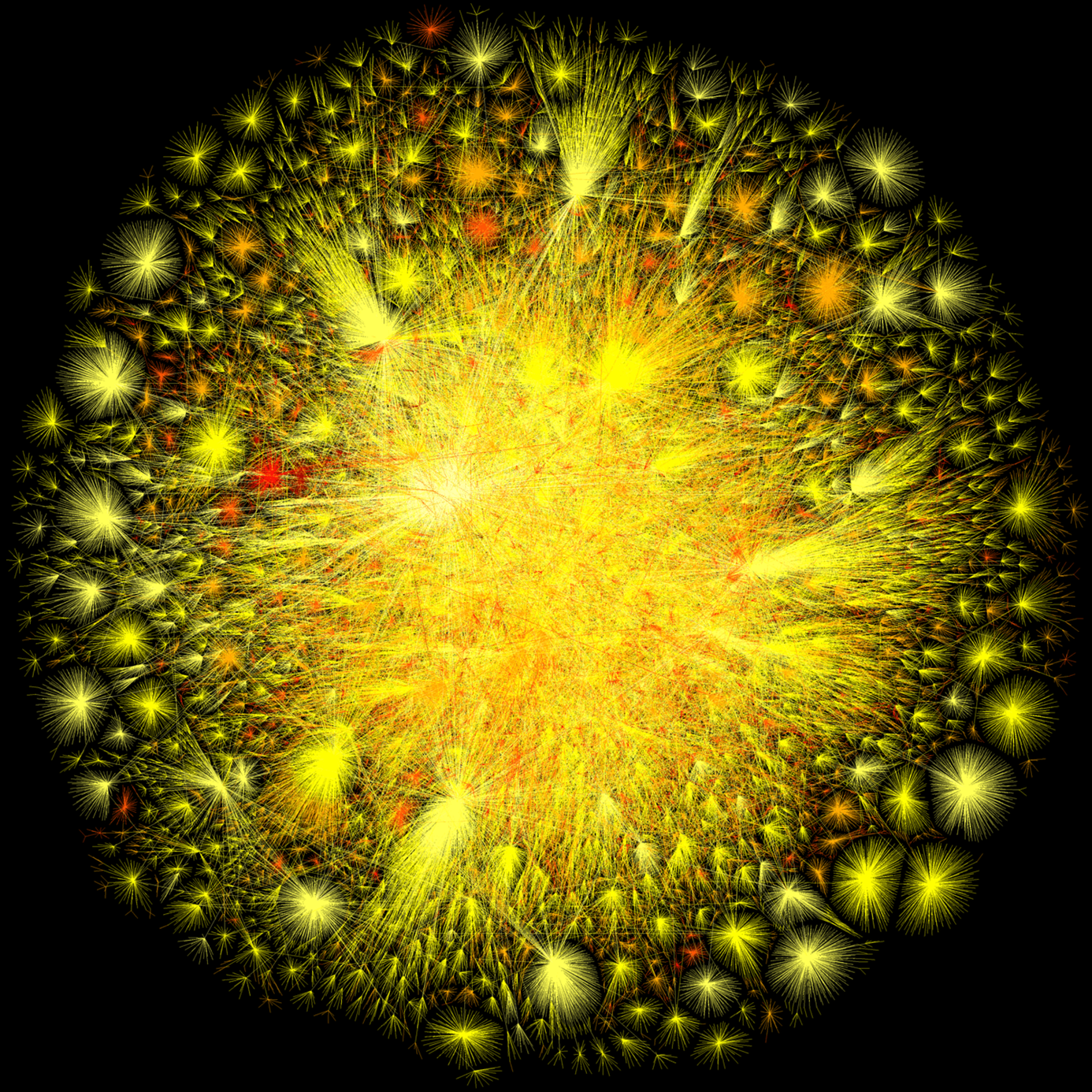
SCALABILITY, CONTROL, AND ISOLATION
ON NEXT-GENERATION NETWORKS

High Availability and Resilience for Business Continuity

Adrian Perrig

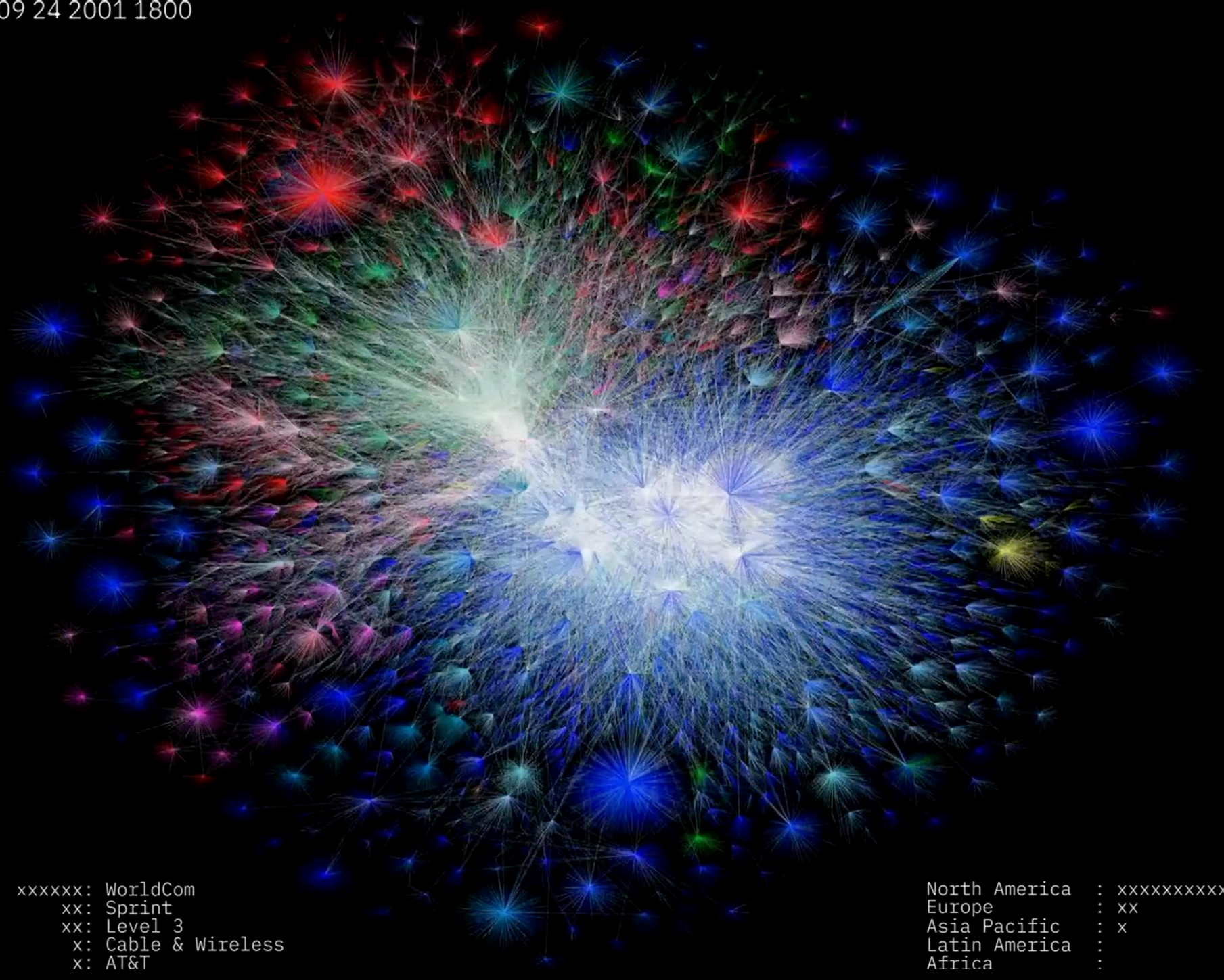
ETH zürich

SCION



Opte Project

09 24 2001 1800



xxxxxx: WorldCom
xx: Sprint
xx: Level 3
x: Cable & Wireless
x: AT&T

North America : xxxxxxxxxx
Europe : xx
Asia Pacific : x
Latin America :
Africa :

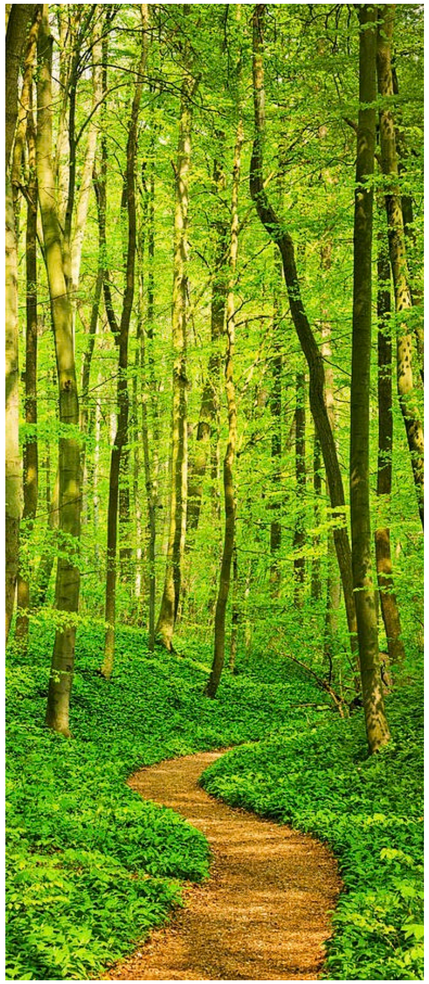
Opte Project

SCION Project

- Started in 2009 at CMU to answer the research questions:
  - How secure can a global inter-domain network be?
  - How to design an inter-domain network to achieve high security to attacks, resilience to failure, and scalability?
- Scion definition in Merriam Webster: "a descendant of a wealthy, aristocratic, or influential family"
  - Also: heir to the throne

Journey through SCION's Attributes

- Governance domains: scalable trust roots in a heterogeneous world
- Scalable path discovery and dissemination for rapid global connectivity
- Massive multipath for fine-grained path optimization
- High-speed packet authentication and path validation
- Real-world deployment incentives

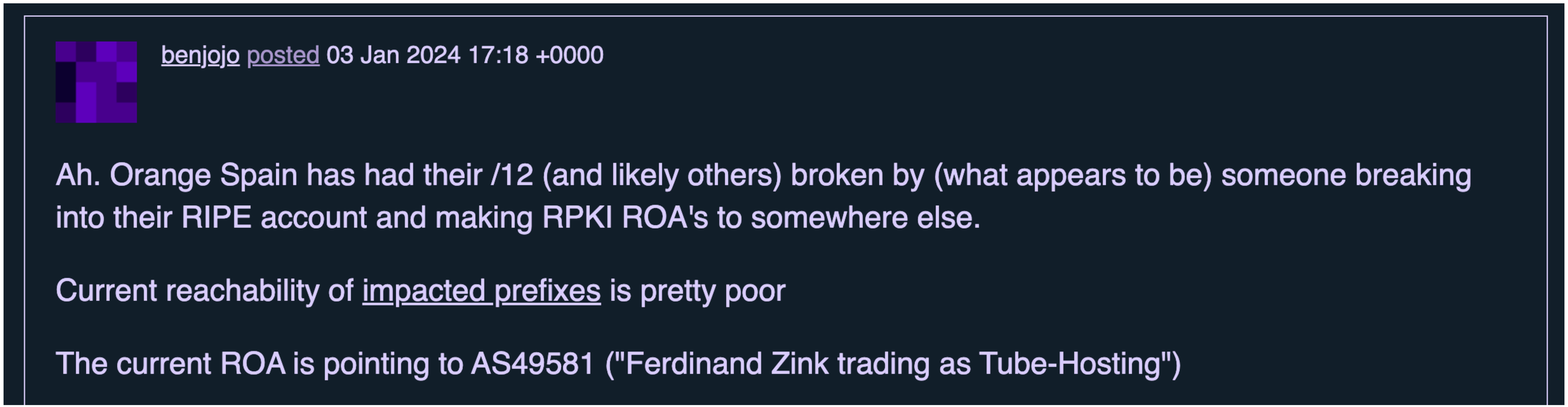


Problem: Non-Scalability of Trust

- As the Internet has grown to encompass a large part of the global population, trust relationships have become heterogeneous: **no single entity trusted by everyone**
  - Complicates construction of entity authentication infrastructures
- Current Internet trust infrastructures have weak security properties because of their single points of failure

Example Issue

- https://benjojo.co.uk/u/benjojo/h/r1zj333N4L6cF7P1xv



benjojo posted 03 Jan 2024 17:18 +0000

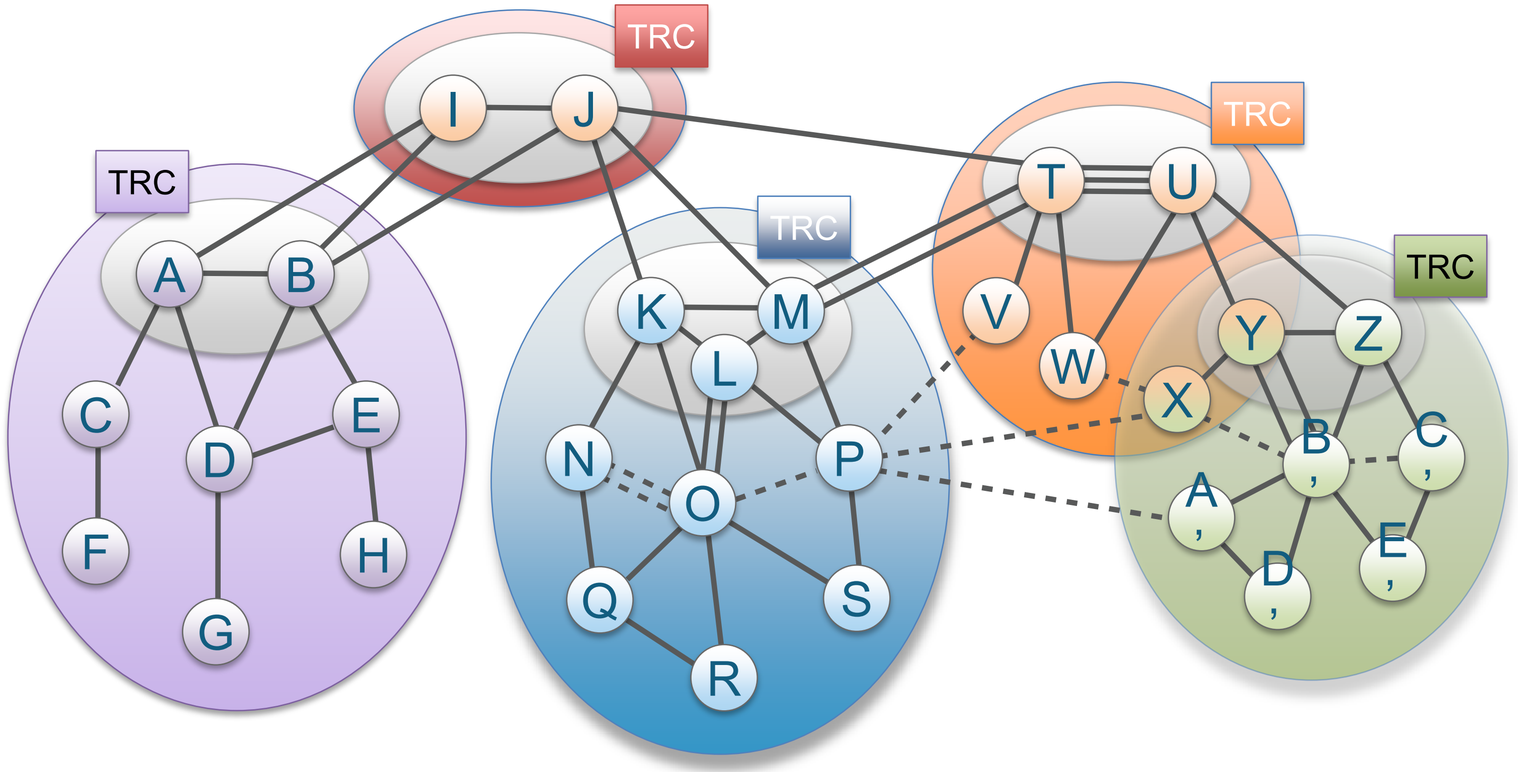
Ah. Orange Spain has had their /12 (and likely others) broken by (what appears to be) someone breaking into their RIPE account and making RPKI ROA's to somewhere else.

Current reachability of impacted prefixes is pretty poor

The current ROA is pointing to AS49581 ("Ferdinand Zink trading as Tube-Hosting")

Approach for Trust Scalability: Isolation Domain (ISD)

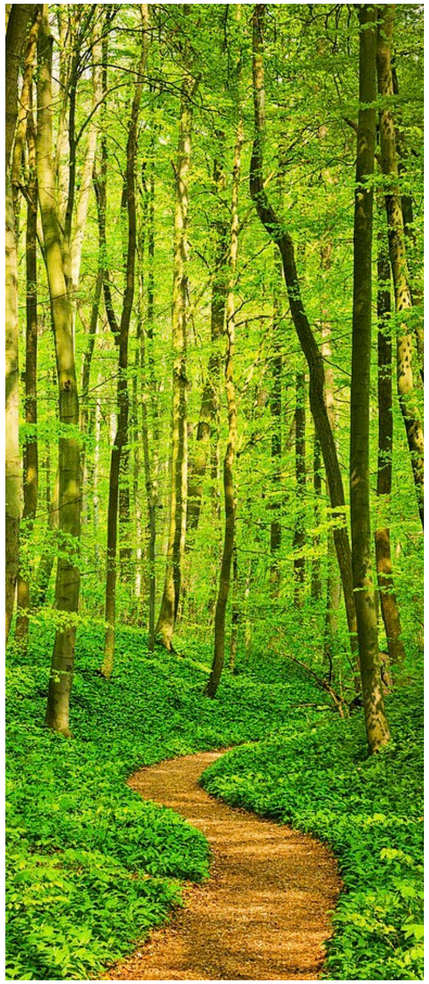
- Isolation Domain (ISD): grouping of Autonomous Systems (AS)
- ISD core: ASes that manage the ISD and provide global connectivity
- Core AS: AS that is part of ISD core



ETH zürich

Observation: Governance Domains are Versatile

- (Fault) Isolation Domain (ISD) can be seen as a Governance Domain
- Governance domain enables local definition of trust roots and trust policy, accommodating Internet's heterogeneity
- Compliance has become challenging in today's Internet: Governance Domain can define local regulations
- Supports scalability through hierarchical routing, matching Internet's structure



SCION Overview in One Slide

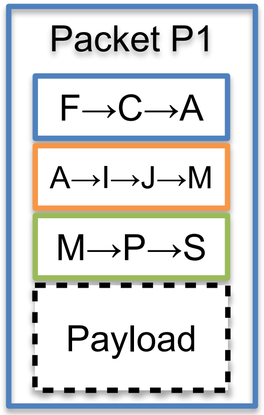
Path-based Network Architecture

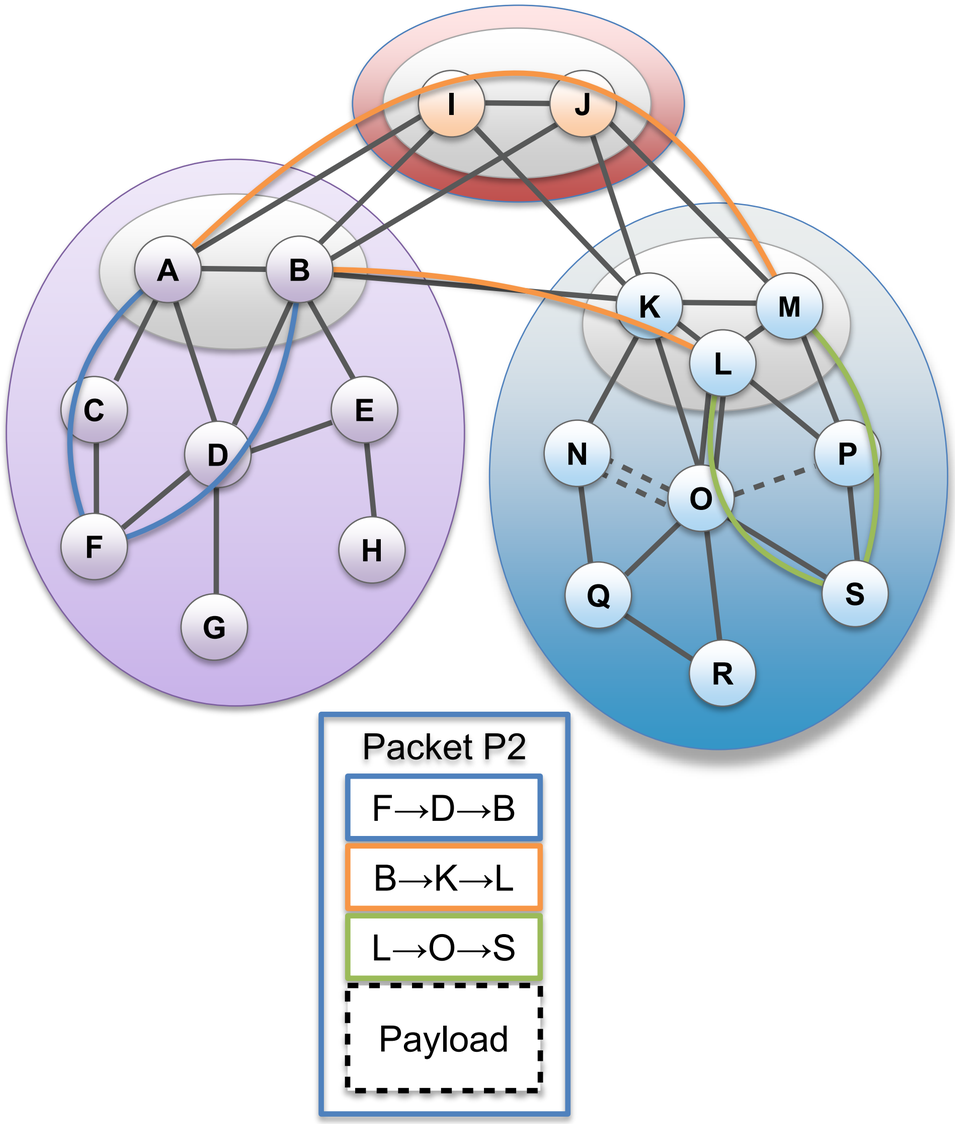
Control Plane - Routing

- 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

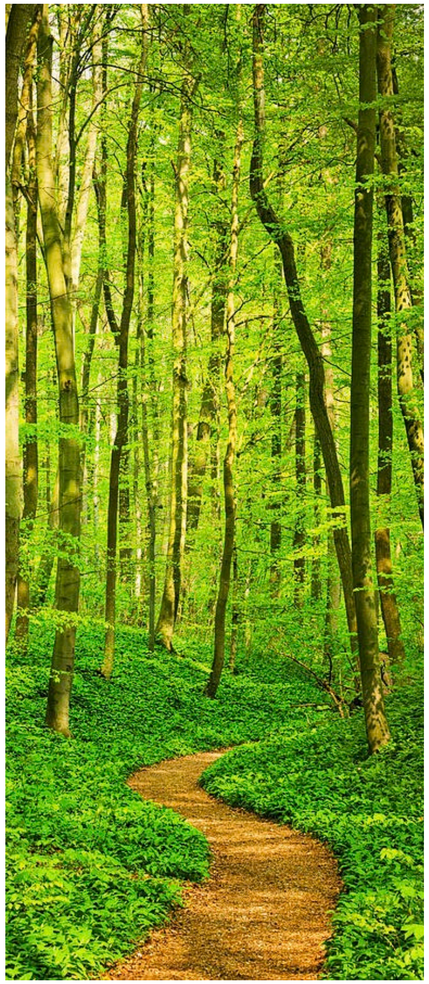




SCION

Observation: Scalable Path Discovery and Dissemination for Rapidly Establishing Global Connectivity

- Reasons for scalability
  - AS-level instead of IP prefix based routing
  - Leaf ASes only receive but do not forward any beacons (only core ASes initiate beacons)
  - Beaconing does not rely on iterative convergence nor forwarding table updates
- Consequences
  - Rapid path exploration between all pairs of core ASes
  - “Instantaneous” path exploration within ISD
  - Simulations suggest that global connectivity after “cold boot” is achieved within seconds

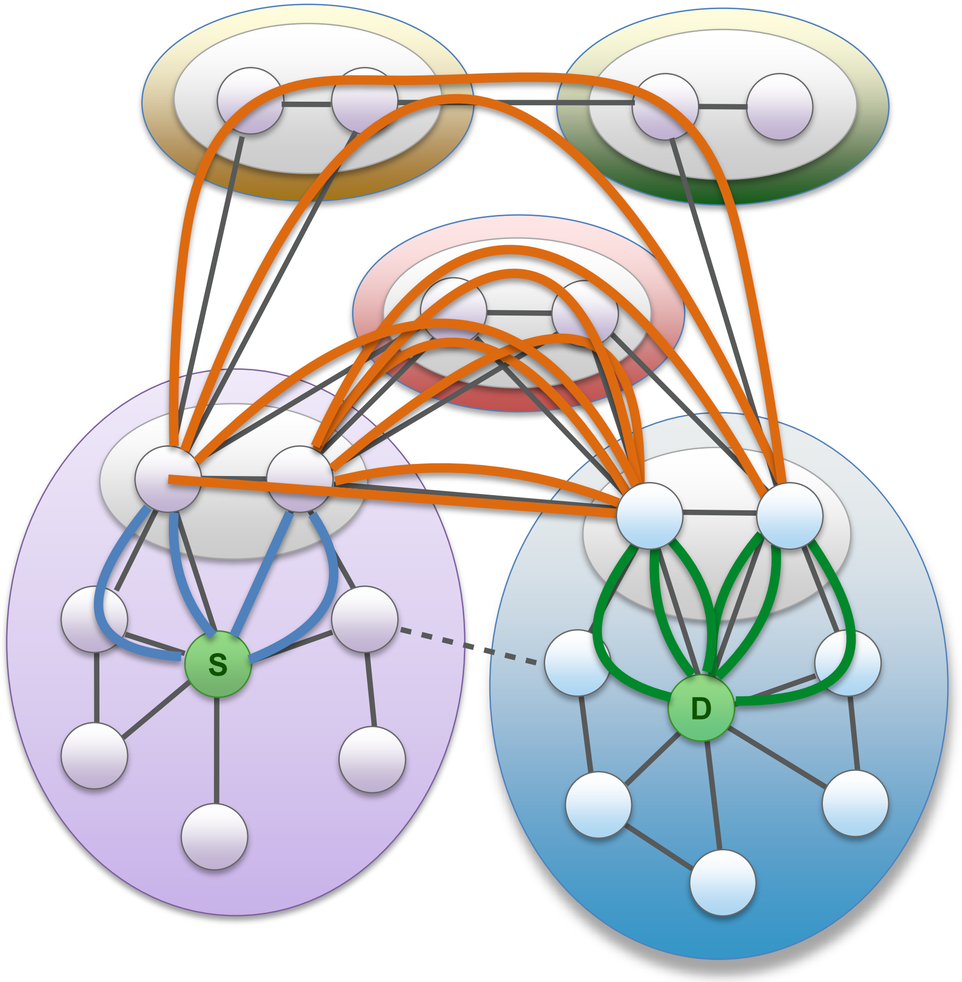


Importance of Path Awareness & Multi-path

- Generally, two paths exist between Europe and Southeast Asia
  - High latency, high bandwidth: Western route through US, ~450ms RTT
  - Low latency, low bandwidth: Eastern route through Suez canal, ~250ms RTT
- BGP is a “money routing protocol”, traffic follows cheapest path, typically highest bandwidth path
- Depending on application, either path is preferred
- With SCION, both paths can be offered!

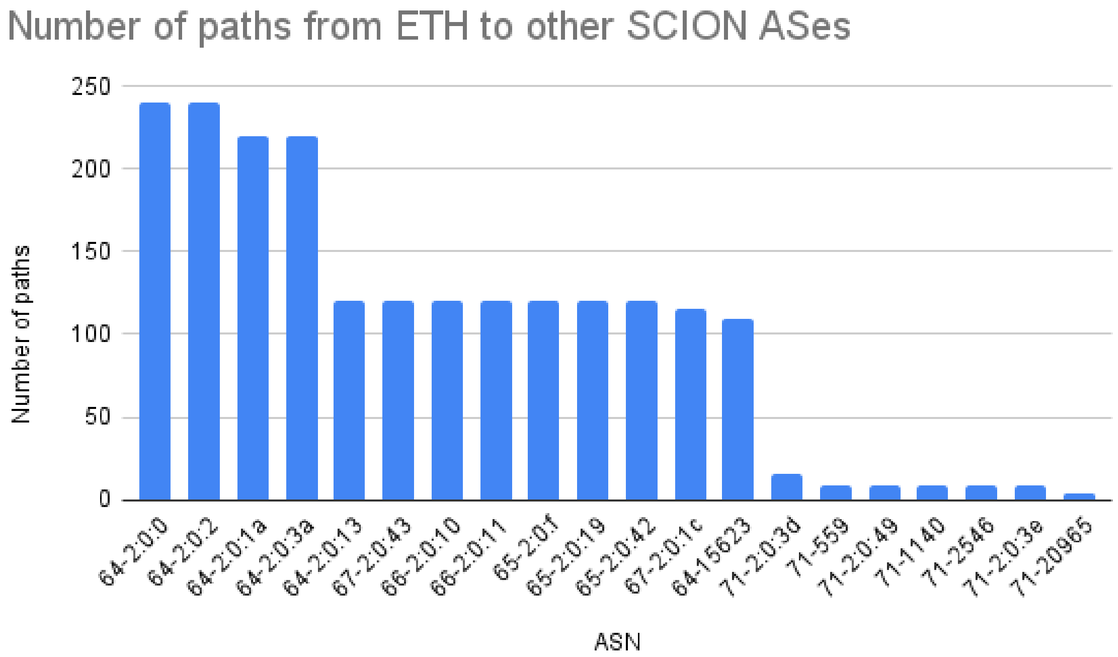
SCION is Massively Multipath

- SCION not only finds many disjoint path segments, but enables a massive number of multipath choices through segment combinations
- In this example, S has 5 path segments to core ASes, D has 6 path segments, and 7 core path segments are provided
- These path segments enable 54 different end-to-end paths!



Path Diversity in Production SCION Network

- Measuring path diversity from ETH to other ASes in production network, we find a minimum of 4 distinct paths and a maximum of 240 paths, with a median of 120 paths

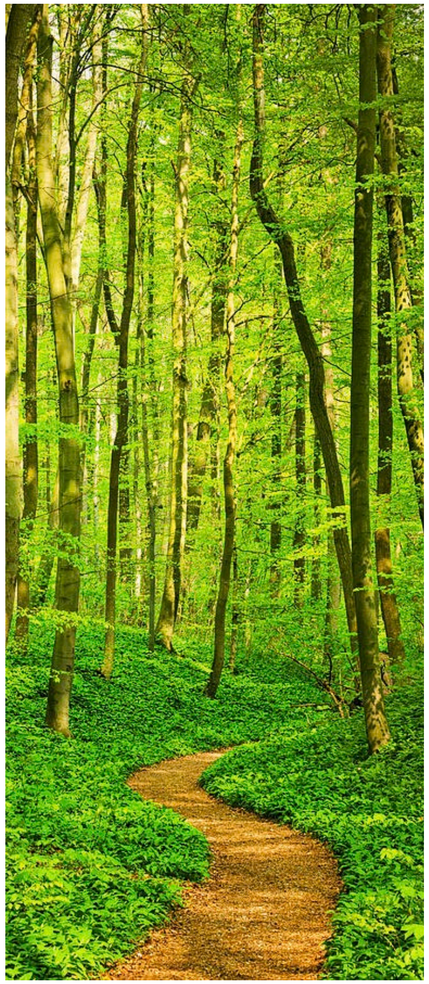


ETH zürich

SCION

Massive Multipath for Fine-grained Path Optimization

- With dozens or even 100+ different paths, SCION will likely offer best path for a variety of different metrics
  - Low latency, jitter
  - High bandwidth
  - Privacy, anonymity
  - Low CO2 footprint
  - Jurisdiction
- Application can make use of multiple paths simultaneously and continuously optimize paths for performance



DRKey & Control-Plane PKI

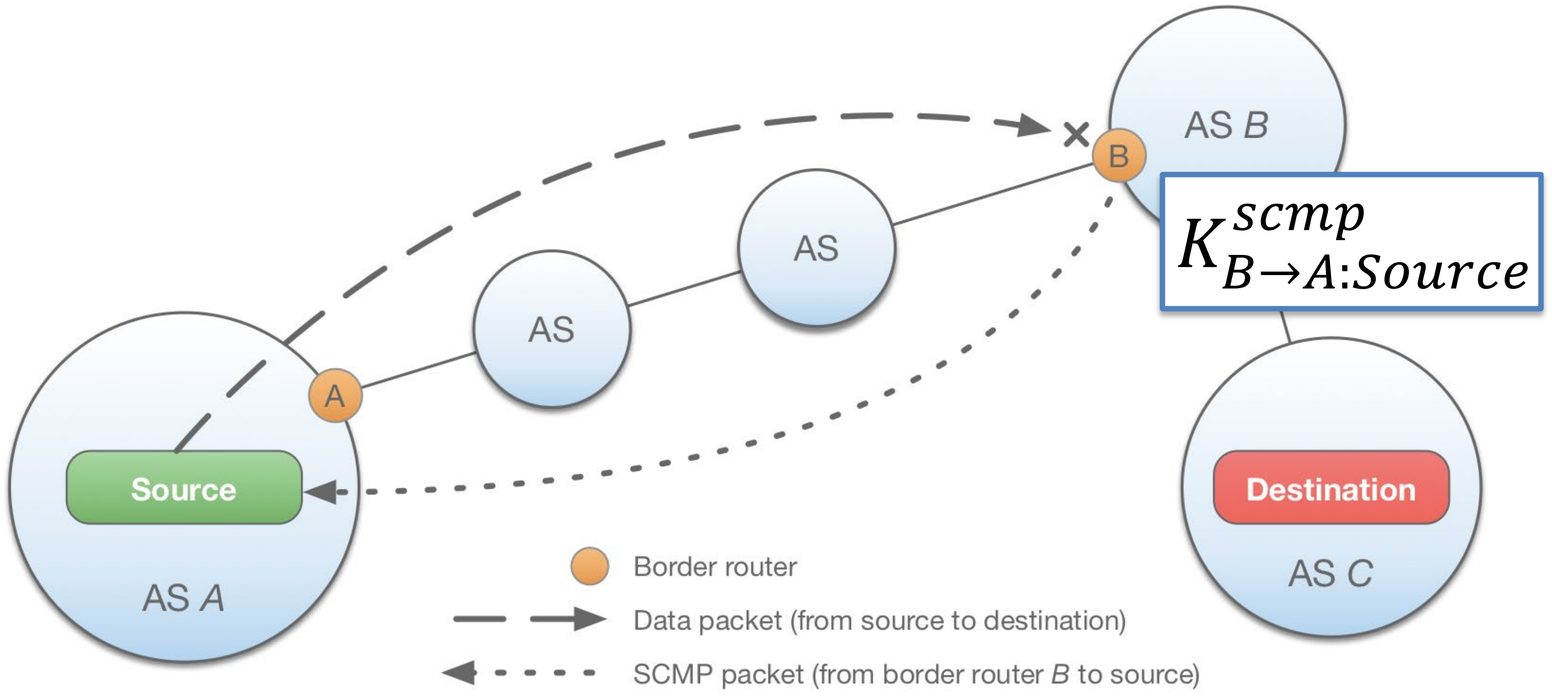
- SCION offers a global framework for authentication and key establishment for secure network operations
- Control-plane PKI
  - Sovereign operation thanks to ISD concept
  - Every AS has a public-key certificate, enabling AS authentication
- Dynamically Recreatable Keys (DRKey)
  - High-speed local key derivation (within ~20 ns)
- PISKES: Pragmatic Internet-Scale Key-Establishment System, Rothenberger et al., ACM ASIACCS 2020

Dynamically Recreatable Key (DRKey)

- *Idea*: use a per-AS secret value to derive keys with an efficient Pseudo-Random Function (PRF)
- Example: AS X creates a key for AS Y using secret value SV_X
  - $K_{X \rightarrow Y} = PRF_{SVx}$ (“Y”)
  - Intel AES-NI instructions compute PRF within 30 cycles
    Key computation is ~7 times faster than DRAM key lookup!
  - Any entity in AS X knowing secret value SV_X can derive $K_{X \rightarrow *}$

Example: SCMP Authentication

- SCMP: SCION Control Message Protocol
- Border router in AS B can derive key $K^{scmp}_{B \rightarrow A:Source}$ from SV_B
- Host “Source” can fetch key from local key server KS_A to authenticate SCMP message

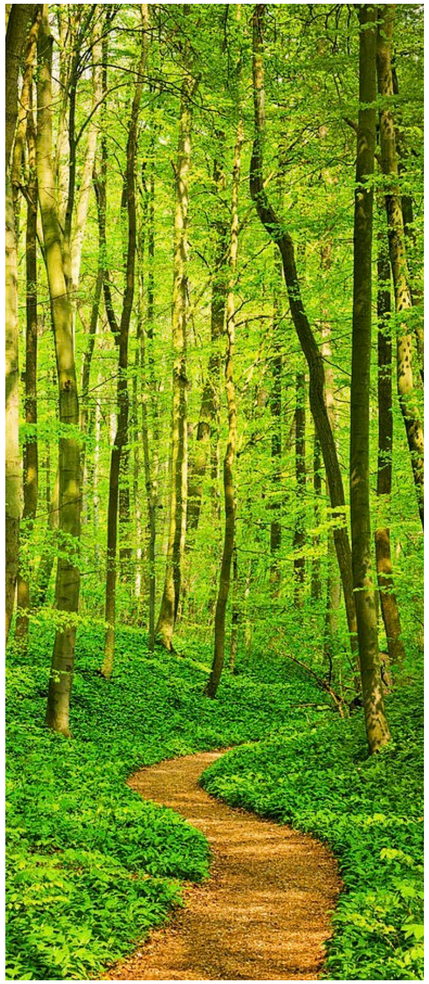


EPIC: Every Packet Is Checked

- Properties
  - Line-rate packet source authentication by routers and destination
  - Path validation by destination
- Assumption: global time synchronization (+/- 100ms)
- Attacks prevented
  - Malicious router replays packets or increases packet size
  - Hop field MAC is brute forced and destination attacked until expiration time
- EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet, Legner et al., USENIX Security 2020

High-speed Packet Authentication and Path Validation

- DRKey provides Internet-wide symmetric keys between hosts and network devices
  - Network devices compute key with 2 AES operations within ~20ns in SW or ~2ns in HW
  - End hosts need to fetch key at local key server
- Packet authentication through SCION Packet Authentication Option (SPAO) or through EPIC header

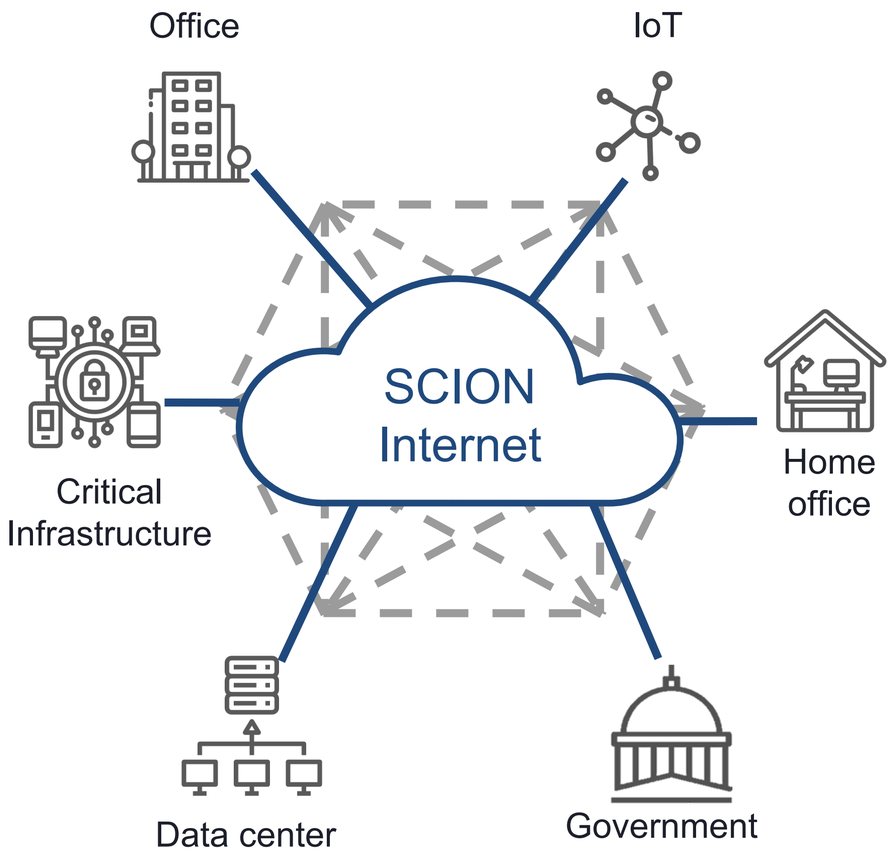


Main Use Case: Communication among Community

Single SCION connection offers secure communication to any other entity on SCION network

- ⊕ High availability, secure against DDoS and routing attacks
- ⊕ Geofencing
- ⊕ High efficiency through path optimization
- ⊕ Fast failover
- ⊕ Easy to extend to new use cases
- ⊕ Low cost
- ⊖ Initial setup requires effort
- ⊖ Training required for network admins

Takeaway:
Single SCION connection approximates a leased line to all SCION destinations



ETH zürich

SCION

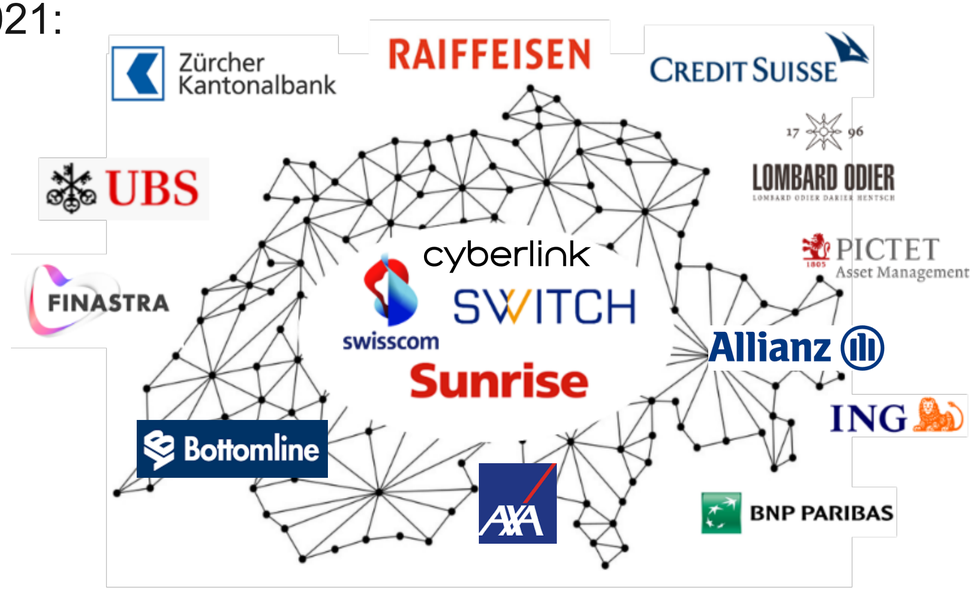
Secure Swiss Finance Network (SSFN)

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

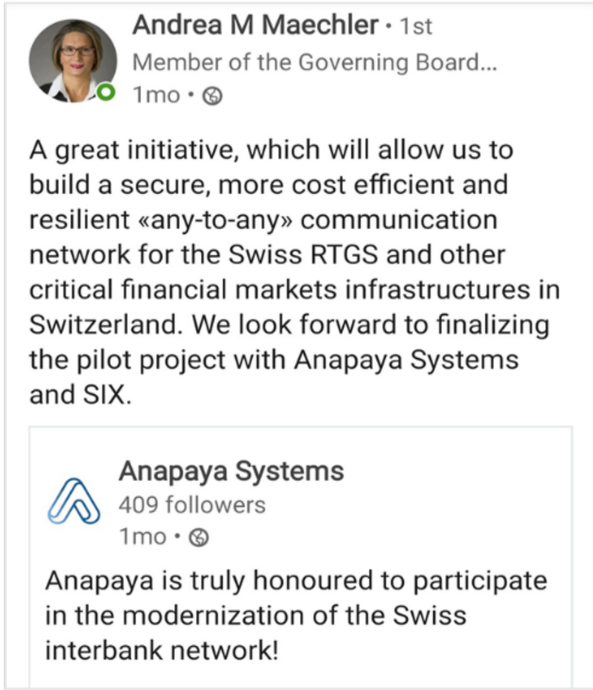
SSFN: Secure Swiss Finance Network

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



SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

SIX



SCION Production Network

- **Not an overlay!**
  BGP-free global communication
  - Fault independent from BGP protocol
- Deployment with international ISPs
  - First **global public secure** communication network
- Construction of SCION network backbone at select locations to bootstrap adoption

ANAPAYA
cyberlink
interCloud
proximus
telindus
DIGITAL REALTY
swisscom
Sunrise
axpo
vtx
swissix SWISS INTERNET EXCHANGE
LGU+
KISTI www.kisti.re.kr
SWITCH
GÉANT
KREONET

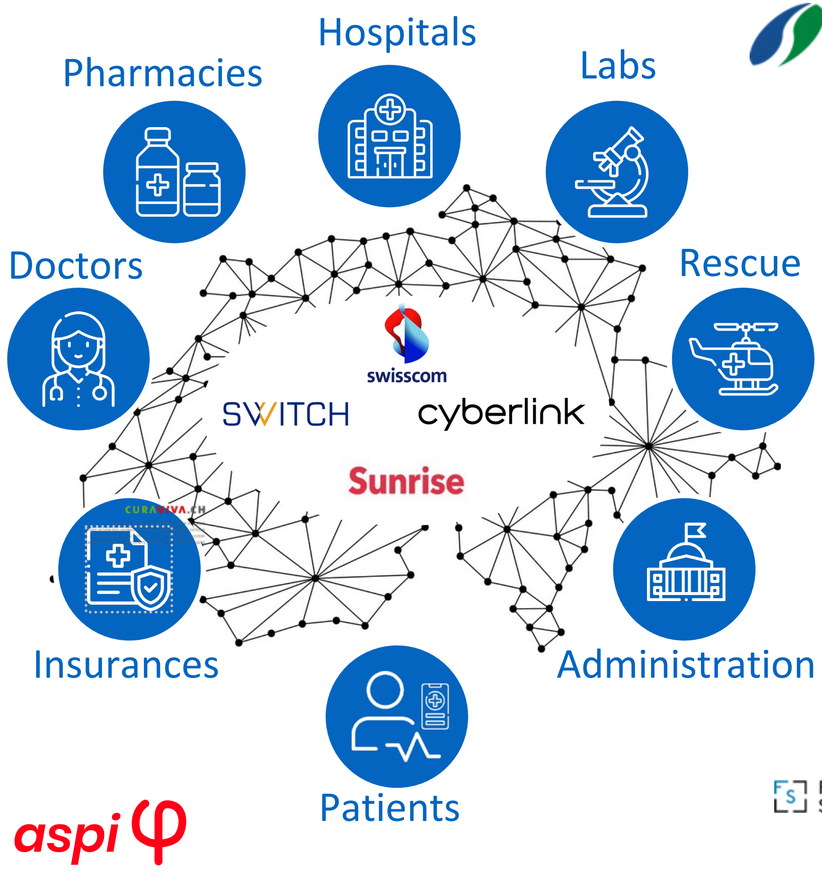
ETH zürich

SCION

Secure Swiss Healthcare Network (SSHN)

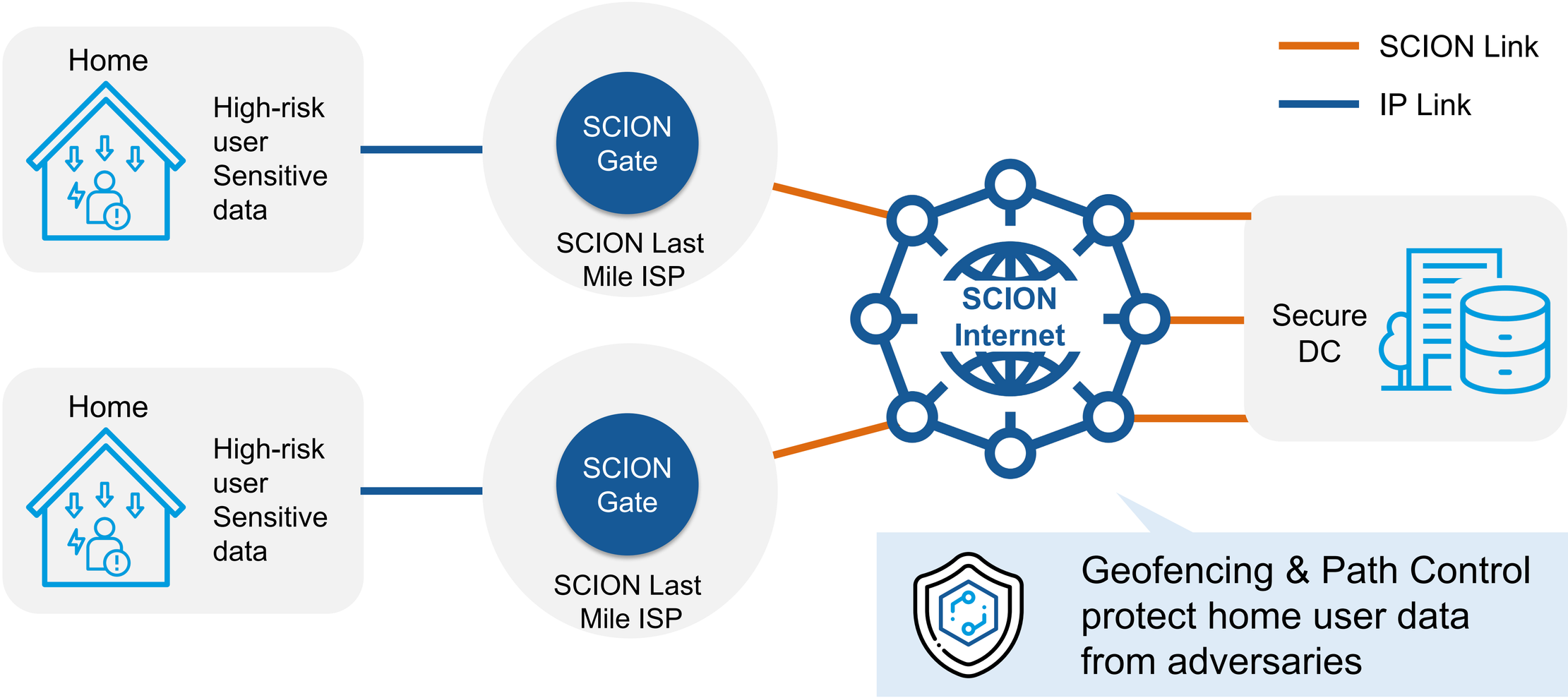
The HIN Trust Circle (HIN Vertrauensraum):

- Interconnecting **hundreds of hospitals** and **tens of thousands of doctors**
- Healthcare is **highly dependent on communication** between multiple parties
- Connectivity can be **life-saving**



GATE Approach Against DDoS

Seamless secure SCION for remote users

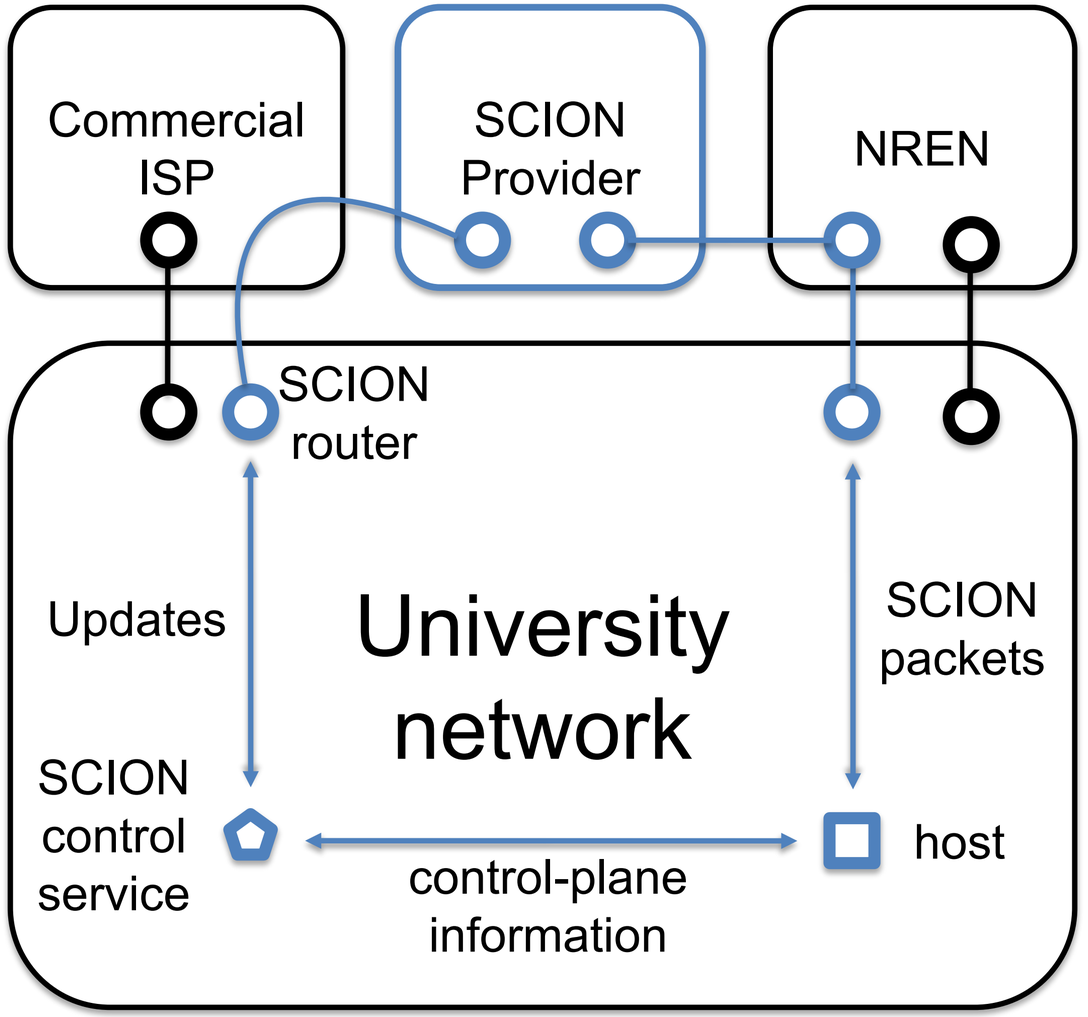


Sui Blockchain Use Case

- Sui properties
  - Transaction finality < 0.5s (majority of transactions)
  - State-of-the-art in terms of scalability, efficiency, resilience
  - Lowest transaction fees
- With the ambition to build the premier blockchain infrastructure, Sui is adopting SCION, initially as a backup, but long-term as an efficient and highly resilient communication infrastructure

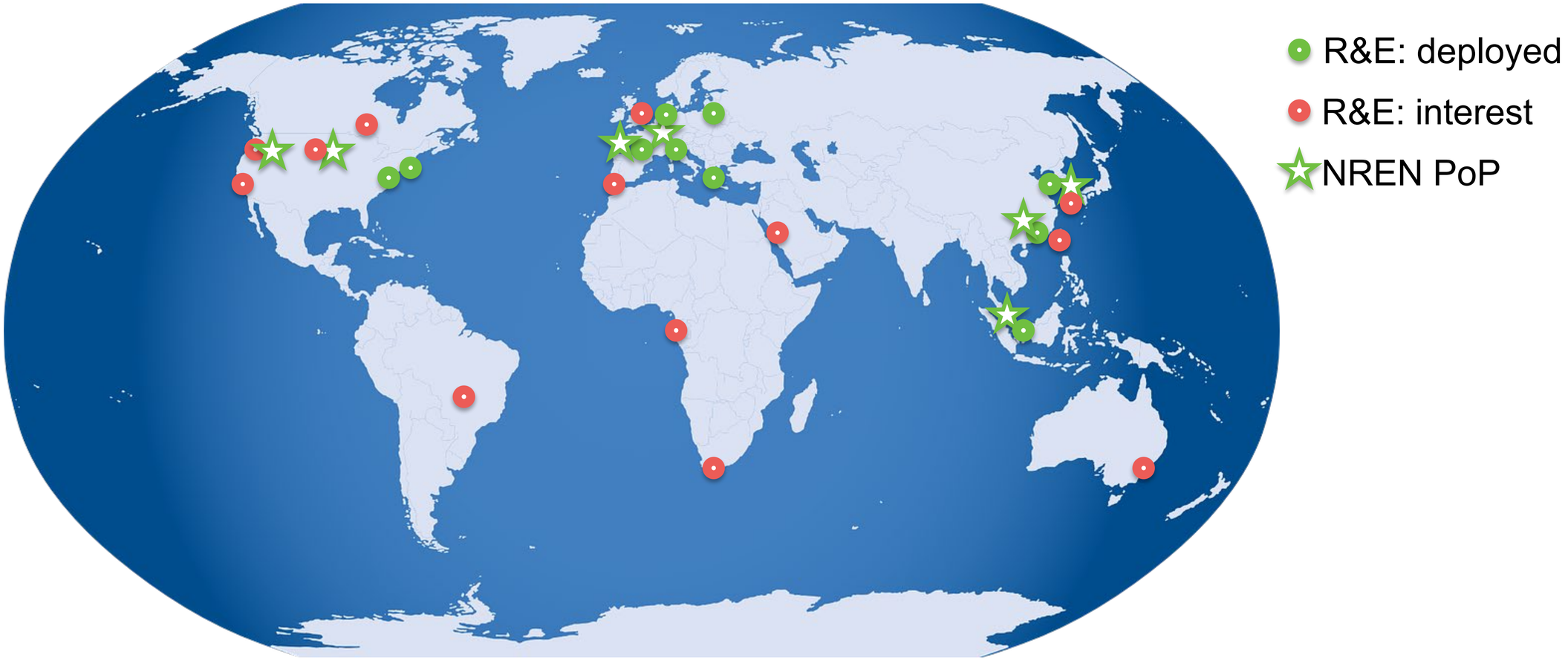
University Setup

- SCION SW router can be installed on a Linux workstation, a VM, or on a commercial router VM (e.g., Extreme Networks)
- Connectivity can be obtained over native or virtual L2 technology (e.g., VLAN, MPLS) to reach a nearby SCION router
- SCION control service runs on a Linux workstation anywhere in the local network

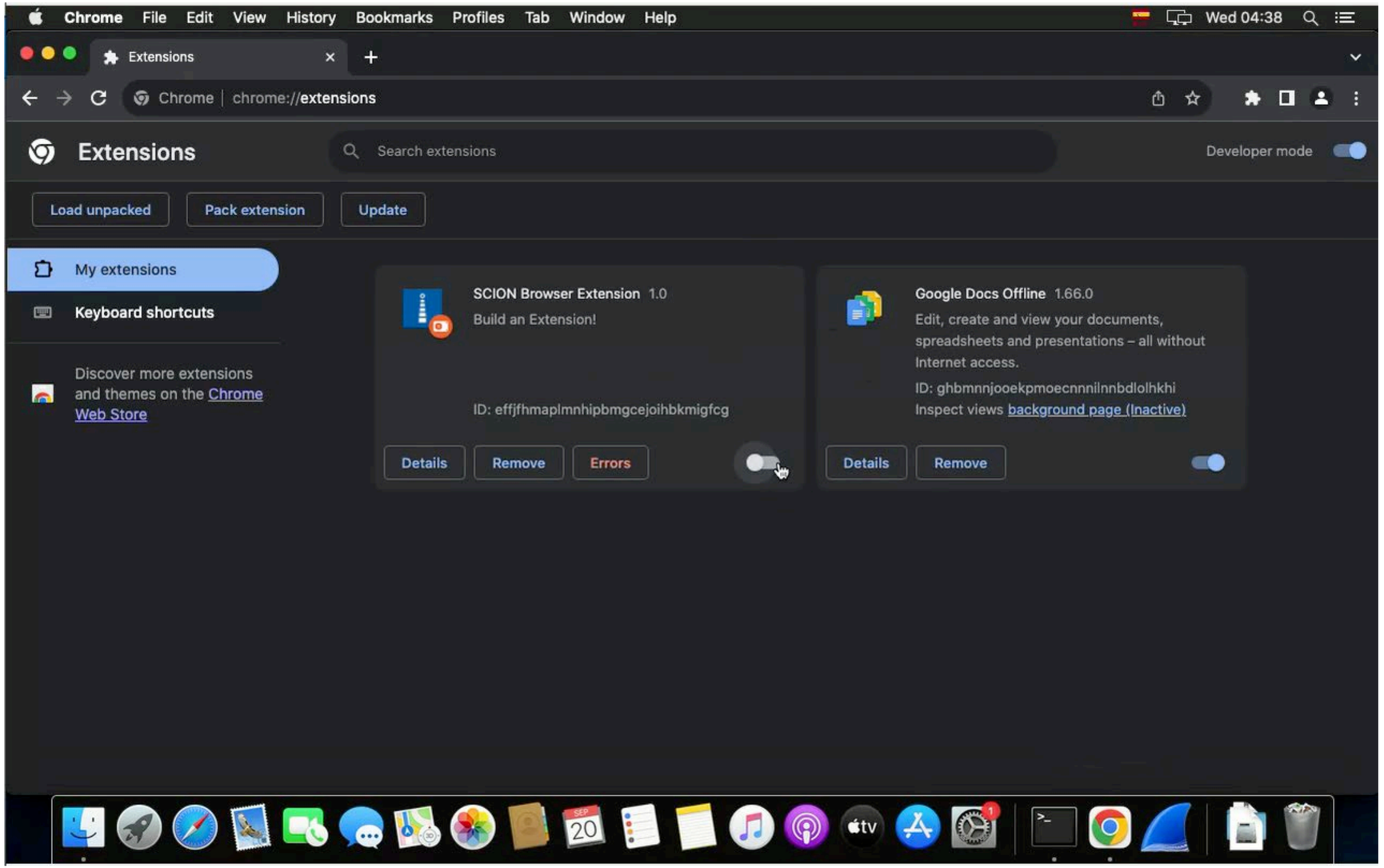


Global SCION Research & Education Network

- Main networks providing connectivity: GÉANT, Kreonet, SWITCH



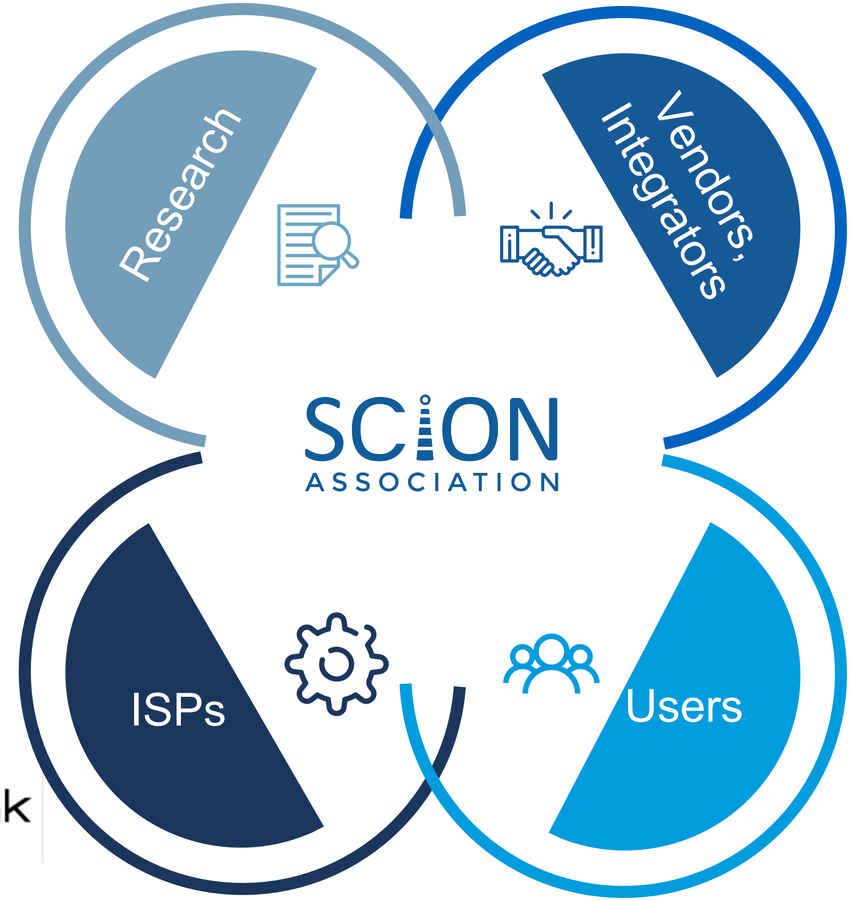
SCION-enabled Browser Demo on macOS



ETH zürich

SCION

Ecosystem nurtured by SCION Association



PRINCETON UNIVERSITY
SIDN
ETH zürich
고려대학교 KOREA UNIVERSITY
NUS National University of Singapore
OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
CYBEXER TECHNOLOGIES
CSCS Centro Svizzero di Calcolo Scientifico Swiss National Supercomputing Centre
KAIST
KiSTi www.kisti.re.kr
UNIVERSITY of VIRGINIA
DEMOKRITOS
BT
proximus telindus
interCloud
swisscom
Sunrise
DIGITAL REALTY
axpo
swissix SWISS INTERNET EXCHANGE
LG U+
vtx
cyberlink
GÉANT
KREONET
SWITCH

ANAPAYA
bnc business network communications
Extreme
infoGuard SWISS CYBER SECURITY
INFOSEC GLOBAL
Startups
eraneos
HIN
ICRC
libC TECHNOLOGIES
securosys

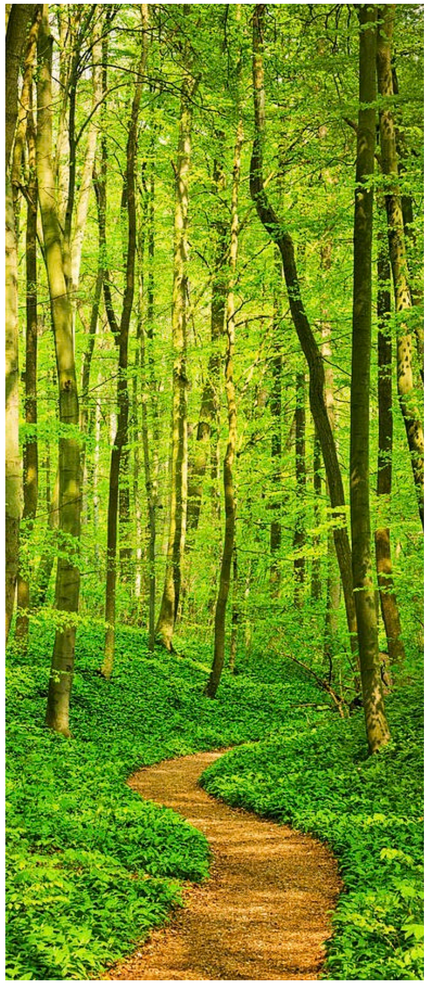
RAIFFEISEN
SIX
Zürcher Kantonalbank
UBS
armasuisse
aws
Sui

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Federal Department of Foreign Affairs FDFA

SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

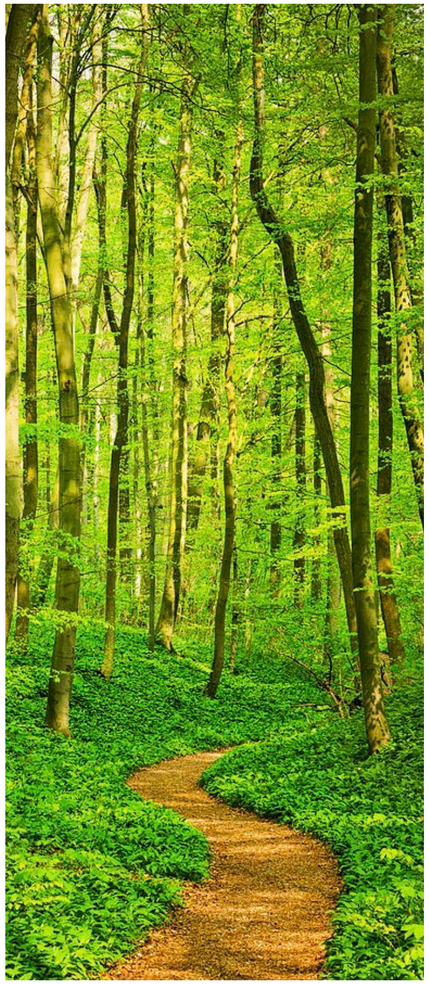
Real-world Deployment Incentives

- Secure and resilient communication fabric to connect entities in finance ecosystem started deployment
- Possibility to set up governance domain for an industry vertical was key for early deployments
- Initial ISPs saw opportunity to offer secure connectivity across different providers
- University network is currently expanding, today providing native SCION connectivity to 100’000+ users



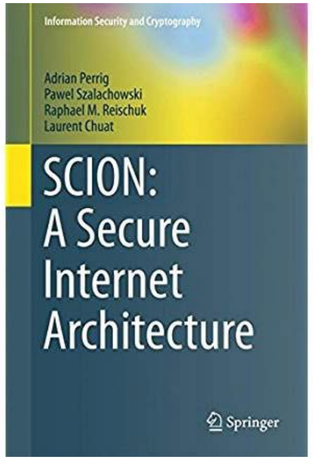
Reaching the Tipping Point

- Once tipping point is reached, deployment of SCION deployment occurs organically
- Anticipation that tipping point is soon reached
  - With the increasing availability of SCION, deploying applications obtain an advantage
  - With the increasing use of SCION in applications, ISPs need to offer it to avoid losing customers
- Competition may lead to a rapid deployment

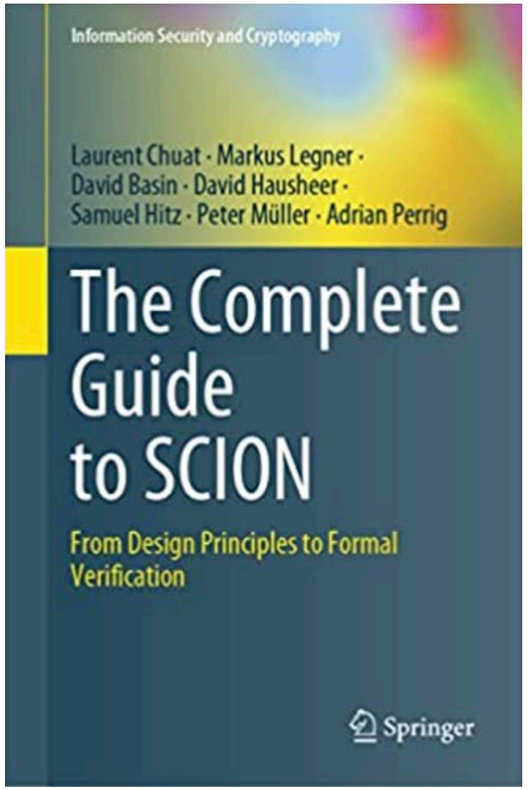


Online Resources

- 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

Summary

- SCION addresses global trust issues, scales up to global heterogeneous trust
- SCION production network and use cases are expanding
- Goal for 2024: Provide 1M hosts access to native SCION connectivity
- Native SCION applications emerging
- Join the native network
- More information:
  https://sciera.readthedocs.io
  https://cloud.inf.ethz.ch/s/ASsE3sqKiG5RXPZ

ETH zürich

SCION

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG