ETH zürich

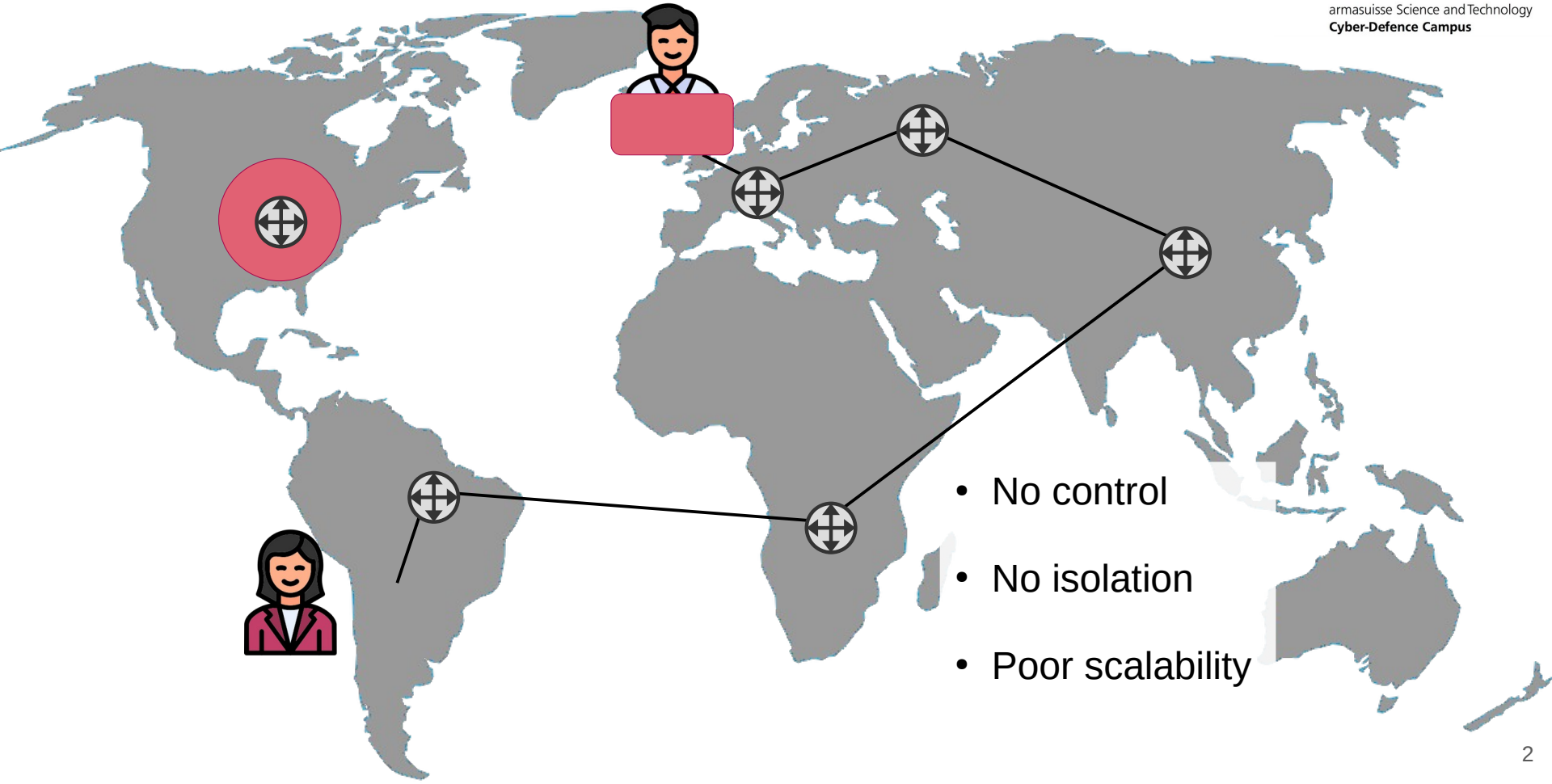
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse Science and Technology
Cyber-Defence Campus

Security Analysis of the SCION Internet Architecture

Master Thesis - Marco Seewer

Supervised by Roland Meier, Jordi Nieto, and Adrian Perrig
This research is supported by armasuisse Science and Technology.



- No control
- No isolation
- Poor scalability

ETH zürich

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse Science and Technology
Cyber-Defence Campus

Scalability, Control, and Isolation on Next-Generation Networks

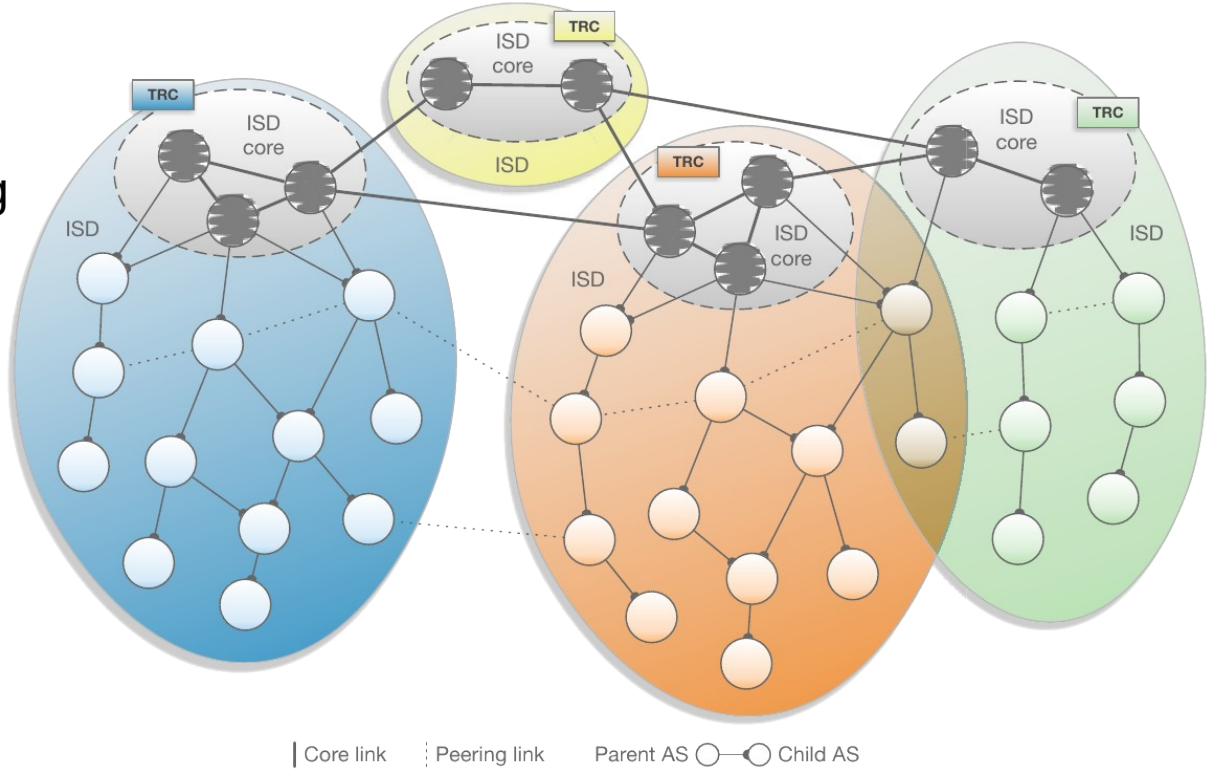
- Developed at ETH Zurich
- Open-Source
- Commercialized by Anapaya

Isolation domain (ISD):

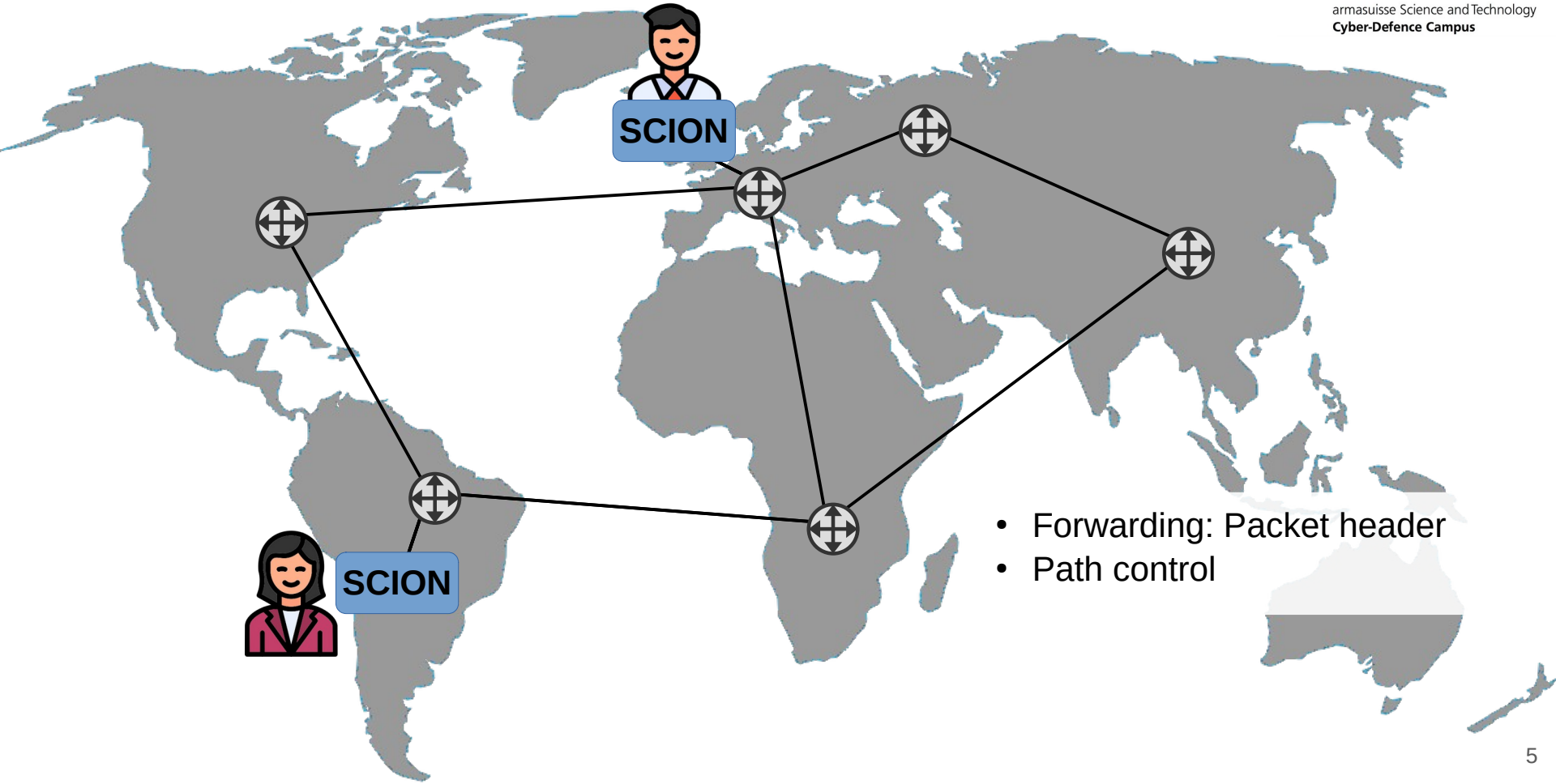
- Isolate routing within ISD
- Scalability: separate routing within / between ISD

ISD Core:

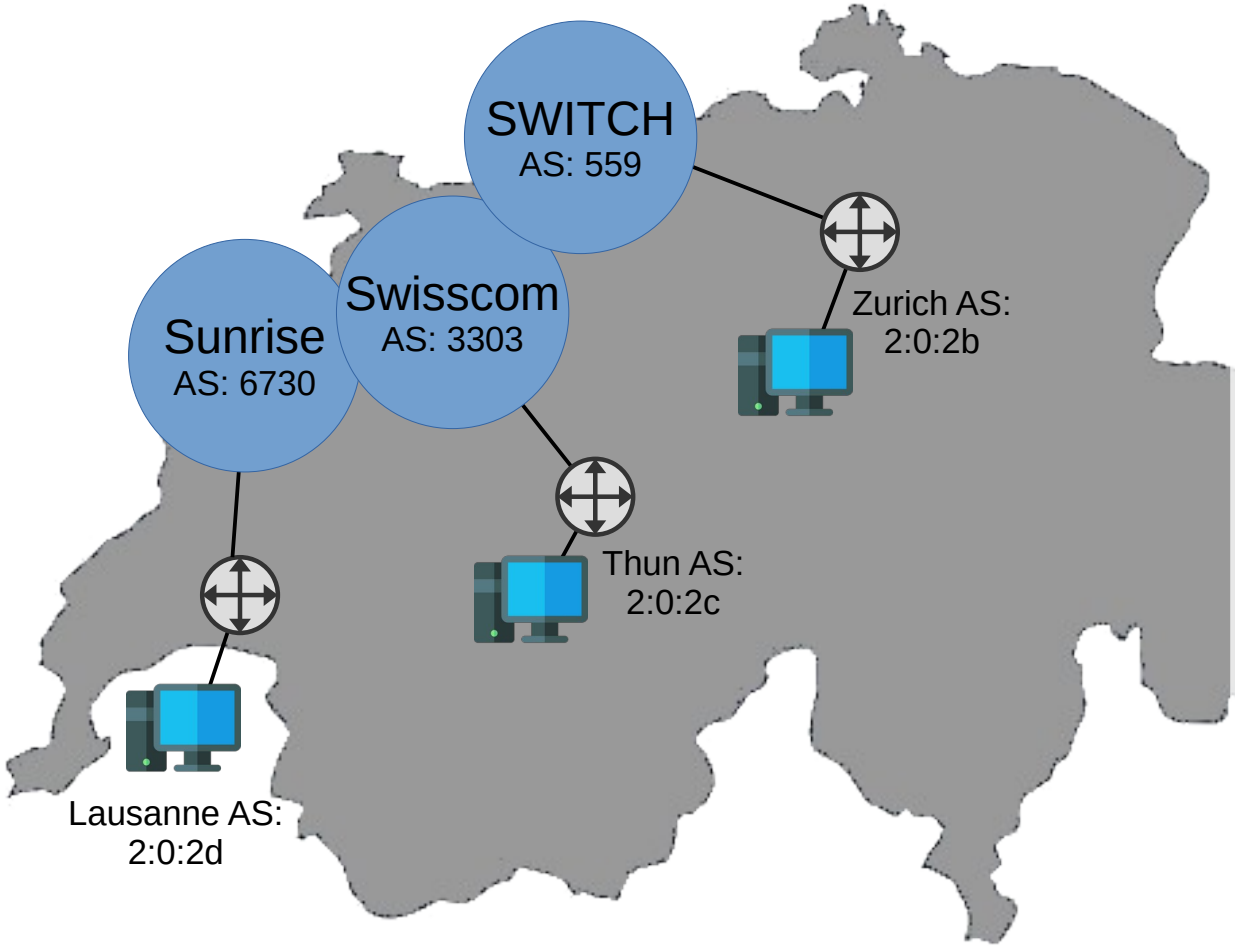
- Root of trust
- Init path construction



The Complete Guide to SCION, Figure 2.1



- Forwarding: Packet header
- Path control



CYD Testbed:

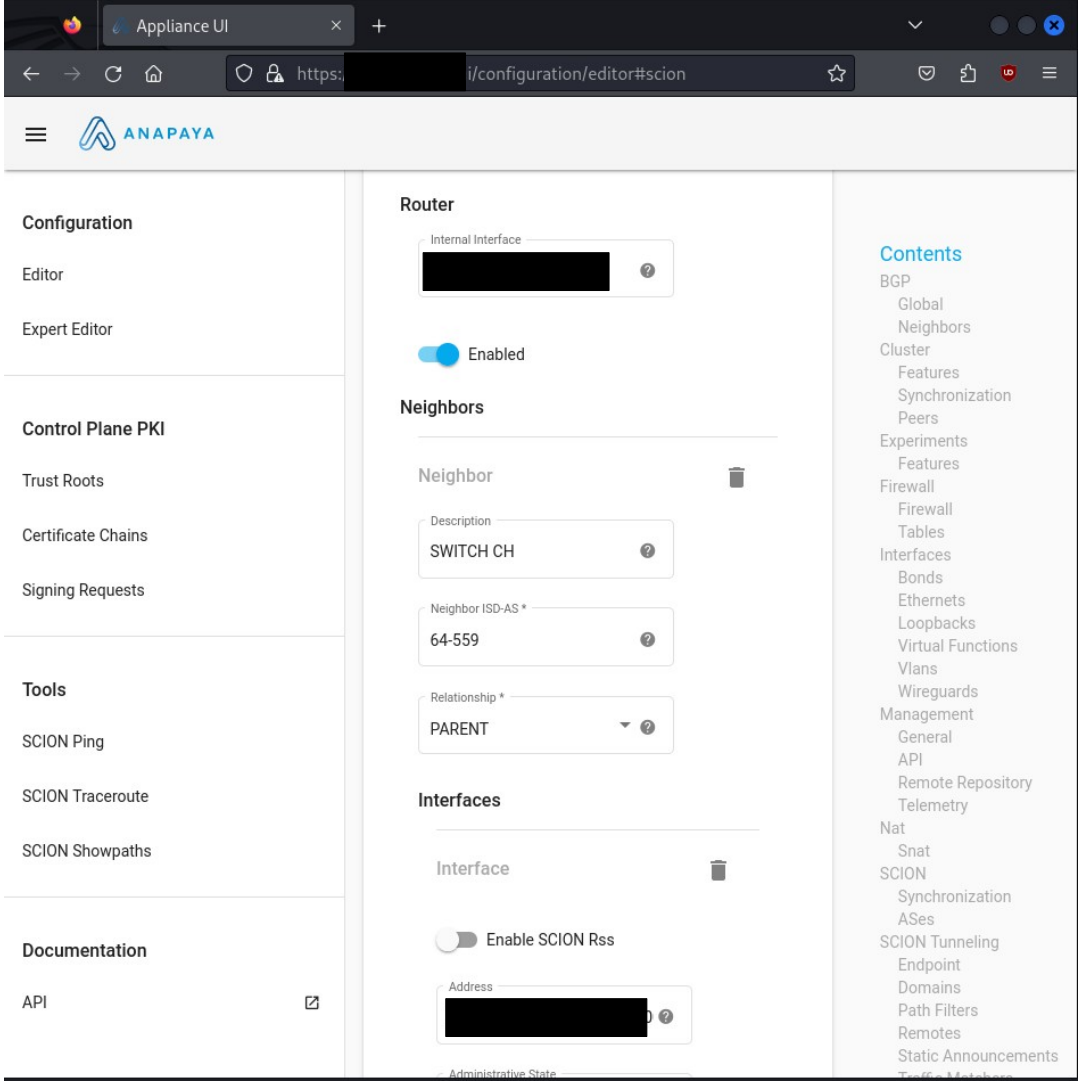
- 3 ASes
- 3 Core Ases
  - SCION Production Network
- Anapaya Routers
  - Different HW / SW
  - Configurations

Anapaya Device – Router

- Automated scans
  - Unauthenticated + authenticated vulnerability scans
  - Compliance scans
  - Docker images
- Manual investigation
  - Scan results applicable
  - Open ports + running services
  - SCION configuration (Appliance)

https://www.supermicro.com/files_SYS/images/System/SYS-110D-8C-FRAN8TP_main.jpg

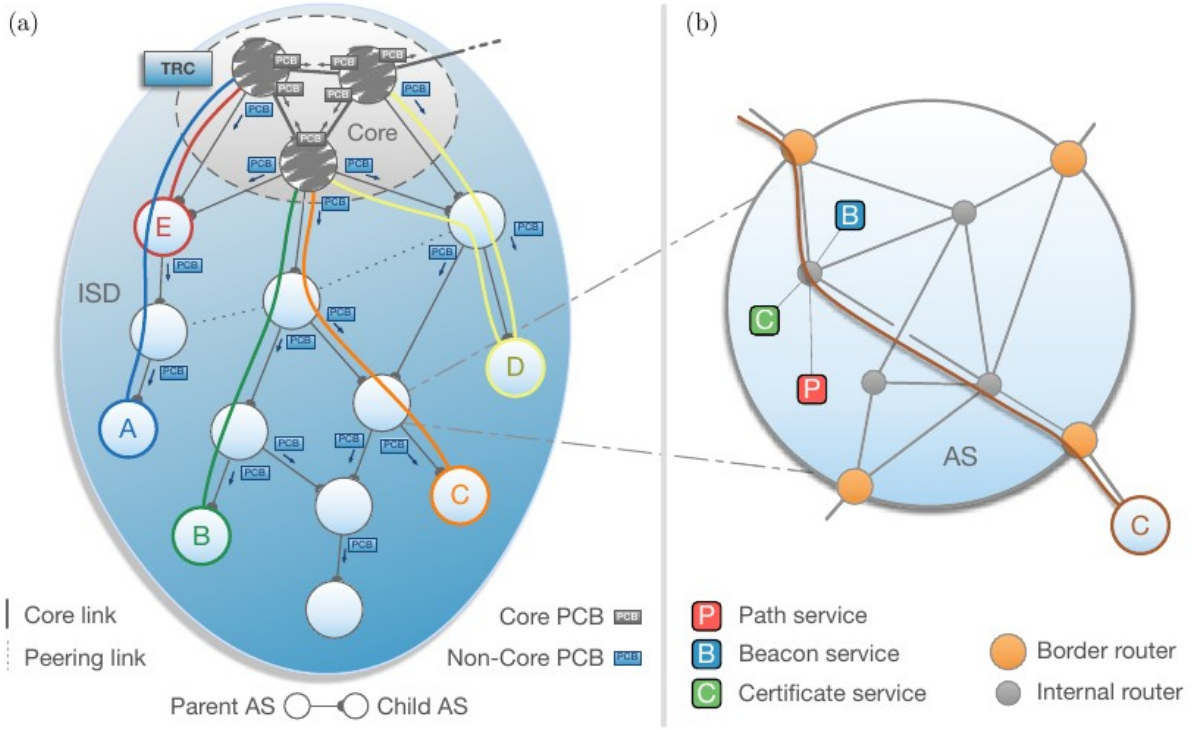
No authentication!



SCION Protocol – Path exploration

- Initiated from core
- Save ingress/egress interfaces
- Each hop is signed (=MAC of whole path)

MAC algorithm
=
Open-Source (CMAC)
=
Secure!

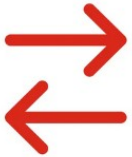


The Complete Guide to SCION, Figure 2.3

More control with SCION

SCION gives you path control over your end-to-end communication, allowing you to avoid certain network sections such as networks in unstable regions. Control over path choice also allows you to make selections regarding available bandwidths and latencies. This increases the security of your data in terms of how it is handled and gives you more control over the transport route of your sensitive data.

https://www.switch.ch/en/network/scion-access



Controlled paths

Controlled path direction allows you to define precisely the route of your data and ensures communication compliance. For example, you can define a geographical area (e.g., Switzerland) that your data may not leave or determine the specific autonomous systems (AS) you want it to pass through.

https://www.sunrise.ch/business/en/enterprise/internet-networking/business-wan/scion

Path control & multipath

SCION allows the sender to control the routing, choosing exactly how and where data packets travel. With the multipath feature, senders can choose multiple paths at the same time.

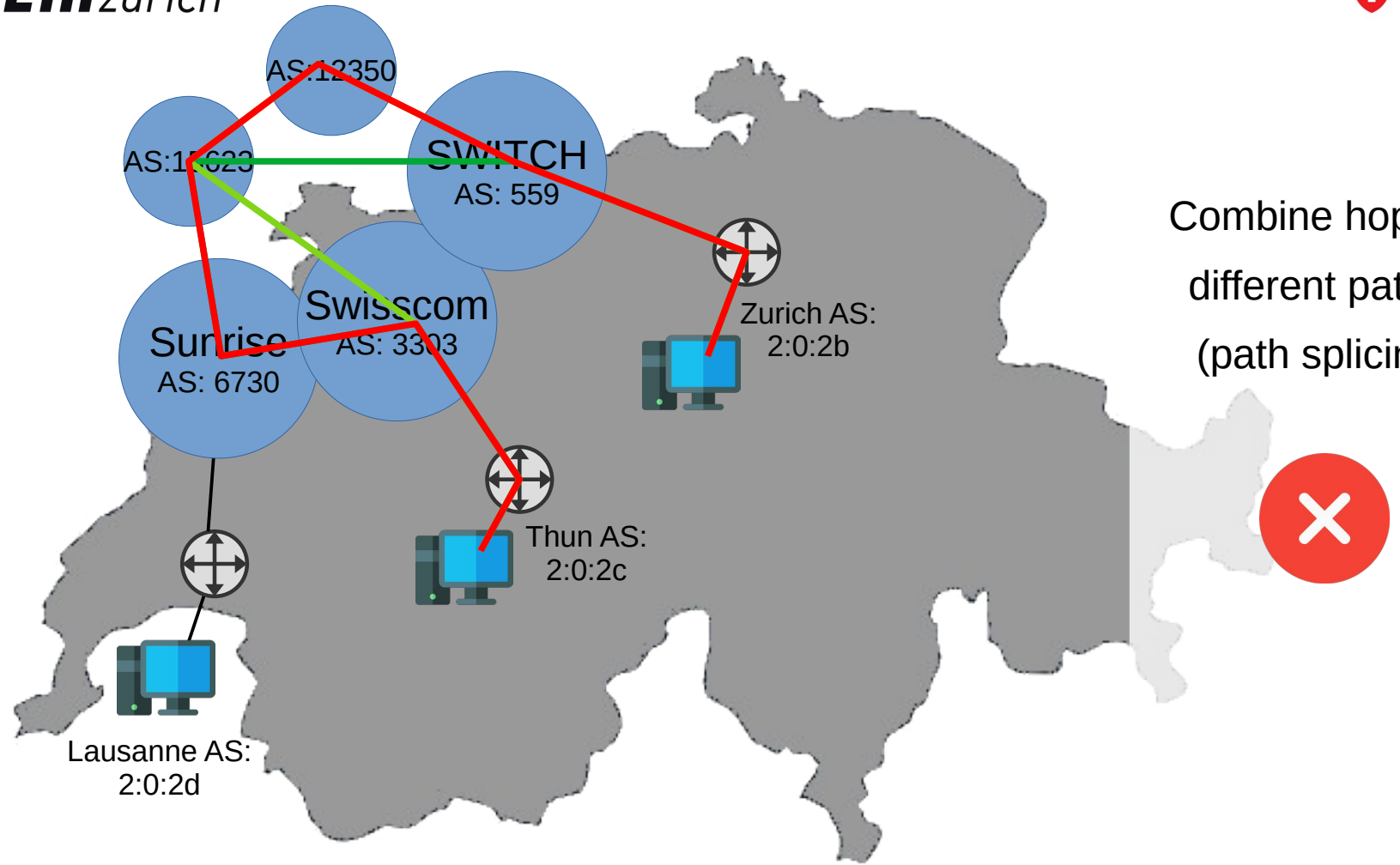
https://www.anapaya.net/scion-internet

Multi-path communication and network AI

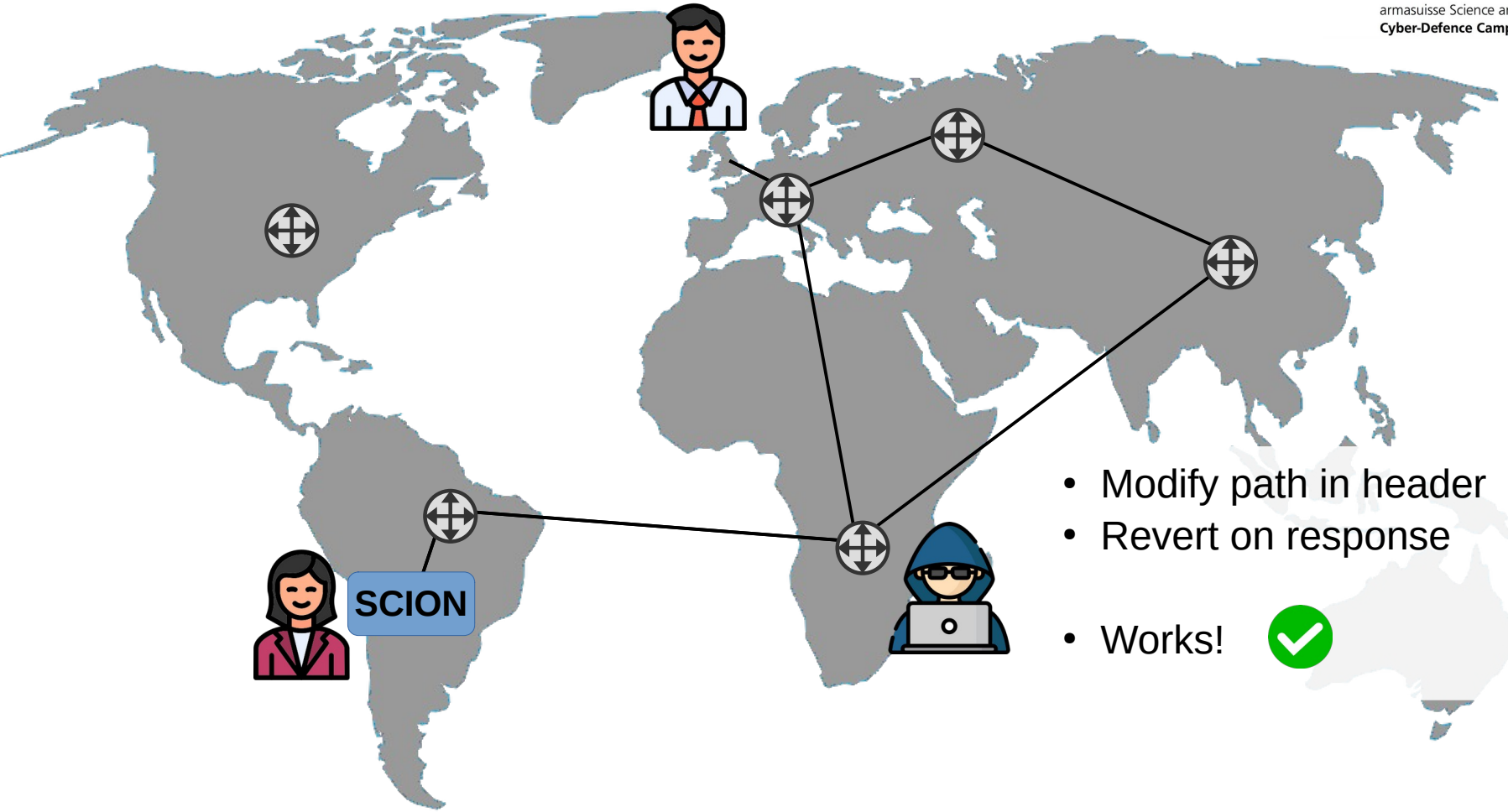
SCION path-based architecture provides in-depth insights into the network and clear visibility of paths, performance metrics and network conditions. The best network path for each application can be selected and routed efficiently using artificial intelligence.

You retain full control over how your data is routed on the Internet, thereby protecting it from routing and DDoS attacks. You can also use geofencing to define which geographical area your data is not allowed to leave or which countries to exclude.

https://www.swisscom.ch/en/business/enterprise/offer/wireline/scion.html



Combine hops of different paths (path splicing)

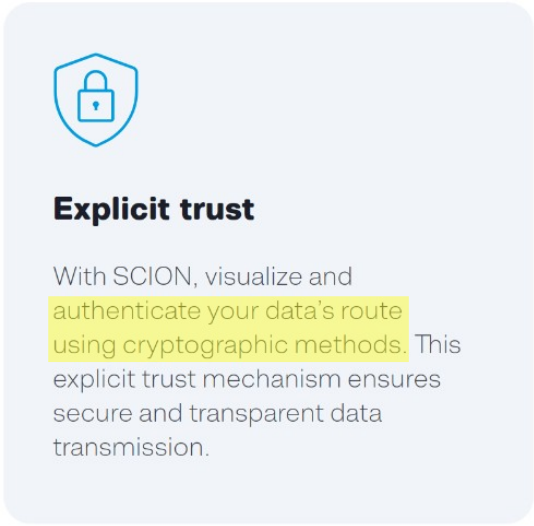


- Modify path in header
- Revert on response
- Works!

Path manipulation – Preventions

- Open source: Packet authentication
- Can not be activated/used in Anapaya SCION

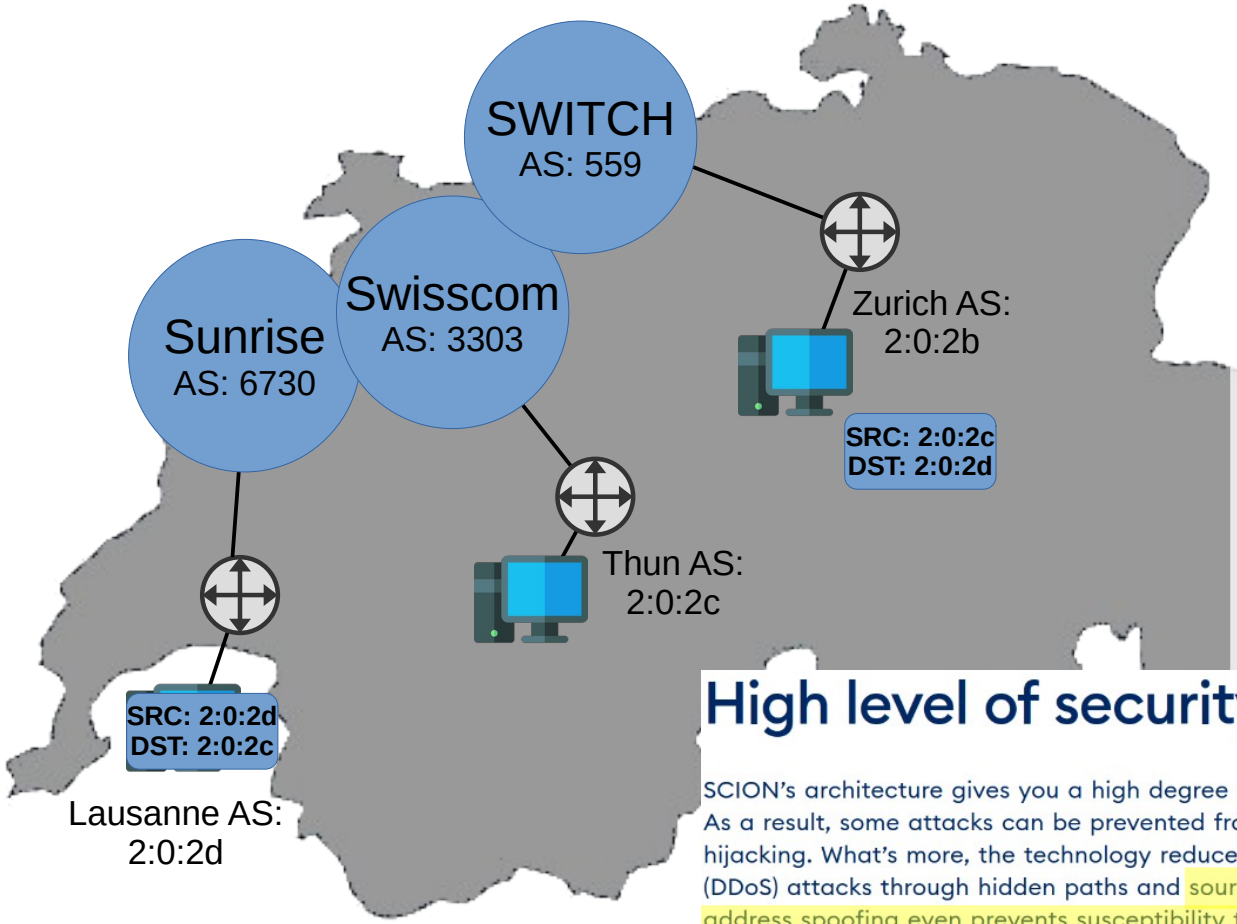
No SCION Packet Authentication Option
=
Implement own solution at end hosts
(e.g. authentication, path comparison)



https://www.anapaya.net/scion-internet

- **Path Verification:** Der Pfad und die Integrität aller Pakete ist kryptografisch gesichert und verifizierbar
- **Multi-Pathing:** zuverlässige Datenübertragung über mehrere Netzwerkpfade gleichzeitig
- **Cybersecurity:** kein Umleiten Ihrer Daten mehr möglich während der Übertragung; Schutz vor DDoS Reflection-Angriffen

https://static.www.switch.ch/sites/default/files/2023-10/switchlan-scion-access-factsheet-de_0.pdf



Source Address Spoofing

- No AS/Address filtering
- If destination performs path-lookup → Works
- Forcing path-lookup (with almost expired paths) → Not working

Prevention:

High level of security

SCION's architecture gives you a high degree of reliability with various features and new concepts. As a result, some attacks can be prevented from the very outset: SCION is immune to prefix hijacking. What's more, the technology reduces the risk of exposure to distributed denial of service (DDoS) attacks through hidden paths and source authentication. The protection provided against address spoofing even prevents susceptibility to DDoS reflection attacks.

https://www.switch.ch/en/network/scion-access

Future Plan

- Anapaya Device – make use of found weaknesses/vulnerabilities (Threat model: Outside attacker, no local access)
- Impact of SCION user outside of CYD
- Volumetric DoS “normal” Internet → Impact on SCION