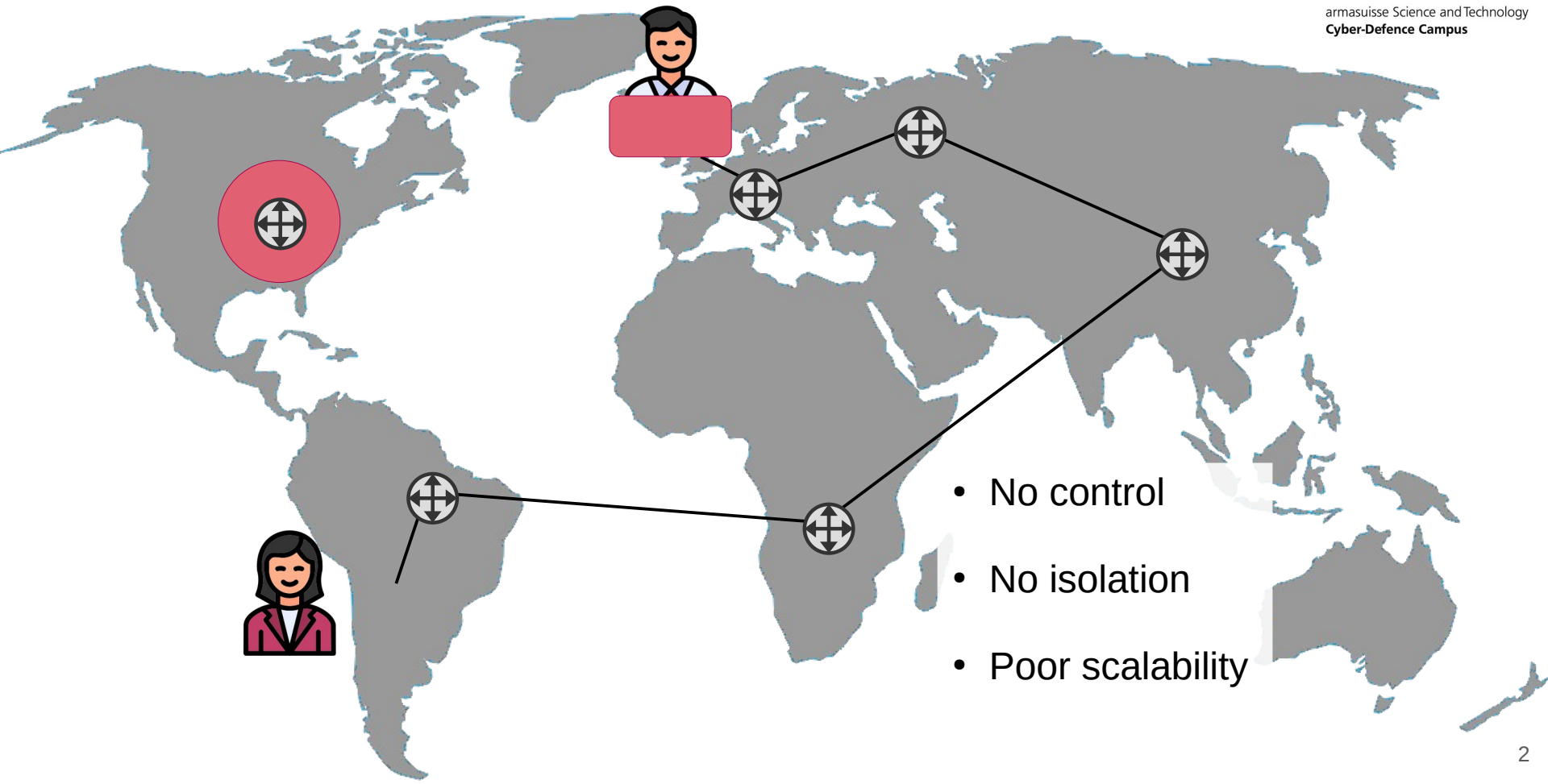


Security Analysis of the Internet Architecture

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

ScionTM

Scalability, Control, and Isolation on Next-Generation Networks

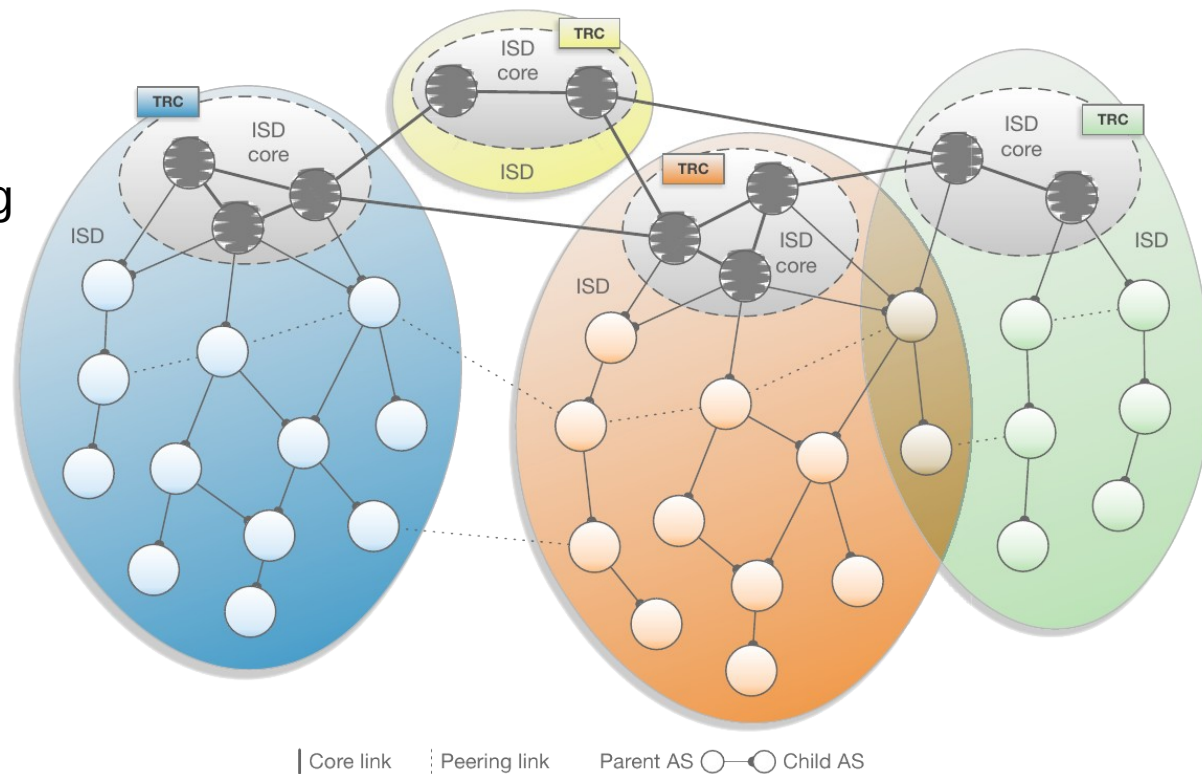
- Developed at ETH Zurich
- Open-Source
- Commercialized by Anapaya

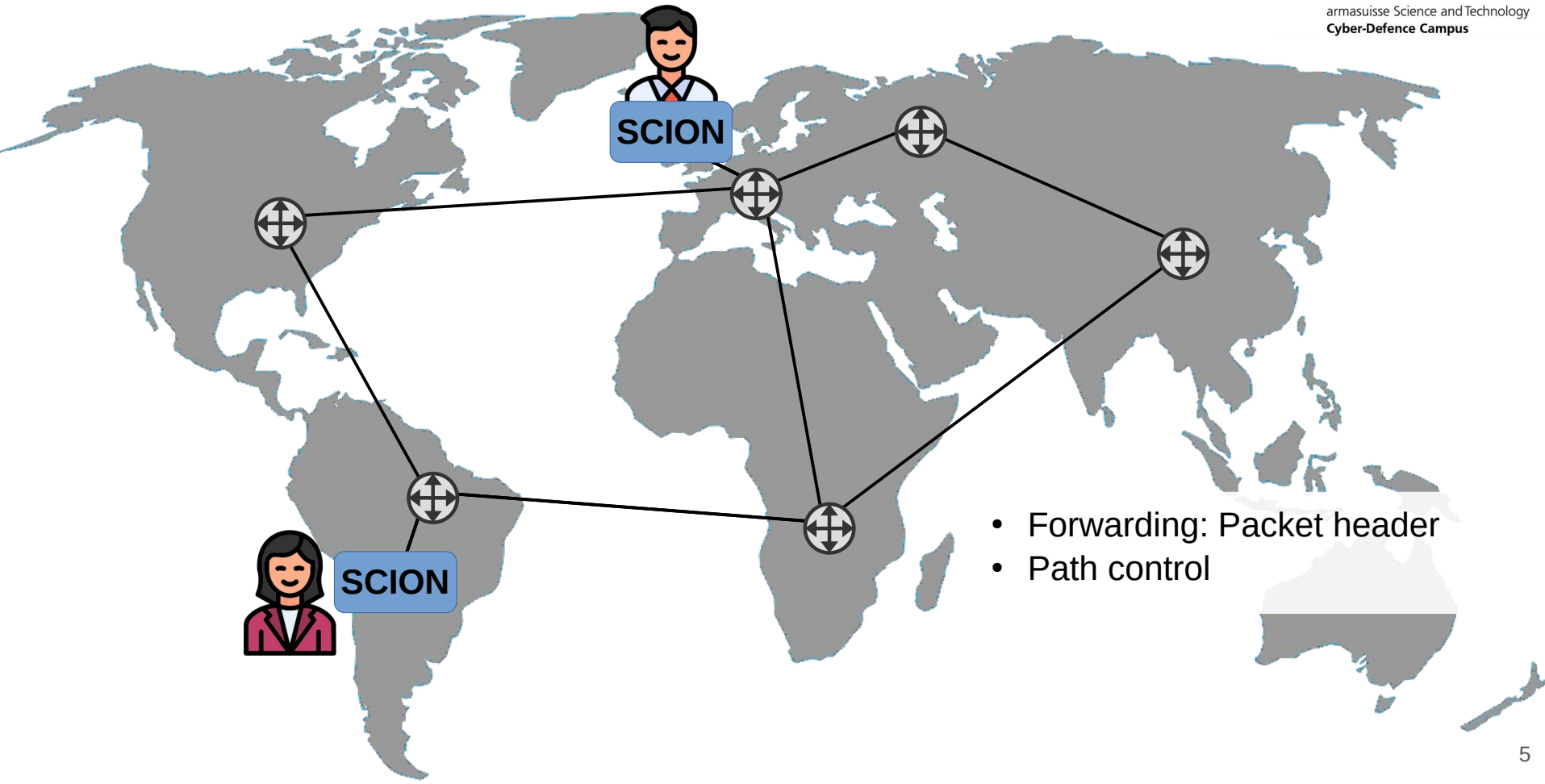
Isolation domain (ISD):

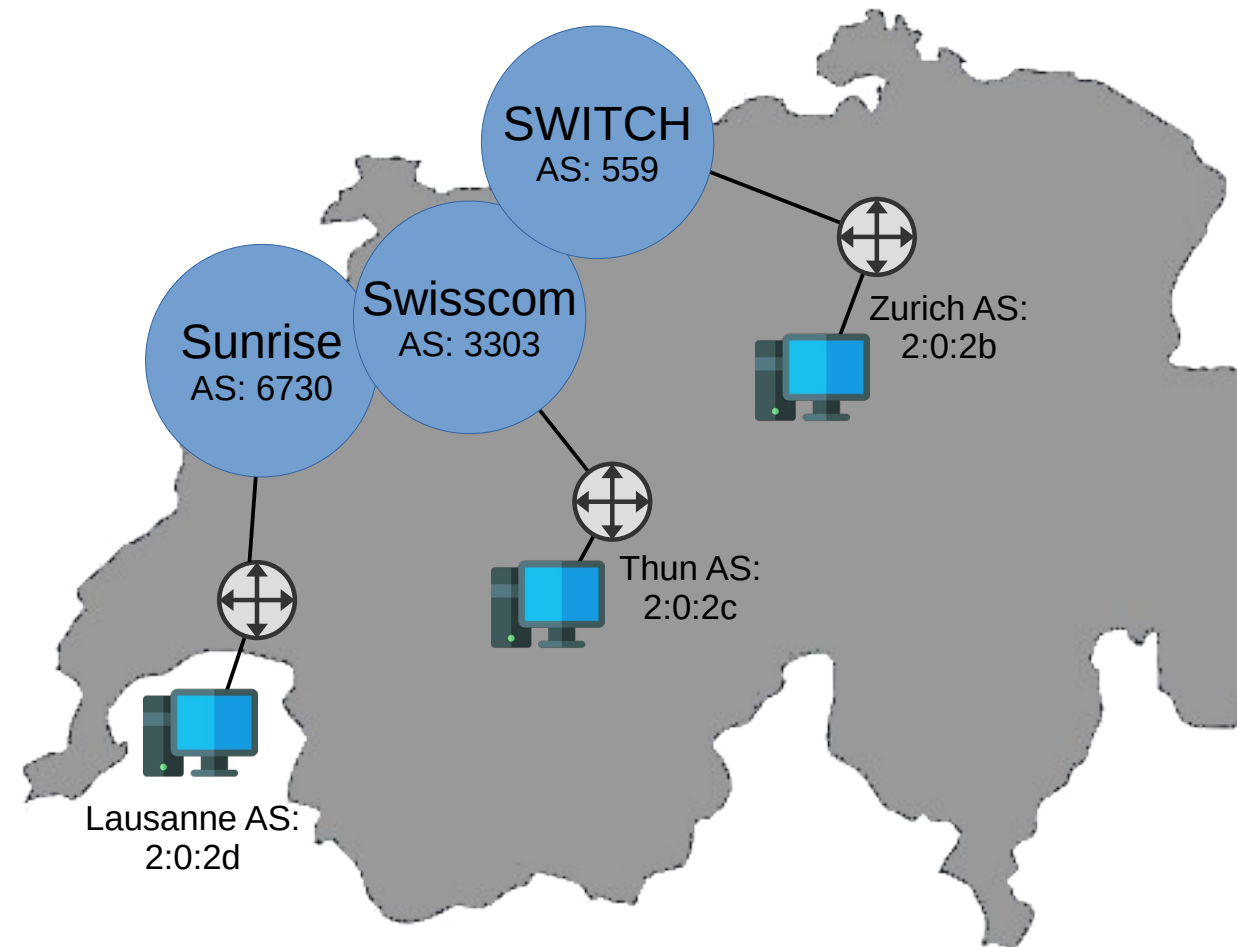
- Isolate routing within ISD
- Scalability: separate routing within / between ISD

ISD Core:

- Root of trust
- Init path construction







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

The screenshot shows a web browser window with the URL `https://[redacted]/configuration/editor#scion`. The page title is "Appliance UI". The interface is for the "ANAPAYA" configuration editor. On the left, there is a sidebar with the following sections:

- Configuration**
 - Editor
 - Expert Editor
- Control Plane PKI**
 - Trust Roots
 - Certificate Chains
 - Signing Requests
- Tools**
 - SCION Ping
 - SCION Traceroute
 - SCION Showpaths
- Documentation**
 - API

The main content area is titled "Router" and contains the following sections:

- Internal Interface**: A text input field with a redacted value and a help icon.
- Enabled**: A toggle switch that is currently turned on.
- Neighbors**: A section with a "Neighbor" entry.
 - Description**: A text input field with the value "SWITCH CH" and a help icon.
 - Neighbor ISD-AS ***: A text input field with the value "64-559" and a help icon.
 - Relationship ***: A dropdown menu with the value "PARENT" and a help icon.
- Interfaces**: A section with an "Interface" entry.
 - Enable SCION Rss**: A toggle switch that is currently turned off.
 - Address**: A text input field with a redacted value and a help icon.

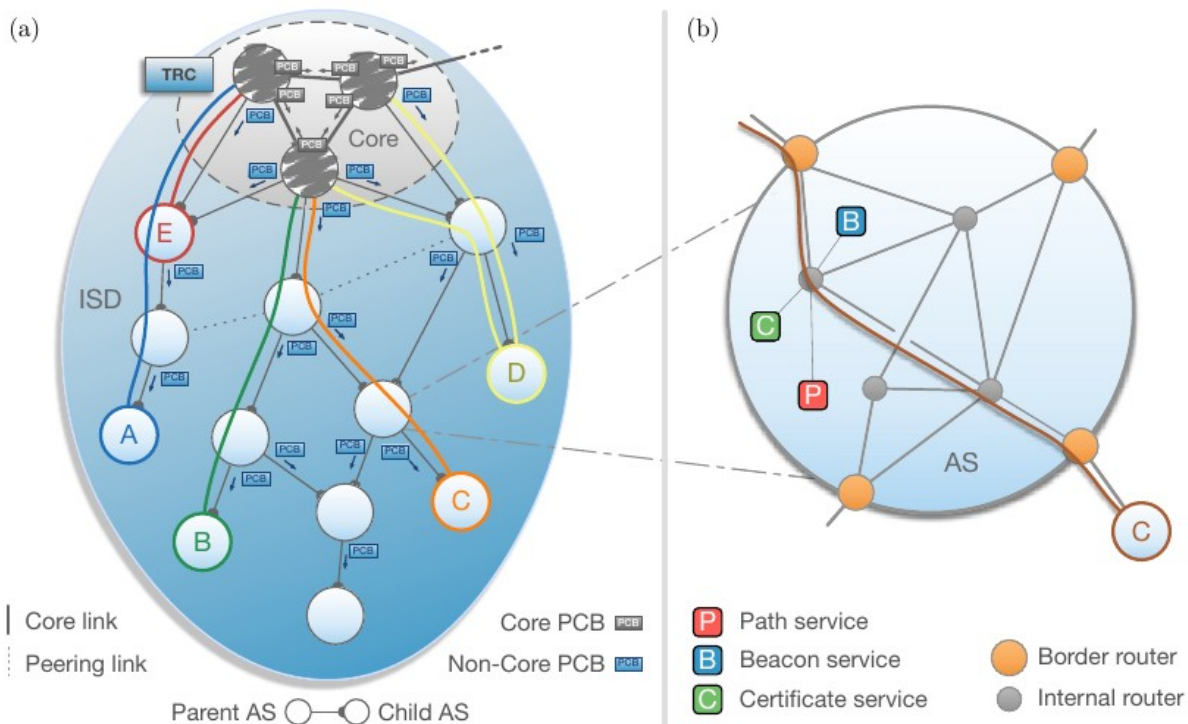
On the right side of the interface, there is a "Contents" sidebar with a list of configuration items: BGP, Global, Neighbors, Cluster, Features, Synchronization, Peers, Experiments, Features, Firewall, Firewall, Tables, Interfaces, Bonds, Ethernets, Loopbacks, Virtual Functions, Vlans, Wireguards, Management, General, API, Remote Repository, Telemetry, Nat, Snat, SCION, Synchronization, ASes, SCION Tunneling, Endpoint, Domains, Path Filters, Remotes, Static Announcements, Traffic Mirroring.

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>

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.

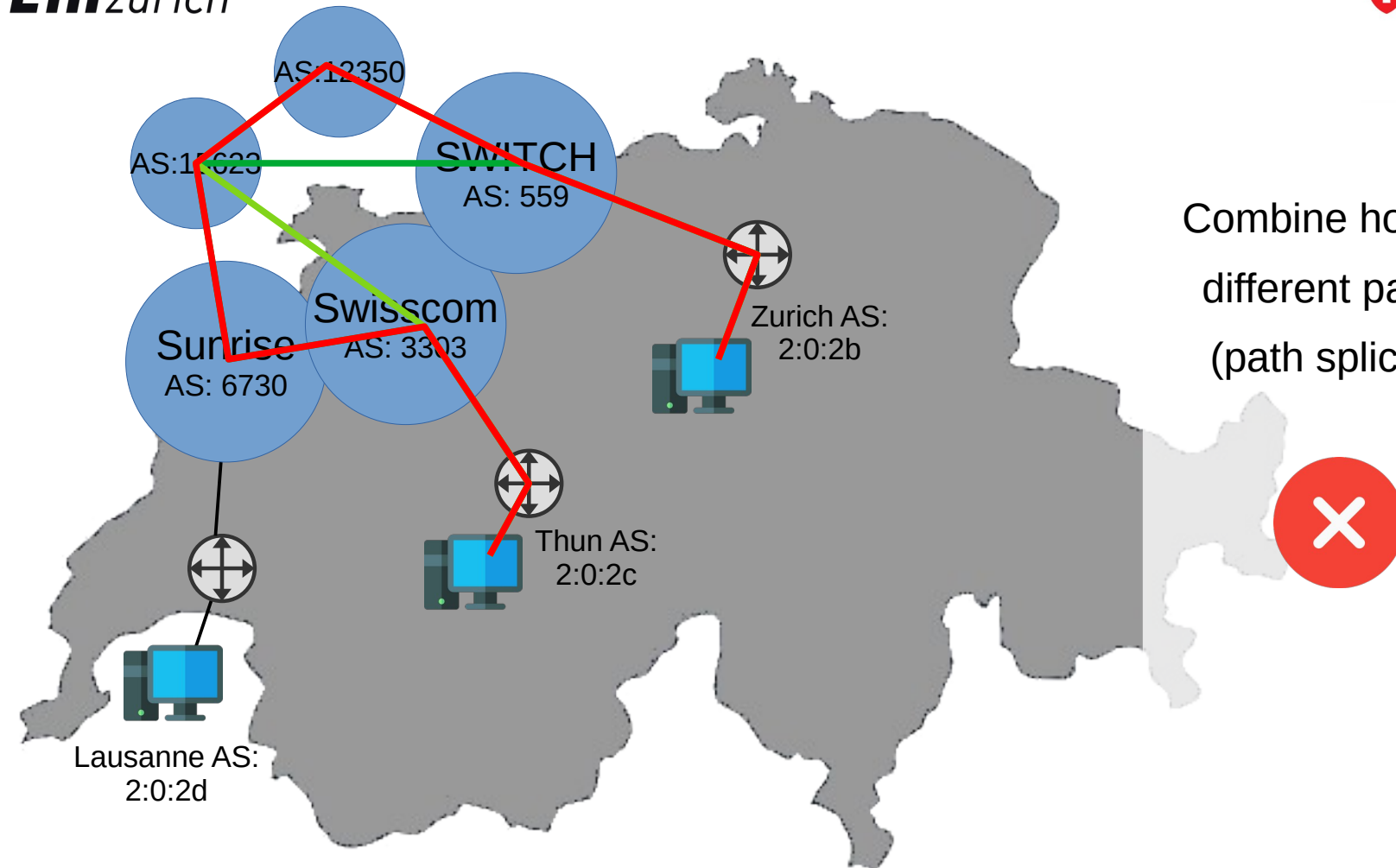
<https://www.swisscom.ch/en/business/enterprise/offer/wireline/scion.html>



Path control & multipath

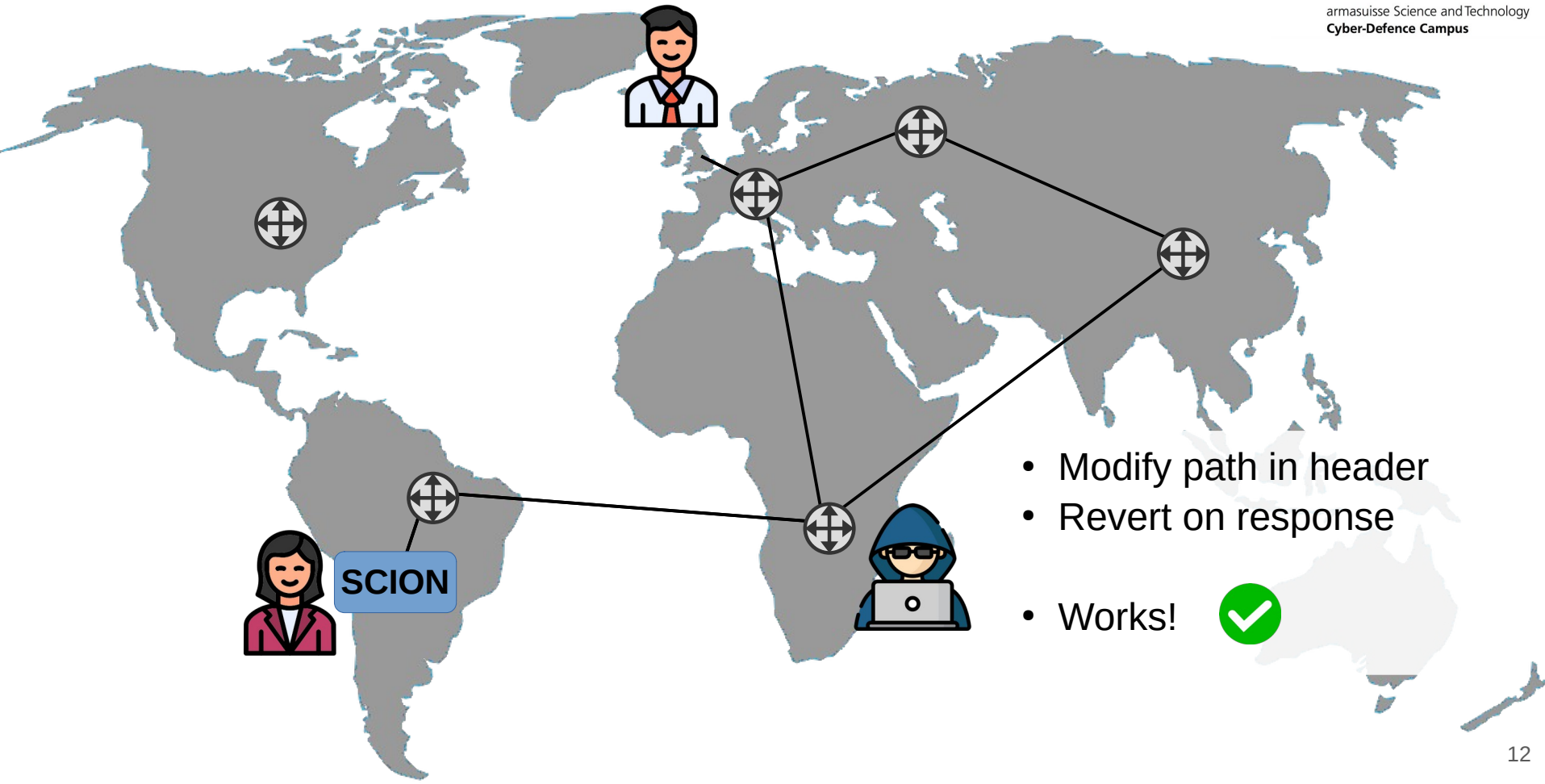
SCION allows the sender to control the routing, choosing exactly how and where data packets travel. With the multipath feature, senders can choose multiple paths at the same time.

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



Combine hops of
different paths
(path splicing)





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)

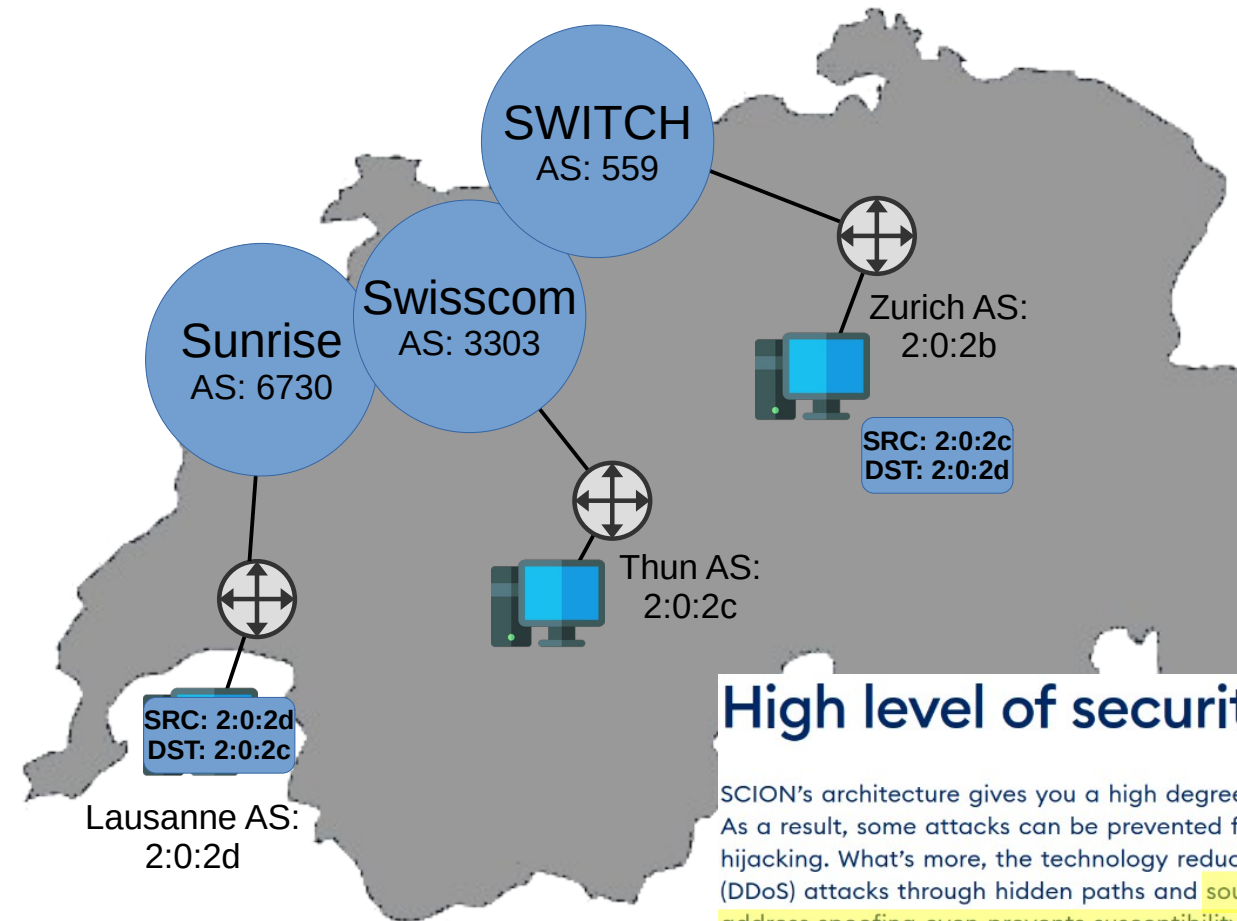


Explicit trust

With SCION, visualize and authenticate your data's route using cryptographic methods. This explicit trust mechanism ensures secure and transparent data transmission.

<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



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.**

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