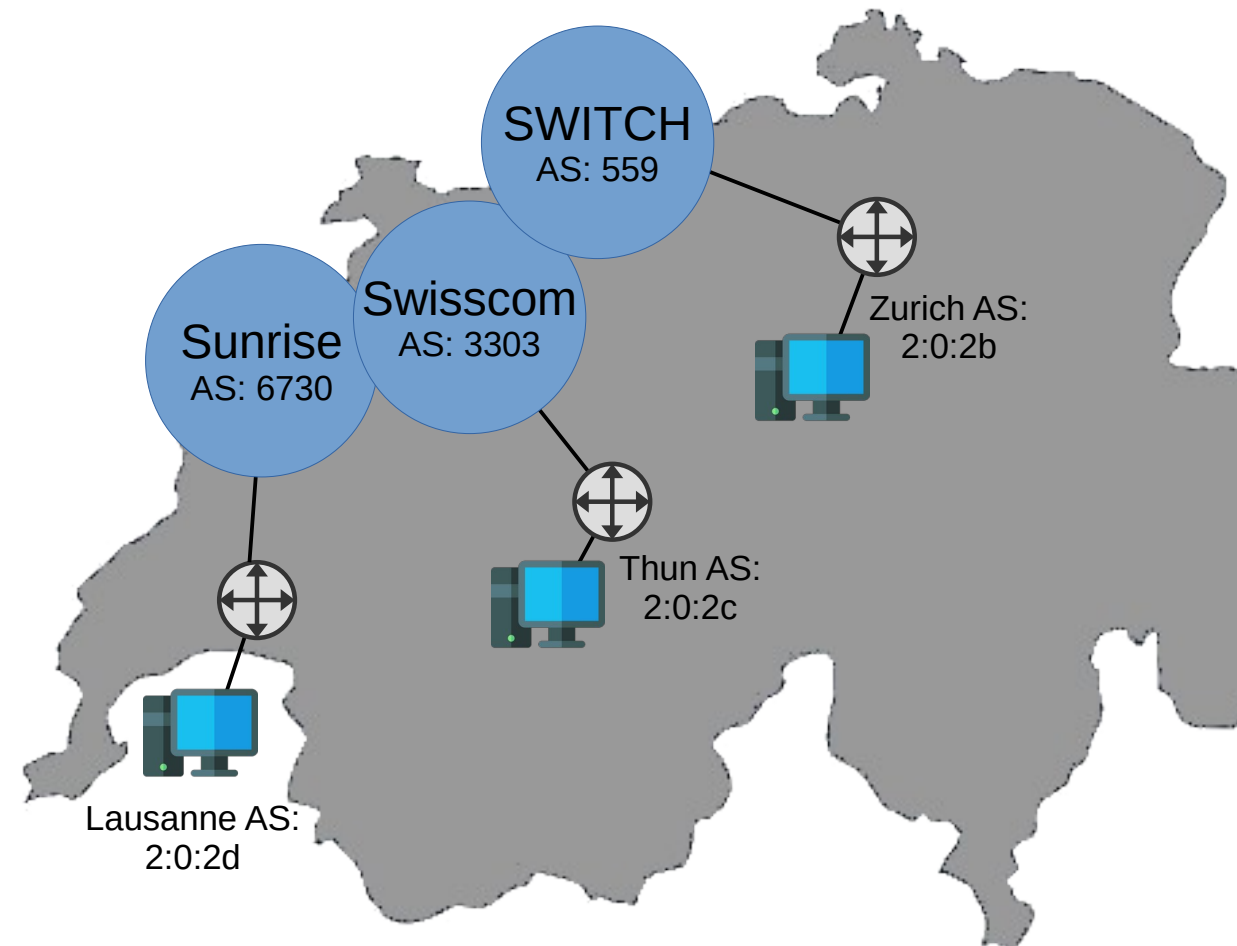


# Security Analysis of the Internet Architecture

Master Thesis - Marco Seewer

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



## 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
  - Rev. engineering SCION binary
  - SCION configuration (Appliance)



[https://www.supermicro.com/files\\_SYS/images/System/SYS-110D-8C-FRAN8TP\\_main.jpg](https://www.supermicro.com/files_SYS/images/System/SYS-110D-8C-FRAN8TP_main.jpg)

# Anapaya Device – Router – Results

- Scans: Many false positives  
(Attacker model: Outside attacker, no local access)
- Compliance scans (Passwordless sudo, no password policy, no login timelimit)
- Docker images (contains vulnerable openssl version, docker base image contains vulnerable libraries)



[https://www.supermicro.com/files\\_SYS/images/System/SYS-110D-8C-FRAN8TP\\_main.jpg](https://www.supermicro.com/files_SYS/images/System/SYS-110D-8C-FRAN8TP_main.jpg)

Appliance UI

https://[redacted]/configuration/editor#scion

ANAPAYA

**Configuration**

- Editor
- Expert Editor

**Control Plane PKI**

- Trust Roots
- Certificate Chains
- Signing Requests

**Tools**

- SCION Ping
- SCION Traceroute
- SCION Showpaths

**Documentation**

- API

**Router**

Internal Interface

[redacted]

Enabled

**Neighbors**

Neighbor

Description
SWITCH CH

Neighbor ISD-AS \*

64-559

Relationship \*

PARENT

**Interfaces**

Interface

Interface
Enable SCION Rss

Address

[redacted]

**Contents**

- 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 Markers

No authentication!

Every CYD SCION  
user can:

- change config
- upload/install/delete  
any packages  
(binaries)
- add new TRC

# SCION Protocol – Hop fields

- MAC in Hop fields
- Extracted BR secret + derive MAC value
- MAC algorithm = open-source = secure

# 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.

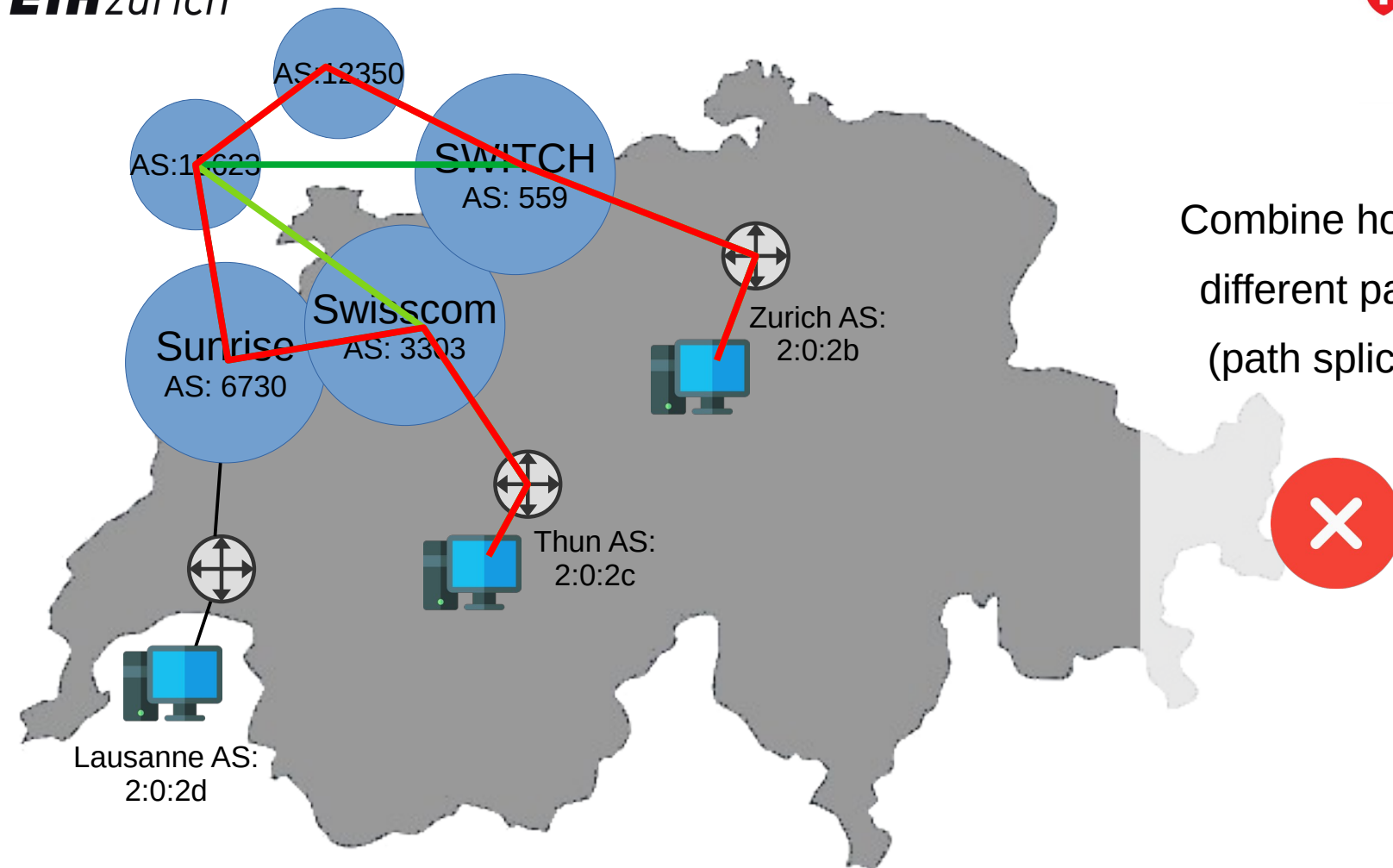
<https://www.swisscom.ch/en/business/enterprise/offer/wireline/scion.html>



## 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.

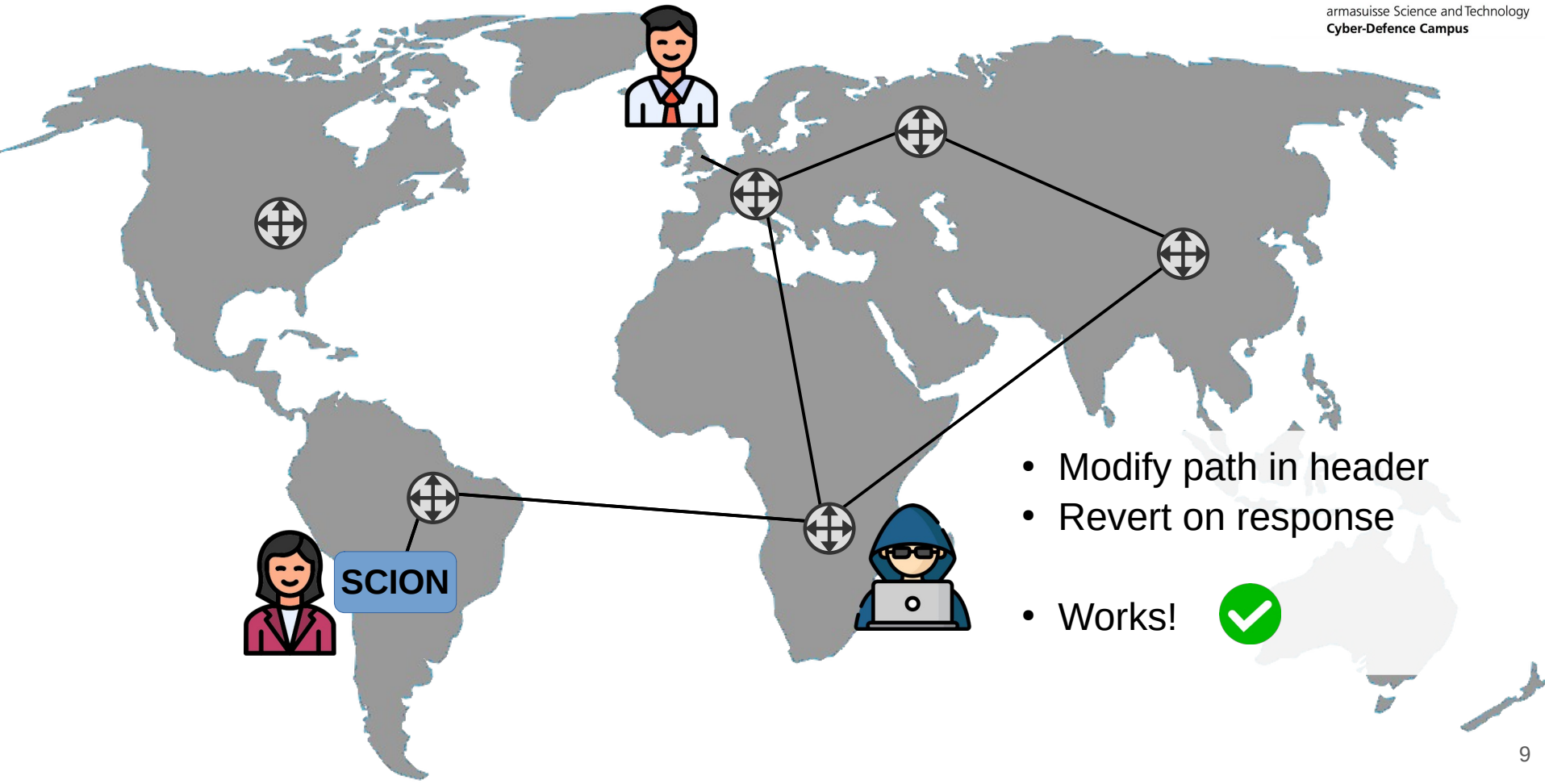
<https://www.anapaya.net/scion-internet>



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)

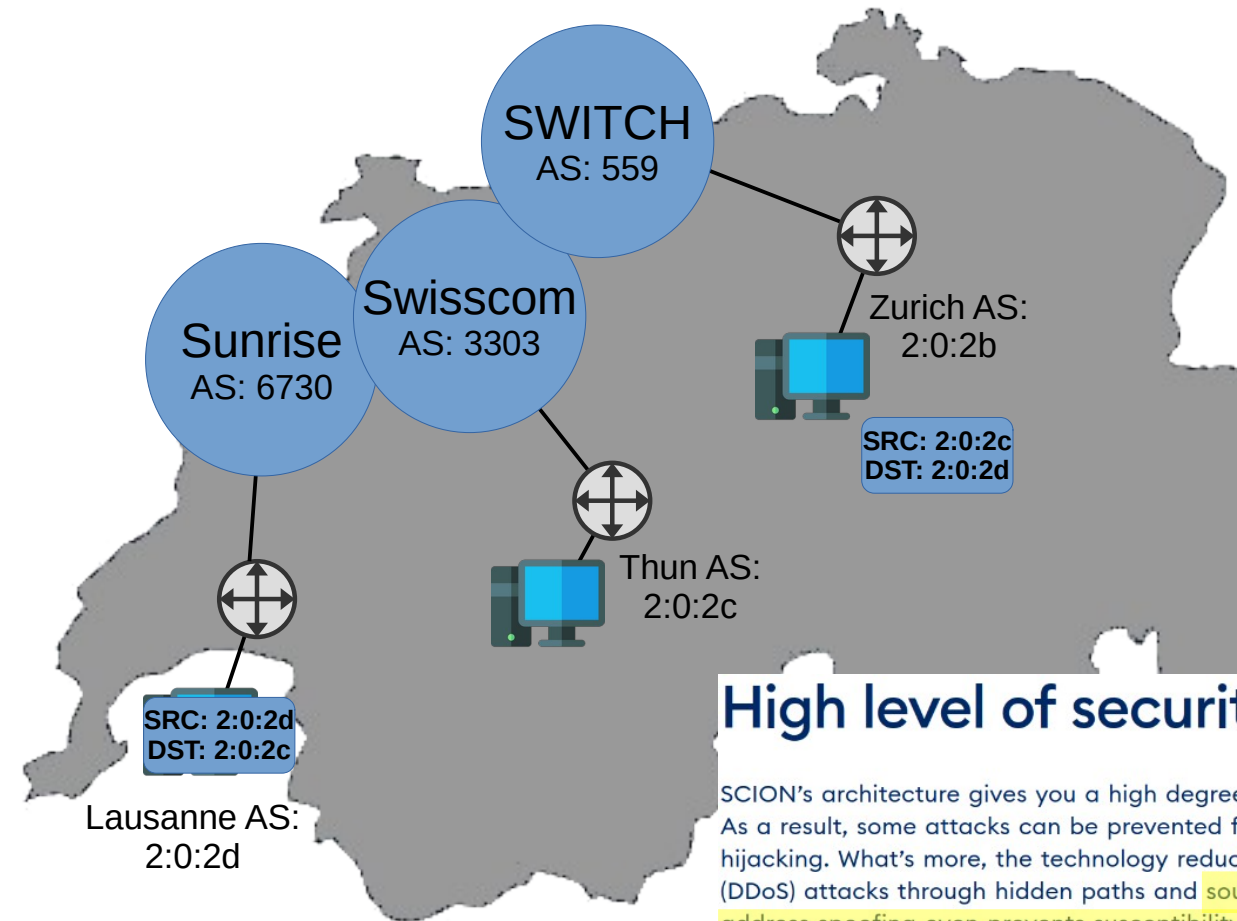


## Explicit trust



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 (exploit possible?), Webapp (=Appliance)
- Source code SCION binary (Anapaya) OR rev. engineering
- Impact of SCION user outside of CYD
- Volumetric DoS “normal” Internet → Impact on SCION