ETH zürich

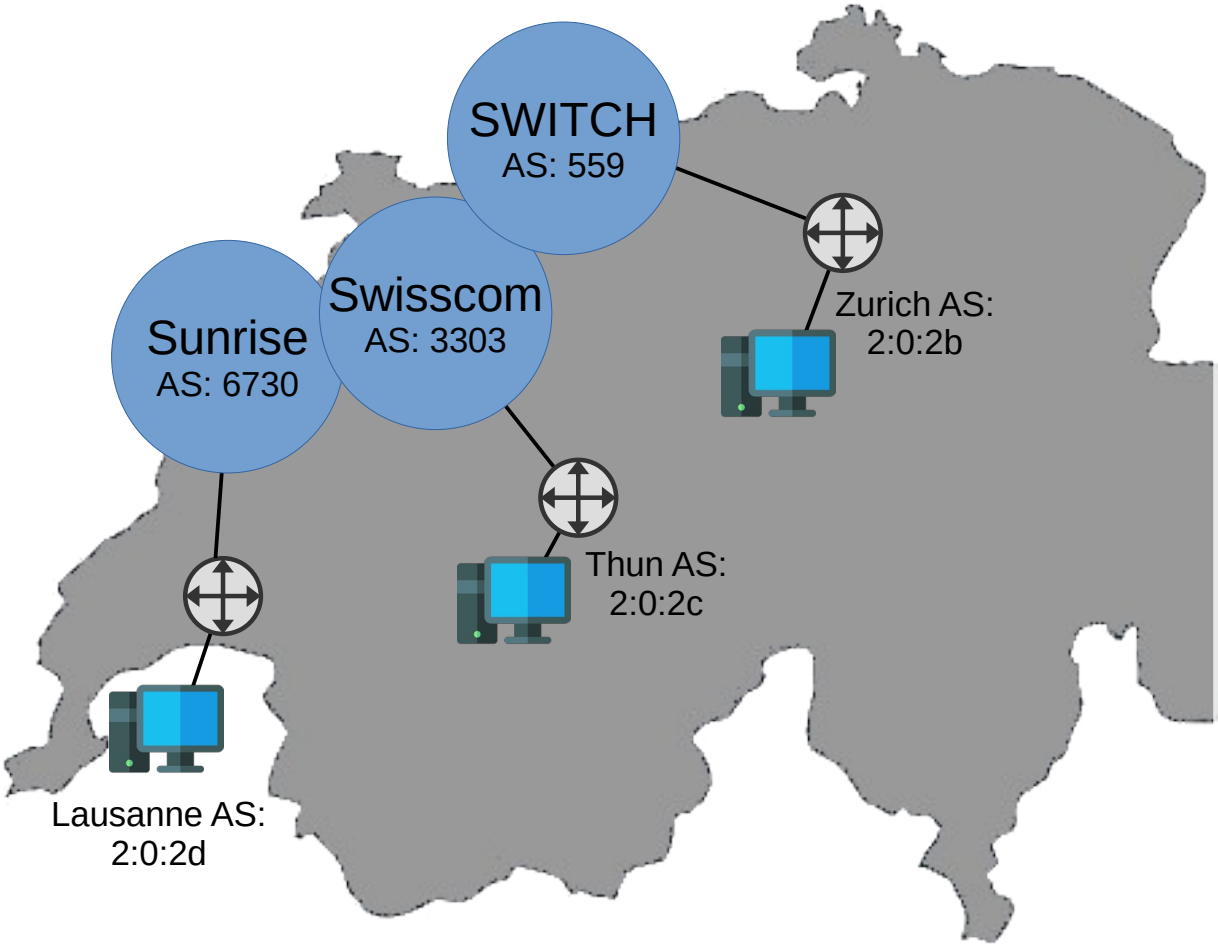
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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.



Setup CYD Testbed:

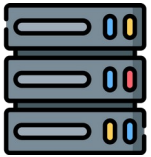
- 3 ASes
- 3 Core ASes
  - SCION Production Network
- Anapaya Routers
  - 3 operational
  - 1 offline test device


WHY?

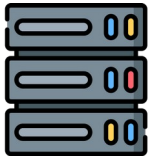
Problem

1) SCION protocol implementation:

Anapaya version  Open-source version

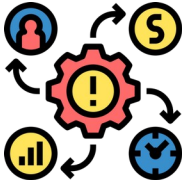
2) Anapaya devices 

Focus



1) Security of Operational Devices

2) SCION Network in use



3) Volumetric Impact

Process

- Independent security analysis
- Disclosure with Anapaya
- Software updates
- Approval for publication/presentation

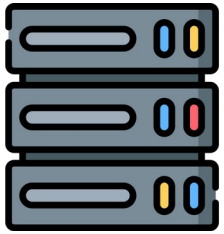
Process

- Independent security analysis
- Disclosure with Anapaya
- Software updates
- Approval for publication/presentation

Attacker models:

- SCION end-host
- On-path
- Off-path
- Non-SCION adversary

1) Anapaya's SCION device



Anapaya Device

- Unauthenticated + authenticated vulnerability scans
- Scan results applicable (threat model: No local access)
- Compliance scans
- Docker images
- Open ports + running services
- Exposure of systemd services
- SSH configurations
- SCION configuration (Management system)

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

SSH Configuration

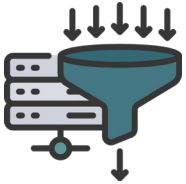
Only public-key authentication

Some less secure algorithms enabled

SSH Configuration

Only public-key authentication

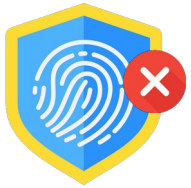
Some less secure algorithms enabled



No rate limiting → DHEat attack:

- Send many DH keys (or random big numbers)
- Expensive modular exponentiation → CPU
- SCION services unaffected

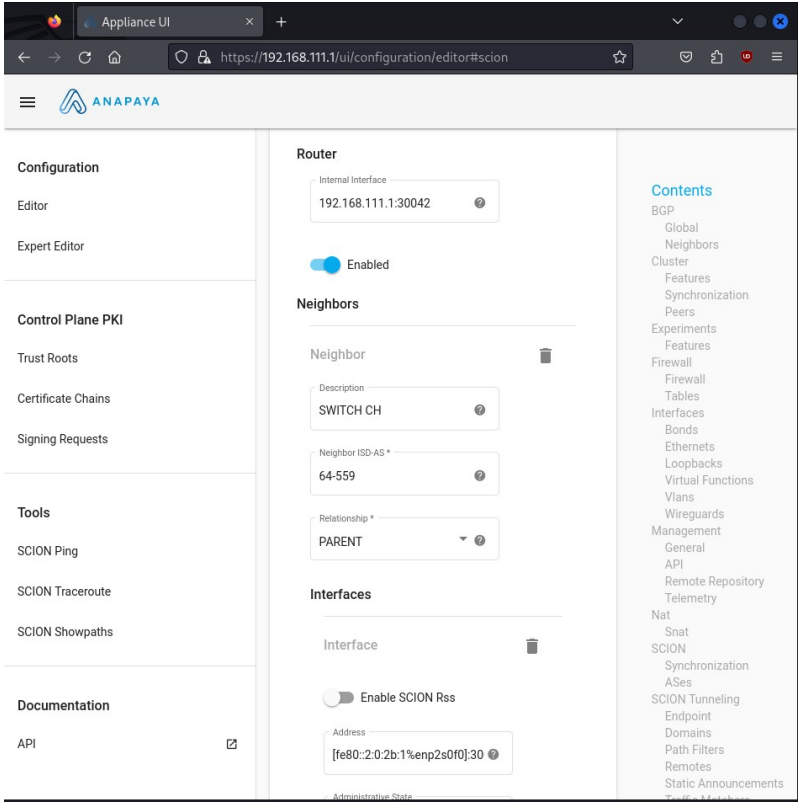
Management System



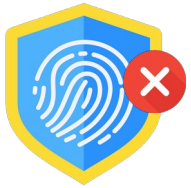
No authentication enabled!

Every CYD SCION user can:

- Change configuration
- Upload/Install/Delete any packages (binaries)
- Add new TRC



Management System

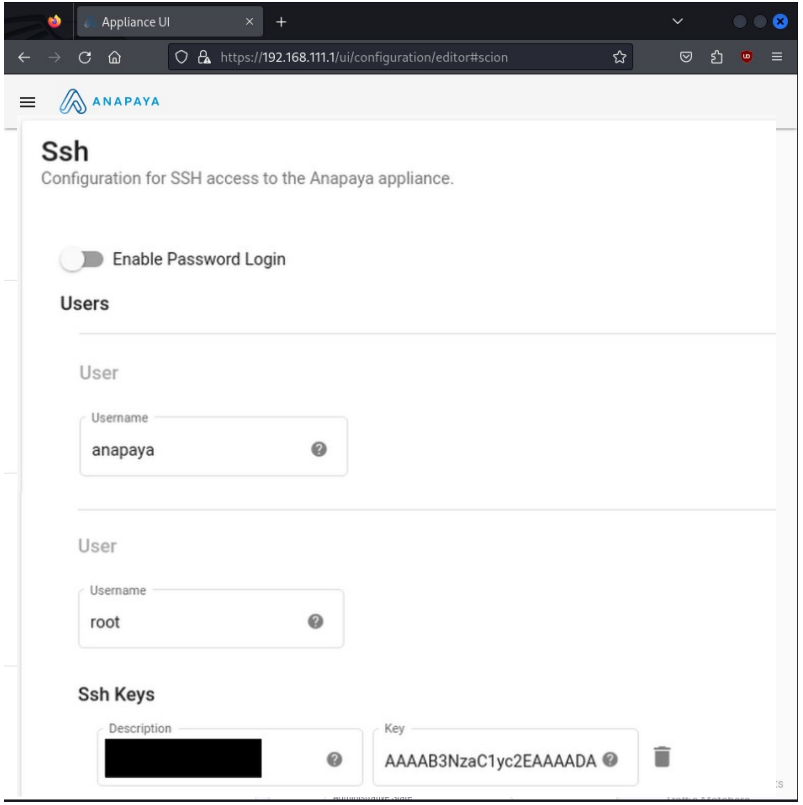


No authentication enabled!

Every CYD SCION user can:

- Change configuration
- Upload/Install/Delete any packages (binaries)
- Add new TRC

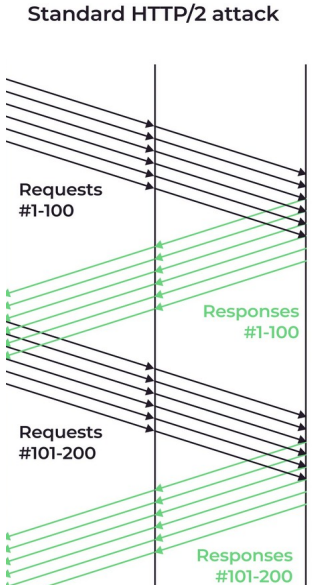
Add/Delete Users + SSH keys

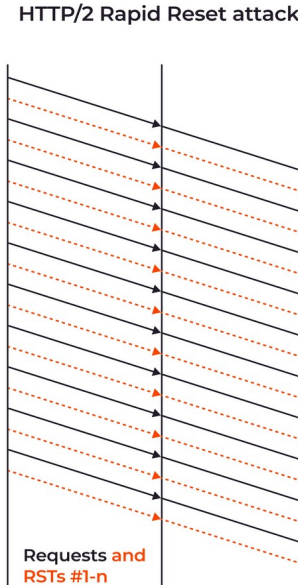


Management System

Webserver (Caddy) vulnerable

HTTP/2 Rapid Reset



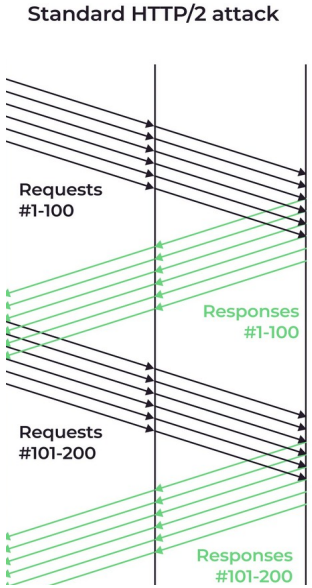


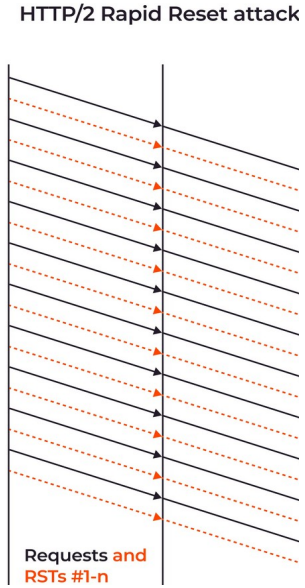
Management System

Webserver (Caddy) vulnerable HTTP/2 Rapid Reset

Resource exhaustion

Works even with enabled authentication



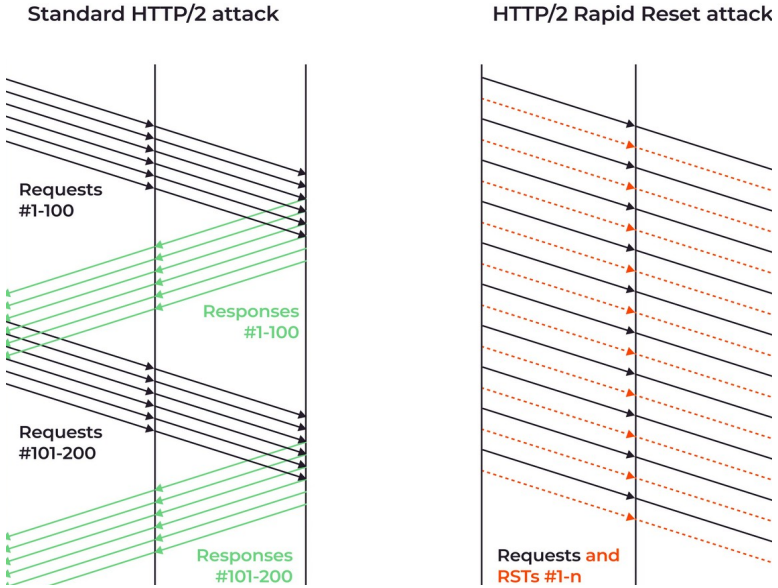


Management System

Webserver (Caddy) vulnerable HTTP/2 Rapid Reset

Resource exhaustion

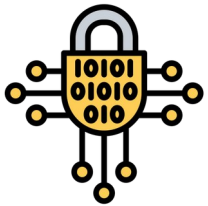
Works even with enabled authentication



Demo

2) Anapaya's SCION protocol

SCION Protocol – Anapaya Version



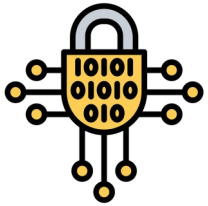
Cryptography

- Hop Field MAC - Algorithm
- Source Authentication – DRKey

Packet Manipulation

- Field/header modifications
- Path modification (Path splicing, path extension)
- Spoofing

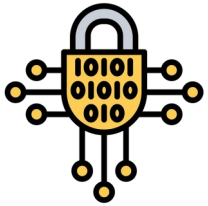
Cryptography



Hop Field MAC

- Anapaya == Open-source (AES-CMAC)
- Master Secret (used to derive MAC key) fixed → never refreshed

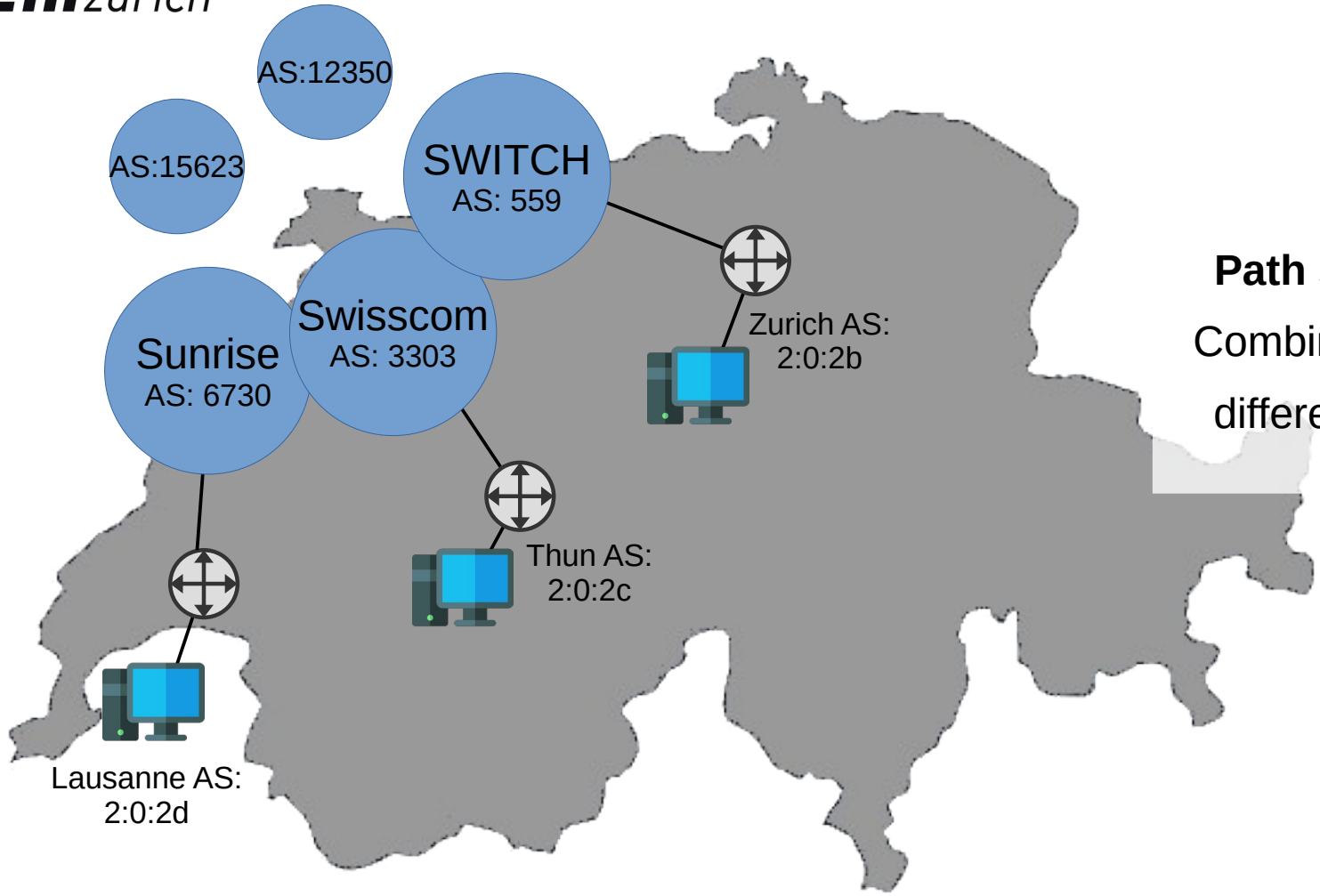
Cryptography



Hop Field MAC

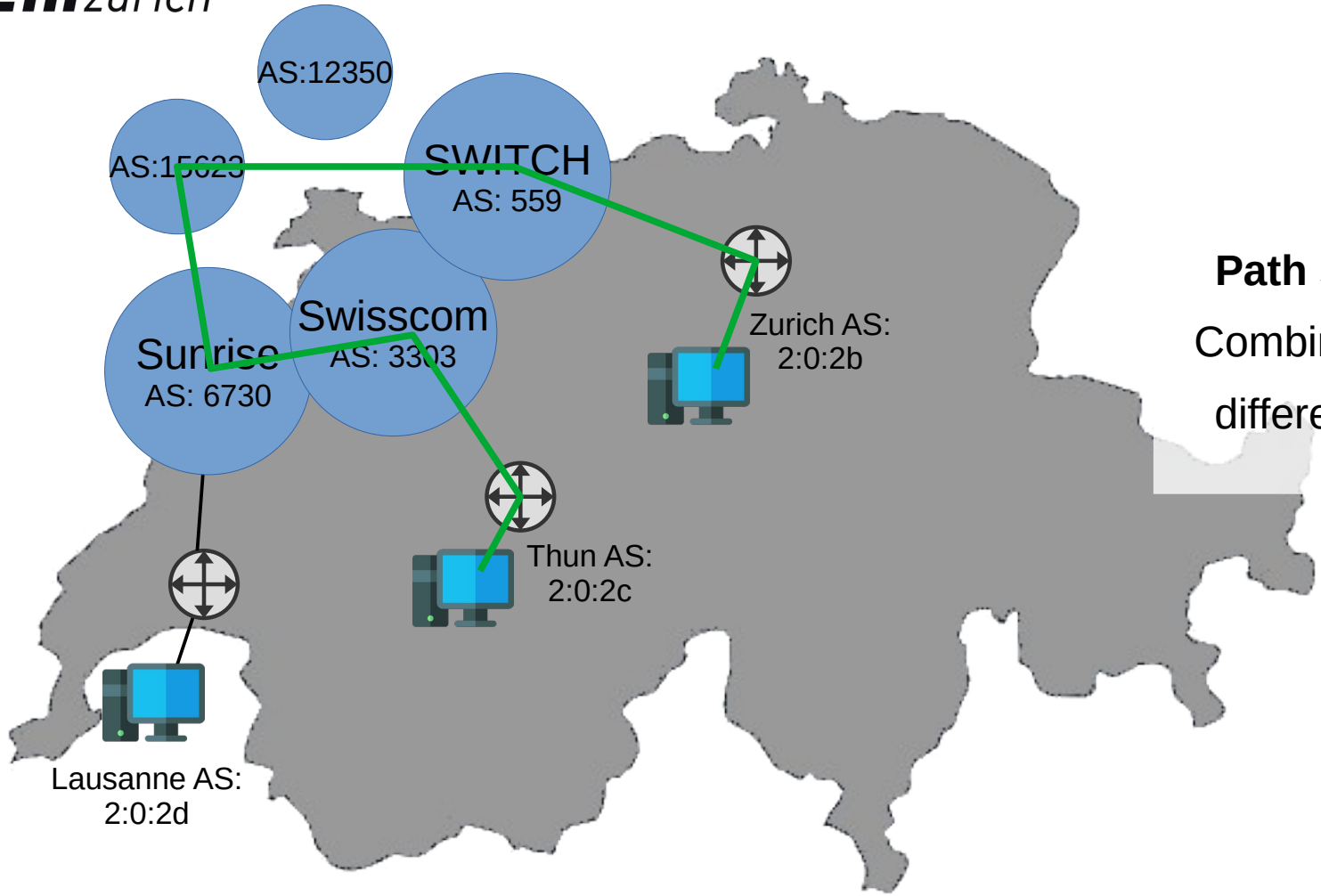
- Anapaya == Open-source (AES-CMAC)
- Master Secret (used to derive MAC key) fixed →never refreshed

Check if MAC is verified



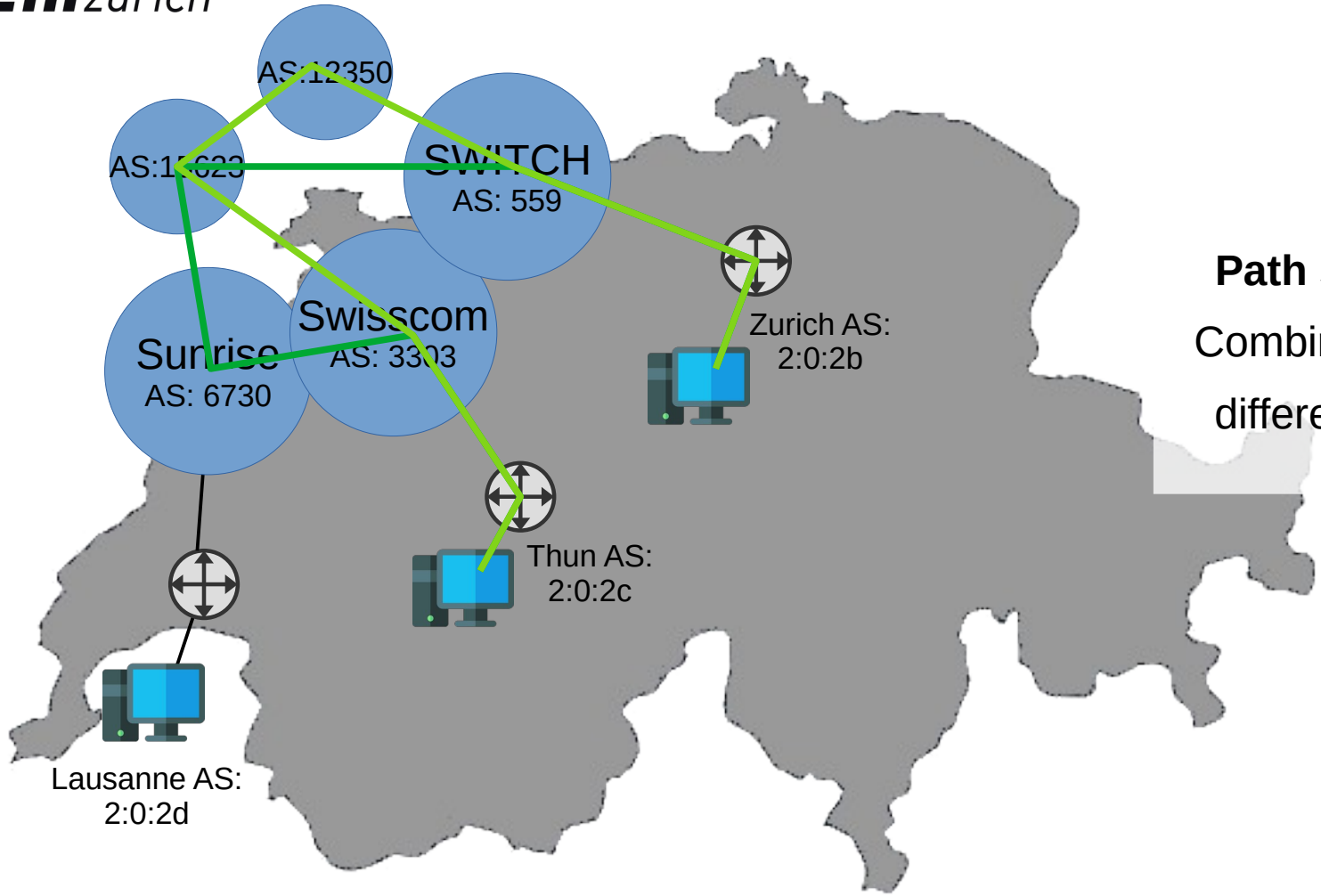
Path splicing:

Combine hops of different paths



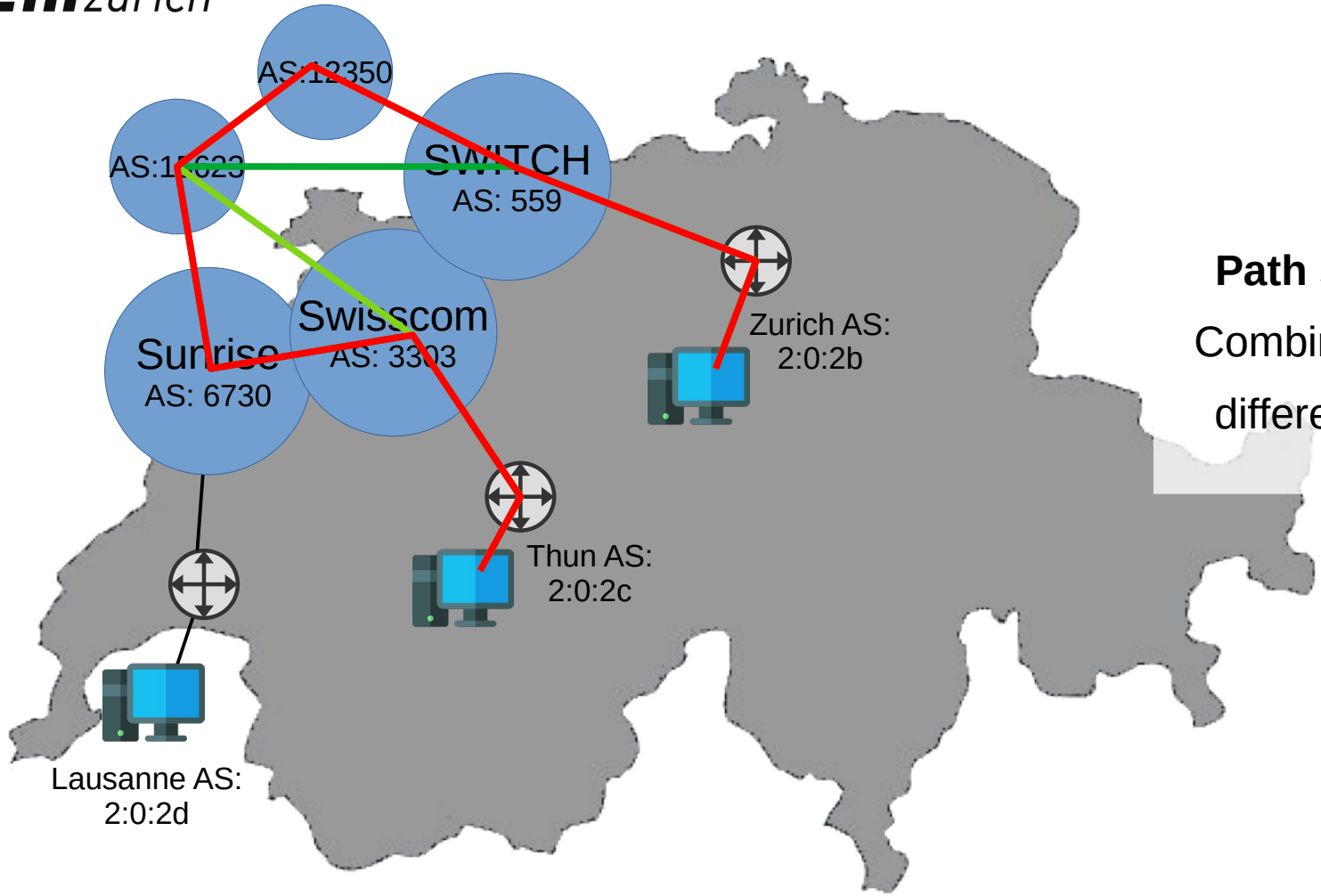
Path splicing:

Combine hops of different paths



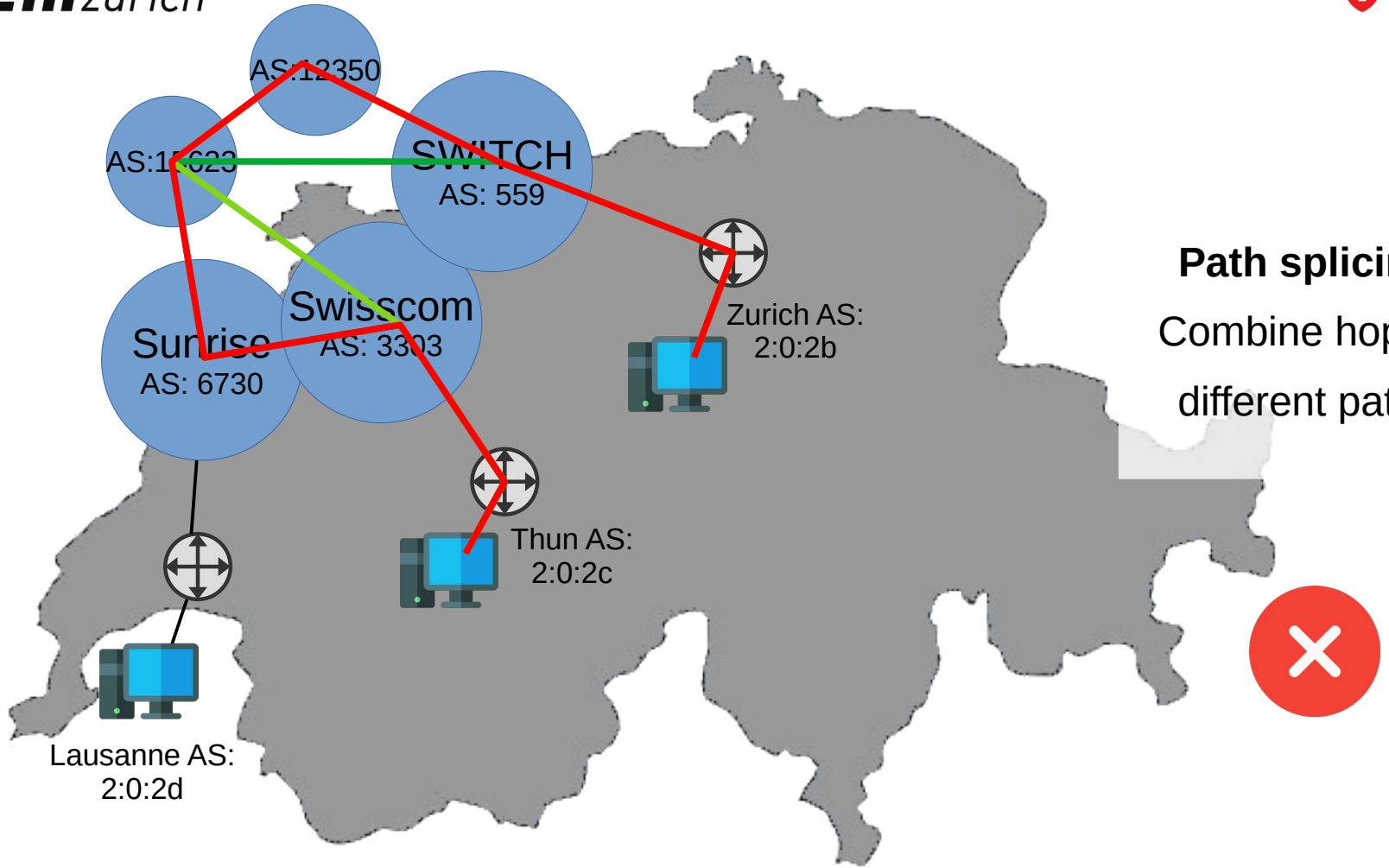
Path splicing:

Combine hops of different paths



Path splicing:

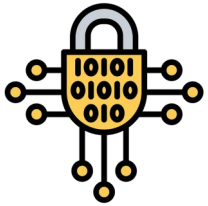
Combine hops of different paths



Path splicing:

Combine hops of different paths

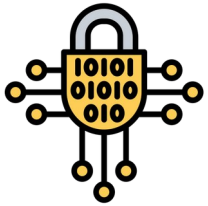
Cryptography



Hop Field MAC

- Anapaya == Open-source (AES-CMAC)
- Master Secret (used to derive MAC key) fixed →never refreshed
- MAC is verified by routers

Cryptography



Hop Field MAC

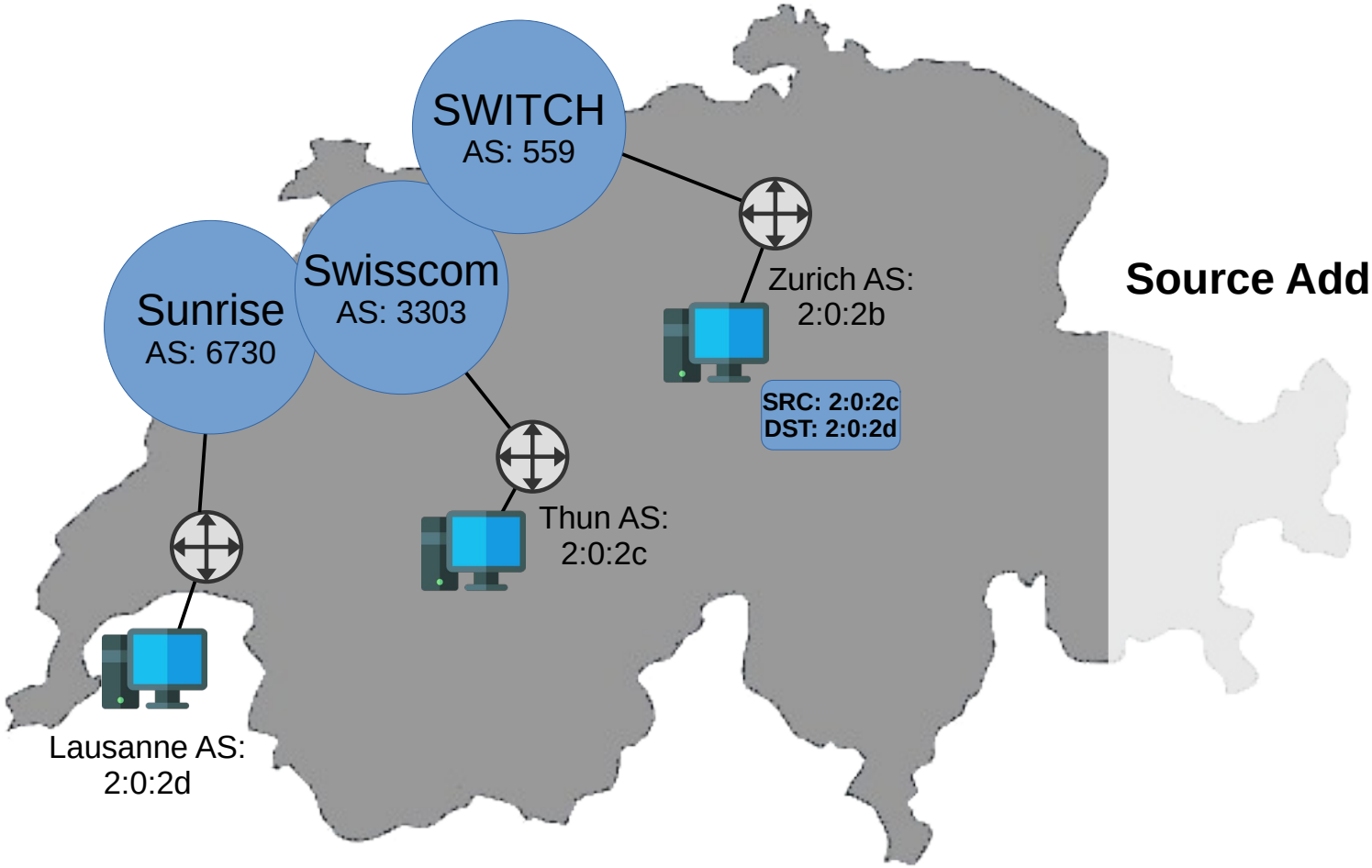
- Anapaya == Open-source (AES-CMAC)
- Master Secret (used to derive MAC key) fixed →never refreshed
- MAC is verified by routers

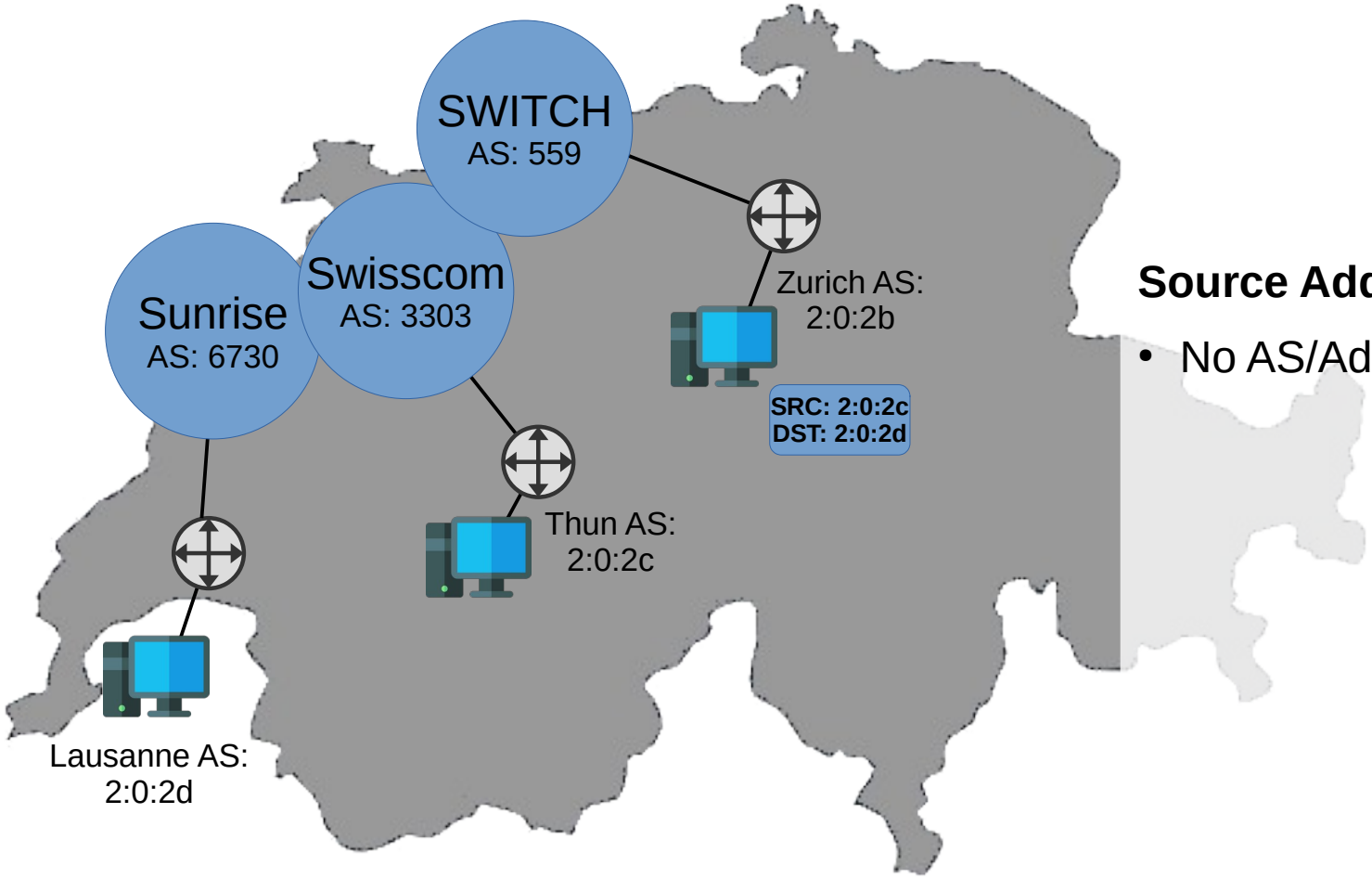
DRKey

- Not enabled/available

  → No source authentication (SPAO) possible
- Unauthenticated SCMP error messages

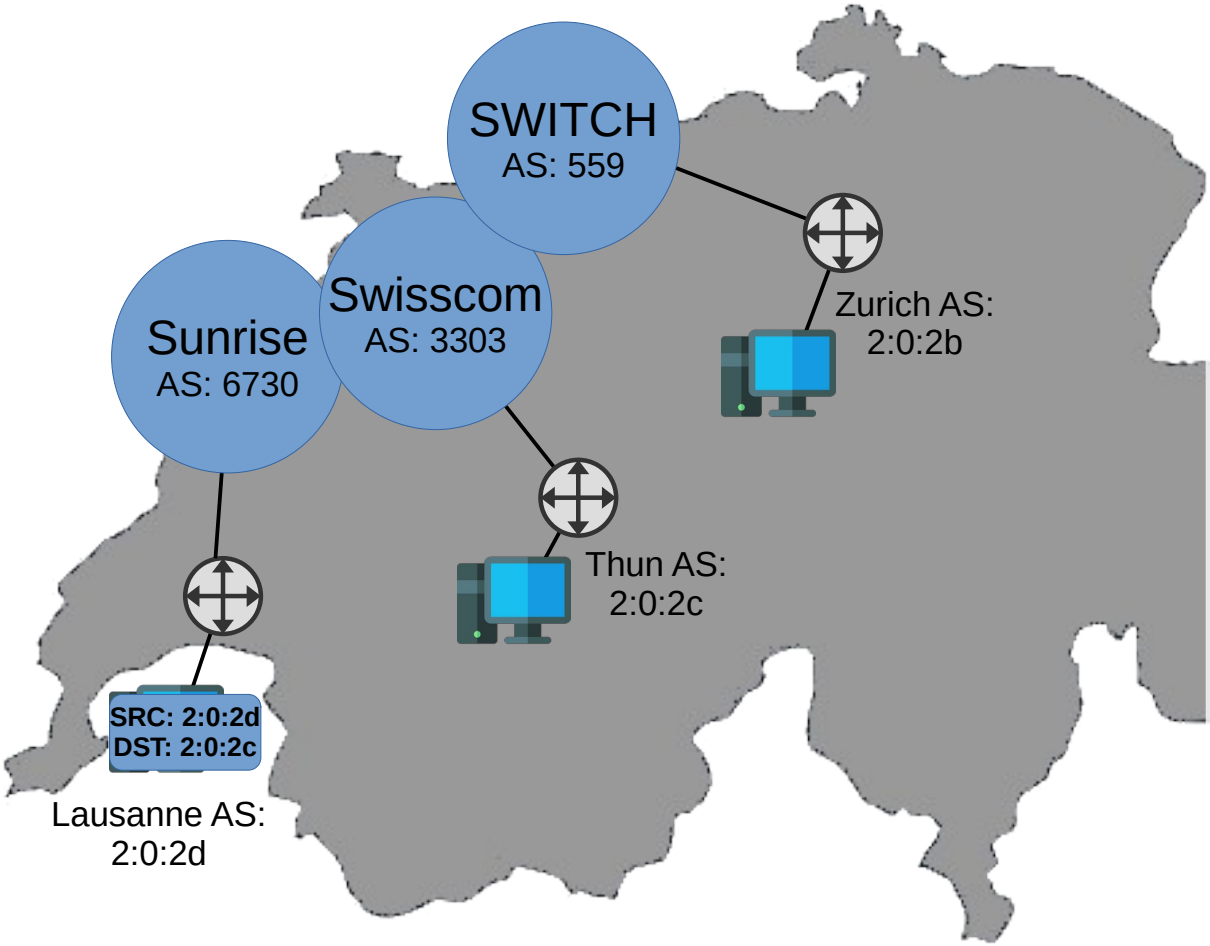
Source Address Spoofing





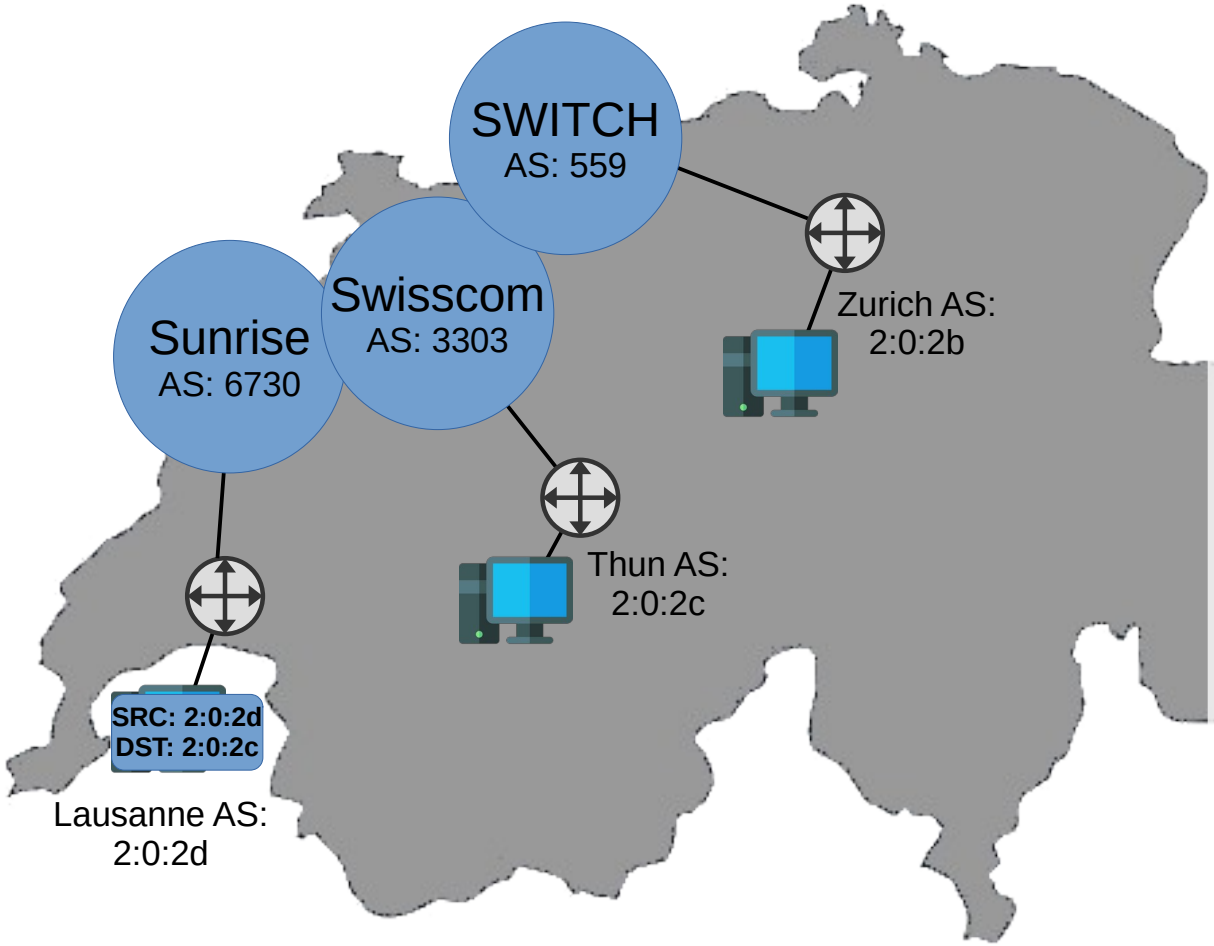
Source Address Spoofing

- No AS/Address filtering



Source Address Spoofing

- No AS/Address filtering
- If destination performs path-lookup → Works



Source Address Spoofing

- No AS/Address filtering
- If destination performs path-lookup → Works

Can we force path-lookup?

Spoofing

Force path lookup with soon-to-expire paths

Feasibility depends on application

Spoofing ⟶ Protocol Divergence

Force path lookup with soon-to-expire paths

Feasibility depends on application

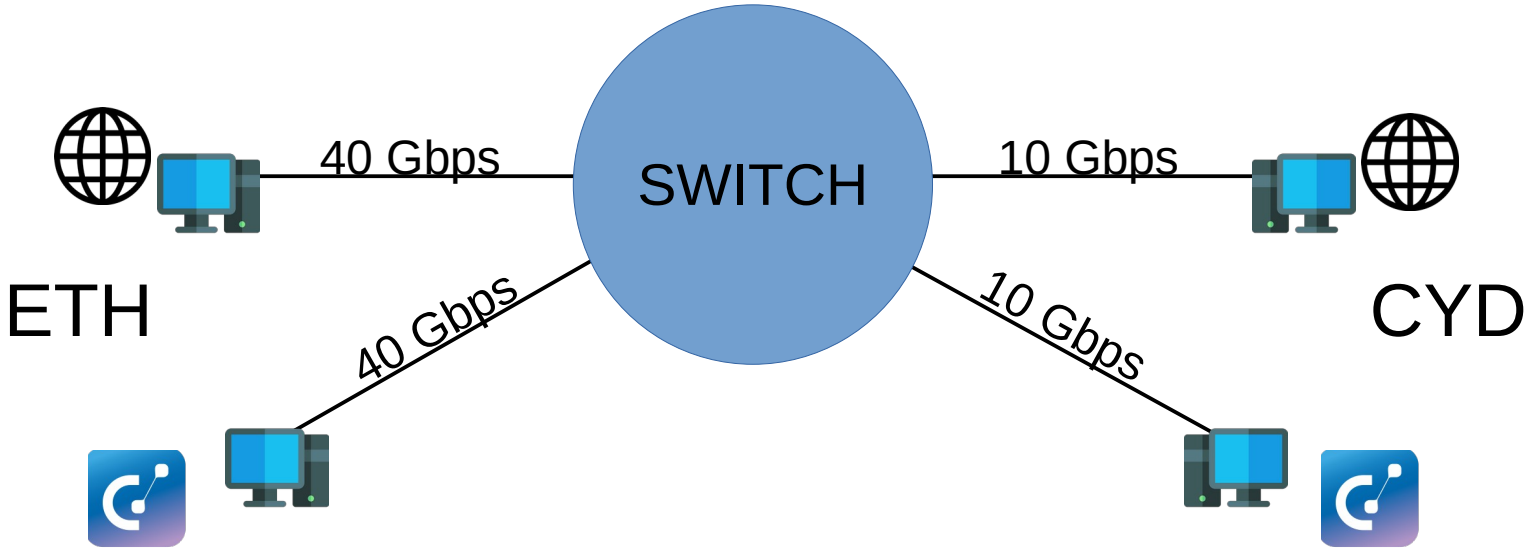
Valid path information got rejected (30s before actual expiry)

```
1 func (p *packetProcessor) validateHopExpiry() (processResult, error) {
2     expiration := util.SecsToTime(p.infoField.Timestamp).
3         Add(path.ExpTimeToDuration(p.hopField.ExpTime))
4     expired := expiration.Before(time.Now())
5     if !expired {
6         <move on with packet processing>
7     }
8     <drop packet + send SCMP packet with path expiry error>
9 }
```

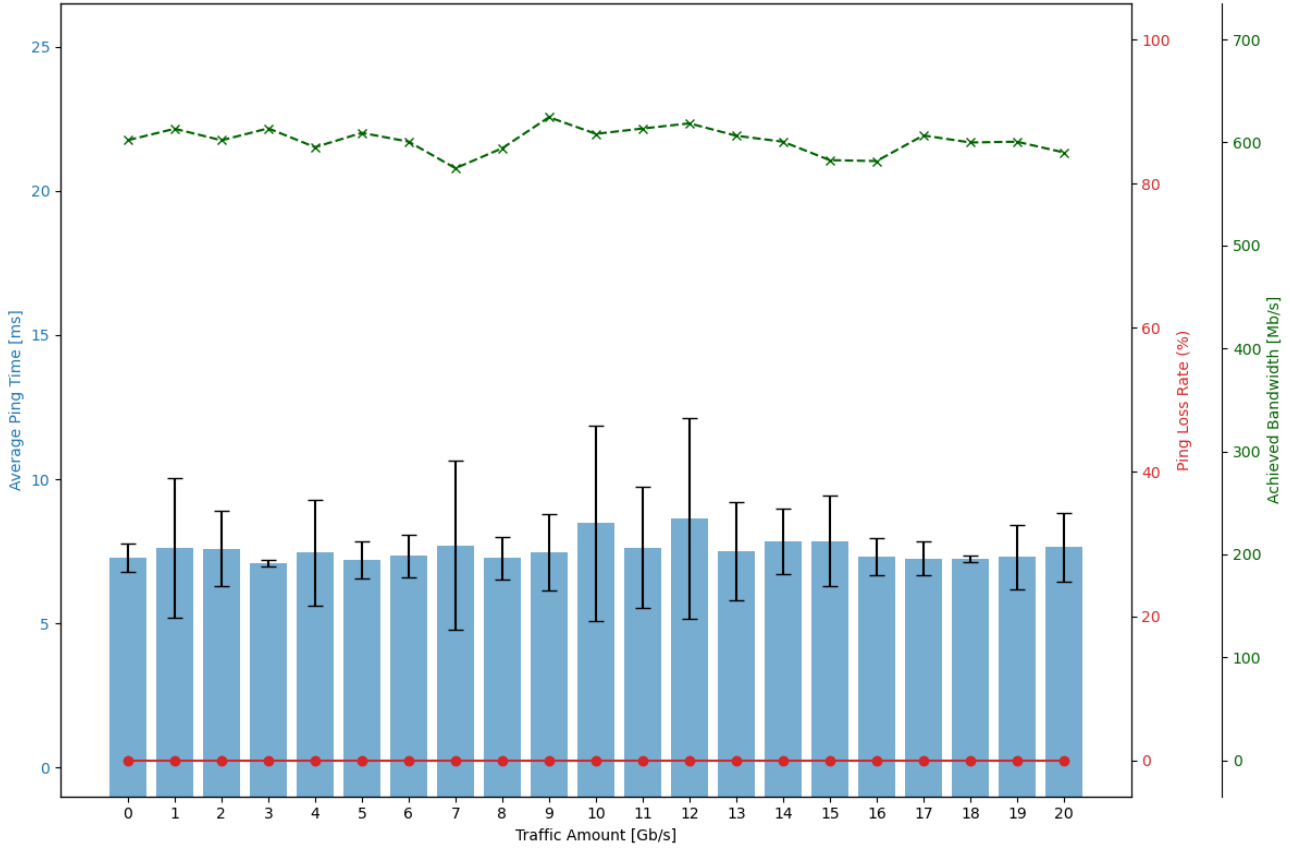
3) Volumetric Impact

Volumetric Denial of Service

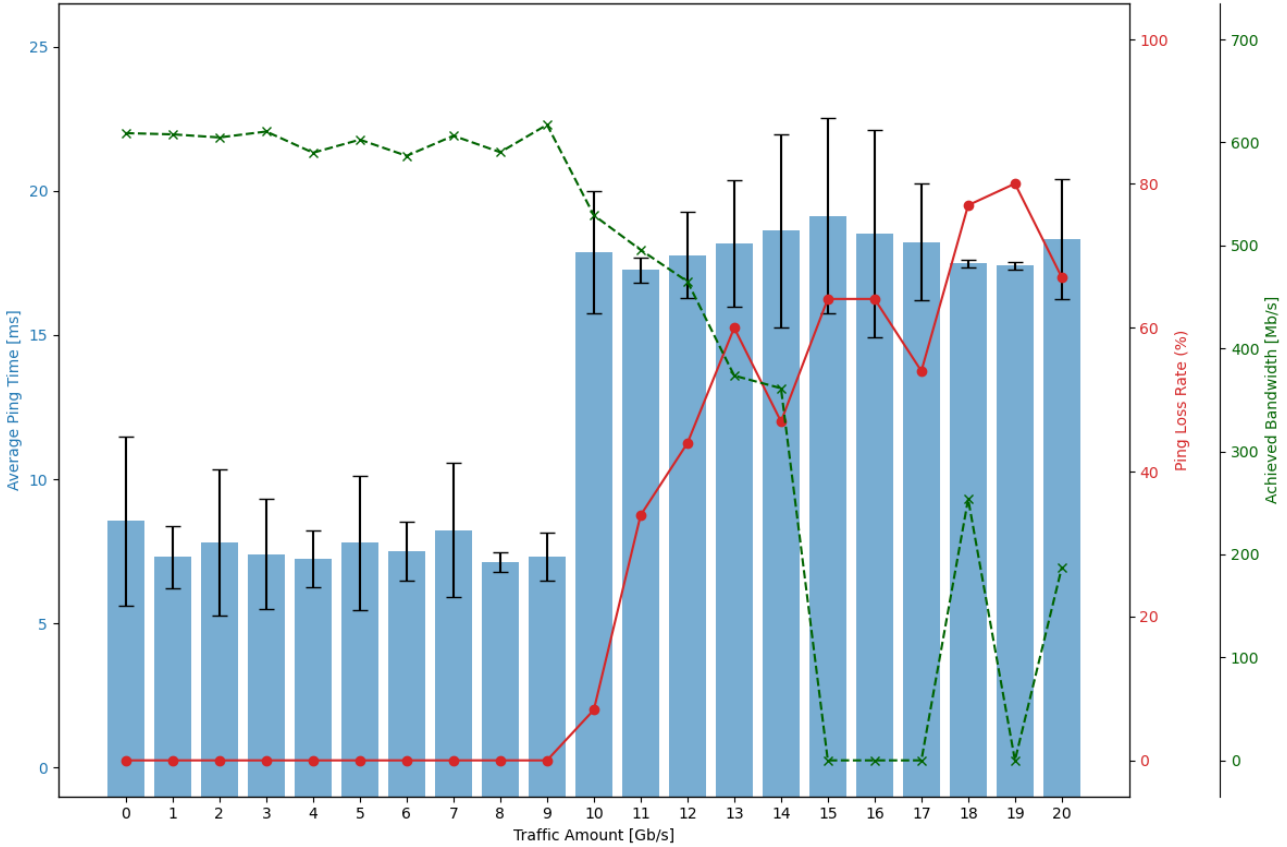
1) Traditional Internet
2) SCION



Impact of Volumetric Internet Traffic



Impact of Volumetric SCION Traffic



Conclusion

Security Analysis:

- Devices
- Protocol
- Impact

Anapaya fixed most of the shortcomings

Future work:

- Other Anapaya products
- Control plane
- Deployment

Conclusion

Security Analysis:

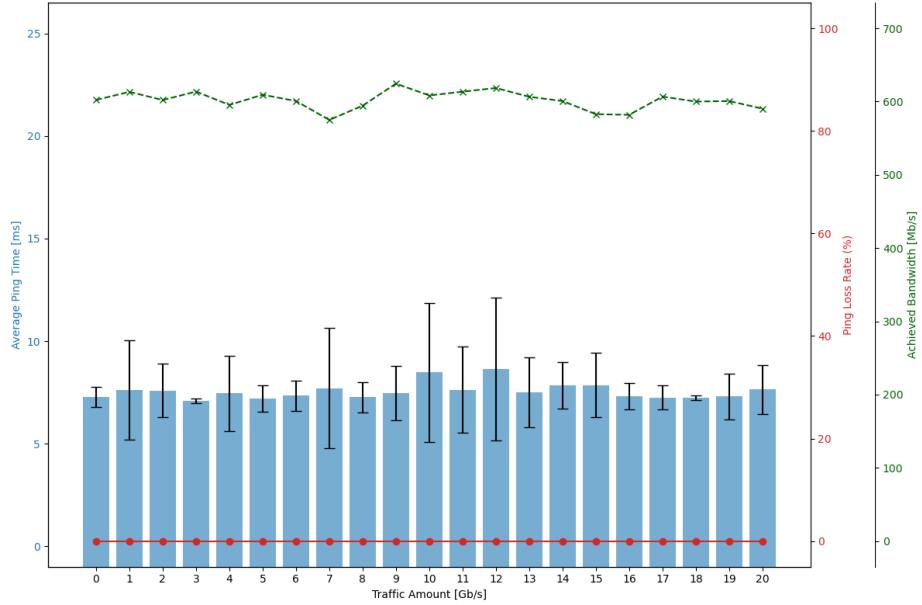
- Devices
- Protocol
- Impact

Anapaya fixed most of the shortcomings

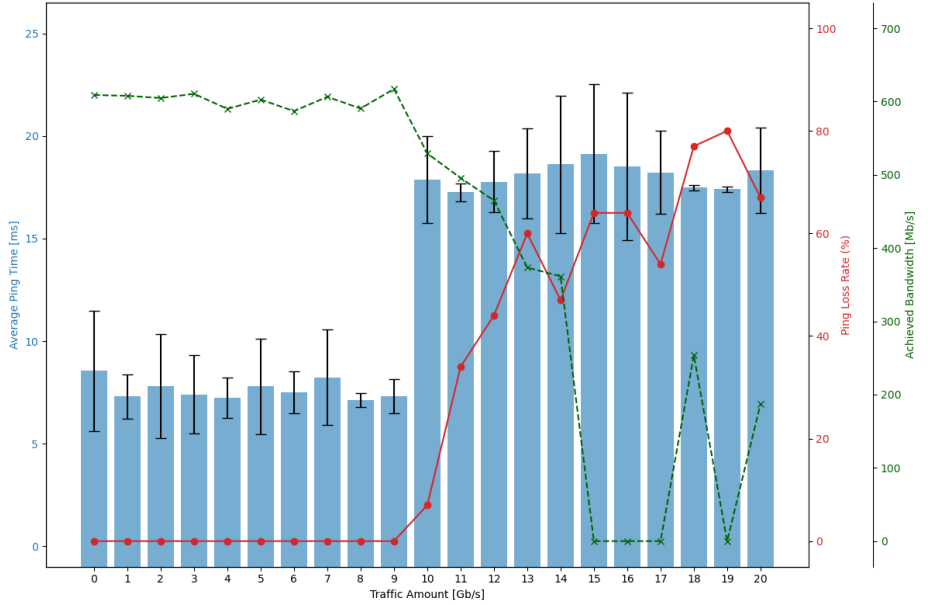
Future work:

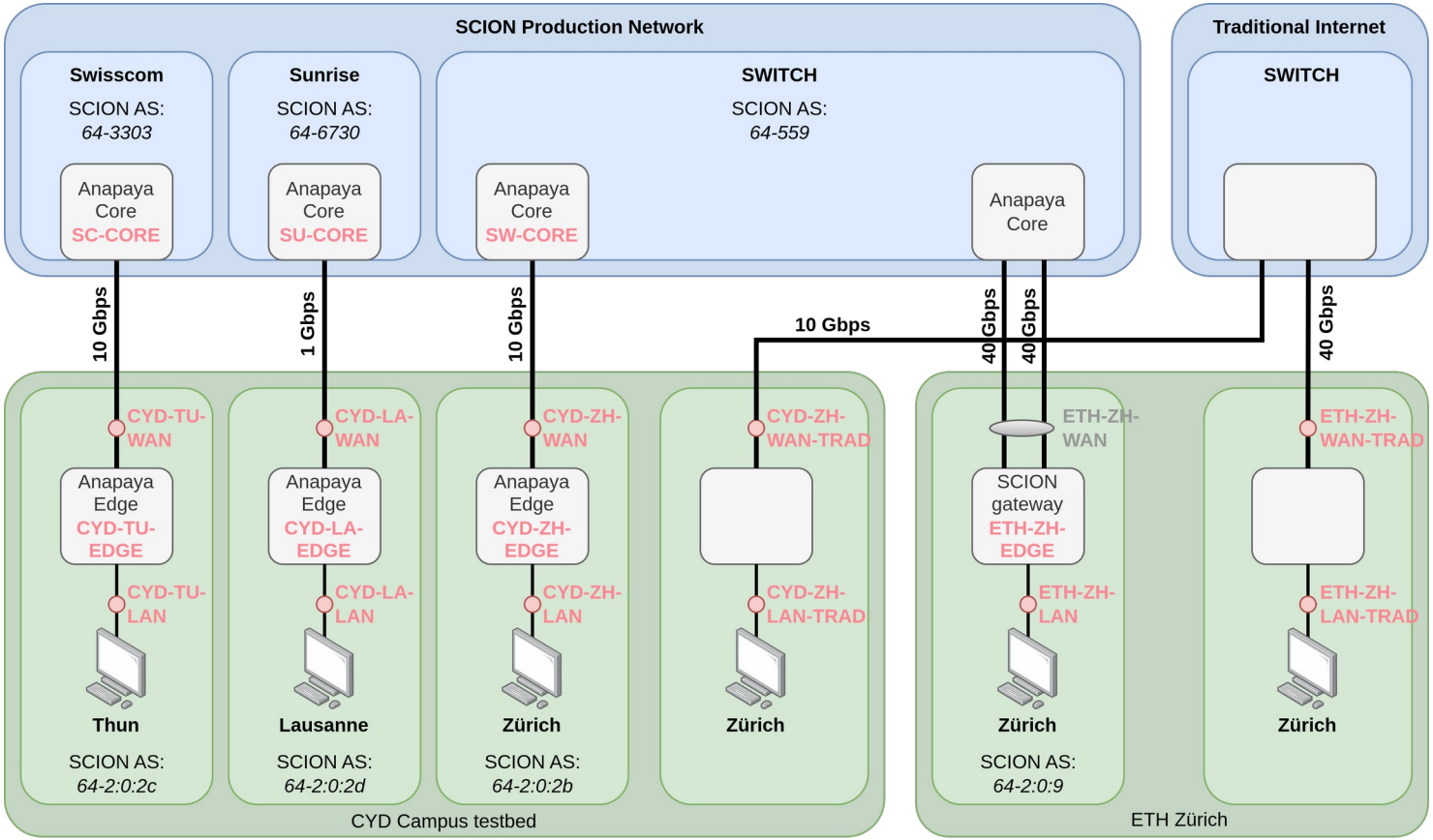
- Other Anapaya products
- Control plane
- Deployment

Internet

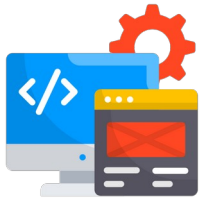


SCION




SCION Production Network
Traditional Internet
Swisscom
SCION AS:
64-3303
Sunrise
SCION AS:
64-6730
SWITCH
SCION AS:
64-559
SWITCH
Anapaya Core
SC-CORE
Anapaya Core
SU-CORE
Anapaya Core
SW-CORE
Anapaya Core
10 Gbps
1 Gbps
10 Gbps
10 Gbps
40 Gbps
40 Gbps
40 Gbps
CYD-TU-WAN
CYD-LA-WAN
CYD-ZH-WAN
CYD-ZH-WAN-TRAD
ETH-ZH-WAN
ETH-ZH-WAN-TRAD
Anapaya Edge
CYD-TU-EDGE
Anapaya Edge
CYD-LA-EDGE
Anapaya Edge
CYD-ZH-EDGE
SCION gateway
ETH-ZH-EDGE
CYD-TU-LAN
CYD-LA-LAN
CYD-ZH-LAN
CYD-ZH-LAN-TRAD
ETH-ZH-LAN
ETH-ZH-LAN-TRAD
Thun
SCION AS:
64-2:0:2c
Lausanne
SCION AS:
64-2:0:2d
Zürich
SCION AS:
64-2:0:2b
Zürich
Zürich
SCION AS:
64-2:0:9
Zürich
CYD Campus testbed
ETH Zürich

On Device Security



Outdated + vulnerable software (need local access to exploit)

Driver of Intel Ethernet Controller (Privilege escalation)

→ Potentially remotely exploitable

Distroless Debian (still contains vulnerable openssl version)

→ Command injection, use-after-free, double-free, DoS

Master Key Refreshment

Anapaya: "The Anapaya appliance is inline with the current SCION ecosystem where there is currently no automatic forwarding key rollover. Our appliance relies on the open source implementation for path creation and discovery. The issue is known and on the roadmap of the open source implementation https://github.com/scionproto/scion/issues/4348. However, we want to highlight that there is currently no practical attack on AES-CMAC to recover the key. Thus a successful attack is unlikely. Furthermore, in a scenario of a key compromise, an AS can manually roll over their key at will."

SCMP Authentication

Anapaya: "The Anapaya appliance is inline with the current SCION ecosystem where there is currently no support for SCMP authentication. The SCION community has not reached a final agreement on whether SCMP authentication should be supported, or in what manner.
We want to highlight that there are also mitigation strategies without SCMP Authentication. E.g., by validating the quoted packet in the SCMP message has been sent by the application."

Spoofing

Anapaya: "This is a hypothetical scenario with a server that is susceptible to reflection attacks by spawning path requests based on unconnected requests. None of the Anapaya authored applications behave this way, nor are we aware of any applications in the SCION ecosystem with this behavior. Well authored server applications should not do work in response to unconnected client requests."

Anapaya: "[...] the DRKey feature needs to be first accepted by the SCION community. As soon as it is, Anapaya will of course add support for it."

Egress filtering

> **Anapaya:** "We will introduce egress filtering in an upcoming release. However, we deem the risk of this affecting real applications as very low."

Path Header Modification (On-path)

Anapaya: "This attack is feasible in the base SCION protocol, hence there is no mitigation in the Anapaya appliance. As soon as the DRKey feature has been accepted by the SCION community and an implementation is available, it will be integrated in the Anapaya appliance."

SSH Rate Limiting

Anapaya: "The firewall rules on the Anapaya appliance can be adjusted to enable rate limiting. In a future release, we will change the default firewall configuration to also take rate limiting into account."

Ubuntu CIS Compliance Audit

Anapaya: "The Anapaya appliance is not intended as a general purpose OS, and thus does not have arbitrary user accounts. This reduces the risks of some of the violated compliance requirements considerably.
For this reason, we also do not deem a strict password policy critical, given there are no arbitrary users on the system."

Systemd Services

- ModemManager (3G/4G/5G)
- systemd-rfkill (for WiFi/Bluetooth)
- open-vm-tools
- ubuntu-advantage
- appliance-controller and appliance-installer

Anapaya: "We will assess how the surface of the systemd services can be reduced exposure where unneeded."

Device Software Vulnerabilities

Anapaya: "At the time of scanning for these vulnerabilities, Anapaya has already published multiple newer releases of the anapaya-system packages with patches for the aforementioned vulnerabilities. The packages have simply not been installed."

Docker Images

Anapaya: "The next release v0.37 will include docker images based on debian 12. The docker live restore feature is disabled on purpose as we implement our own watchdog functionality to bring back the services. Most docker based services did have CPU limits set, but lacked memory limits in older releases. As of v0.36, most services have both CPU and memory limits set. Furthermore, the operator can tune these limits via the appliance configuration to further harden their system. "

Authentication on Management System

Anapaya: "The Anapaya appliance has a default password configured when it is freshly installed from the base image. The user has to actively push a configuration to with basic auth not enabled for it to be disabled. We encourage CYD to enable basic auth in their configuration on their appliances to remedy the situation.
We will assess how we can make not enabling basic auth an even more conscious choice."

Rapid Reset – Caddy

> **Anapaya:** "The system package includes Caddy 2.7.5 as of version v2.9.0 which was released on 14.02.2024, and hence was already published at the time of the scan."