



# SWITCH Security WG



## SCALABILITY, CONTROL, AND ISOLATION ON NEXT-GENERATION NETWORKS

# Network Security Group, ETH Zürich

# What used to keep me up all night ...

## Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

By Russell Brandom | @russellbrandom | Apr 24, 2018, 1:40pm EDT

f t SHARE



Hijack of Amazon CloudFront service used to steal funds in hours unnoticed

Between 11am until 1:30pm, hackers hijacked the service, routing you to a malicious site controlled by an unknown actor.

## \$150K Stolen From MyEtherWallet Users in DNS Server Hijacking

BUY NOW

XCELTOKEN

XCEL  
A BLOCKCHAIN UTILITY TOKEN

\*Invest at your own risk, there is no guarantee for future success.

TOKEN SALE  
NOW OPEN

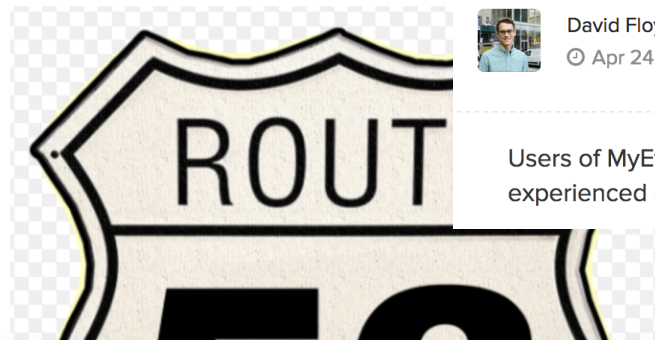
t 363 f g+ in r 7 e



David Floyd

© Apr 24, 2018 at 16:35 UTC | Updated Apr 24, 2018 at 16:37 UTC

NEWS



Users of MyEtherWallet, a web app for storing and sending ether and ethereum-based tokens, experienced an attack Tuesday that saw users of the service lose around \$152,000 worth of ether.

commercial cloud provider who count major websites such as Twitter.com as customers.

ETH zürich

SCION

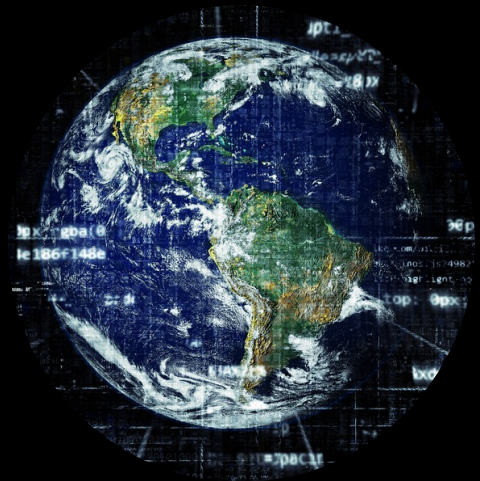


# What's now keeping me up all night?



# Internet Architecture in 21st Century

- Similar to real-world architecture, Internet Architectural trends change over time, typically not just driven by aesthetics, but also by applications
  - Early networks were circuit-switched for telephony
  - 50 years ago, packet switching started and formed the basis of today's Internet
- Recent architectural trends
  - High security and availability
  - Path-aware networking





# “Self-evident” Properties of a Next-Generation Internet Architecture

- Security (broadly defined)
  - High availability even under attack
- Path awareness, path selection
- Multi-path operation
- Formal verification
- Transparency
- Sovereignty

# 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!



# What is SCION?

- Secure inter-domain routing architecture, to replace BGP
- Open Internet platform, open-source
- Highly efficient: enables faster communication than in current Internet
- Highly secure: attacks are either impossible by design or significantly weakened
- Verifiably secure: Security proofs through formal methods
- **Next-generation Internet: path-aware multi-path communication**



# SCION Overview in One Slide



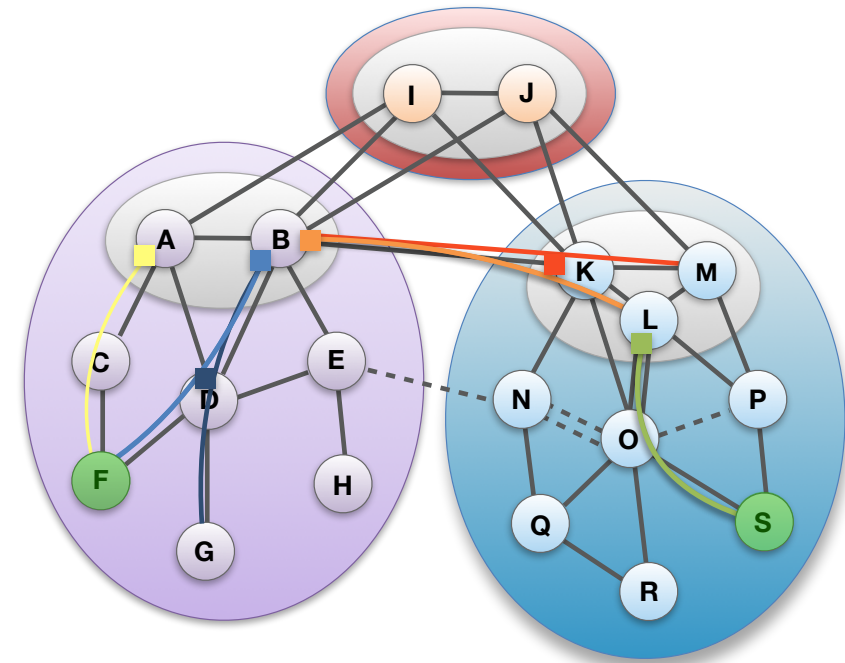
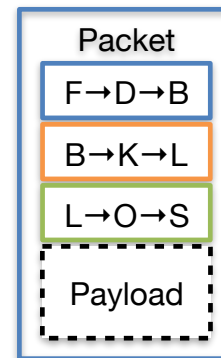
## Path-aware Network Architecture

### Control Plane - Routing

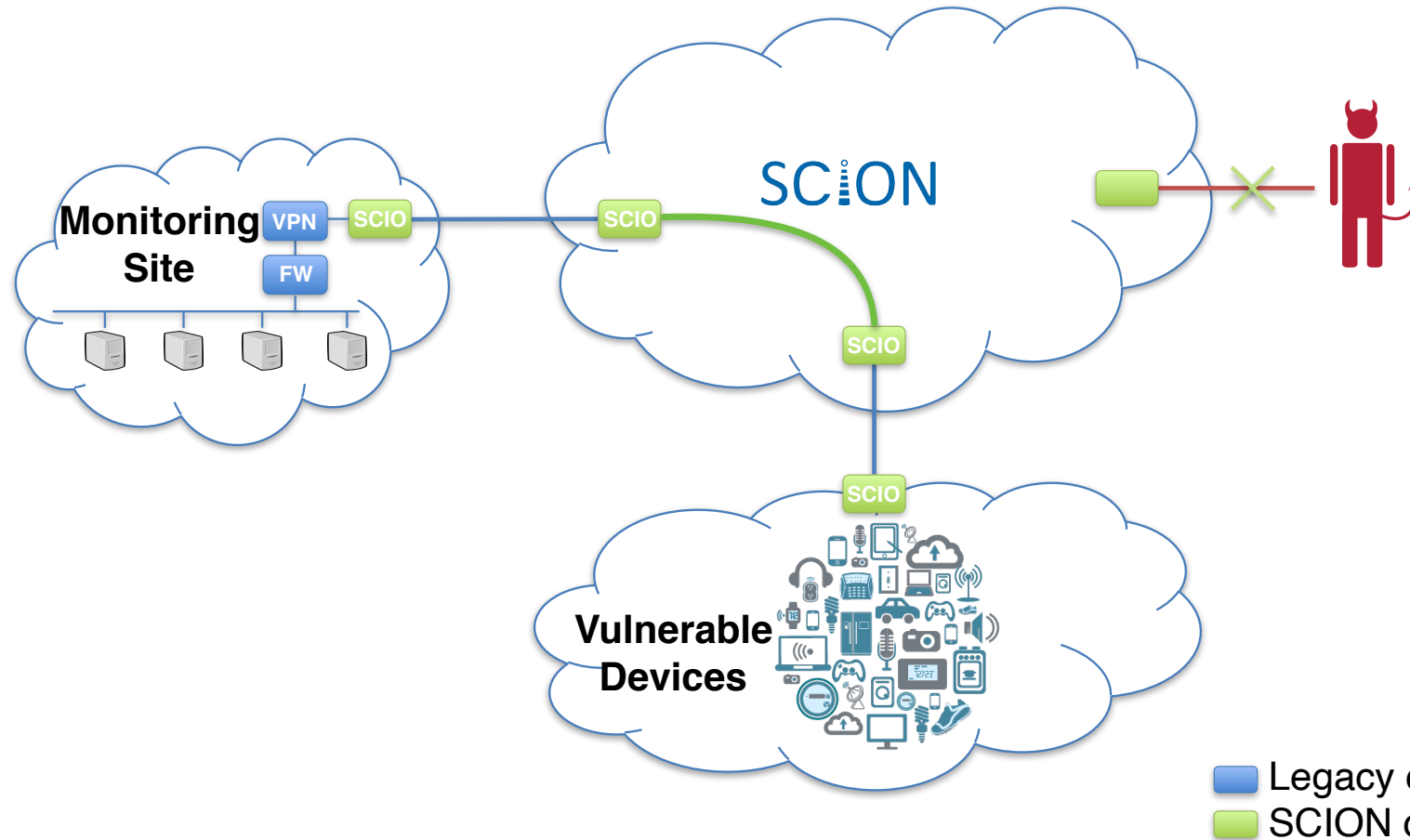
- ❖ **Constructs** and **Disseminates** Path Segments

### Data Plane - Packet forwarding

- ❖ **Combine** Path Segments to **Path**
- ❖ Packets contain Paths
- ❖ Routers forward packets based on Path
  - ▶ Simple routers, stateless operation

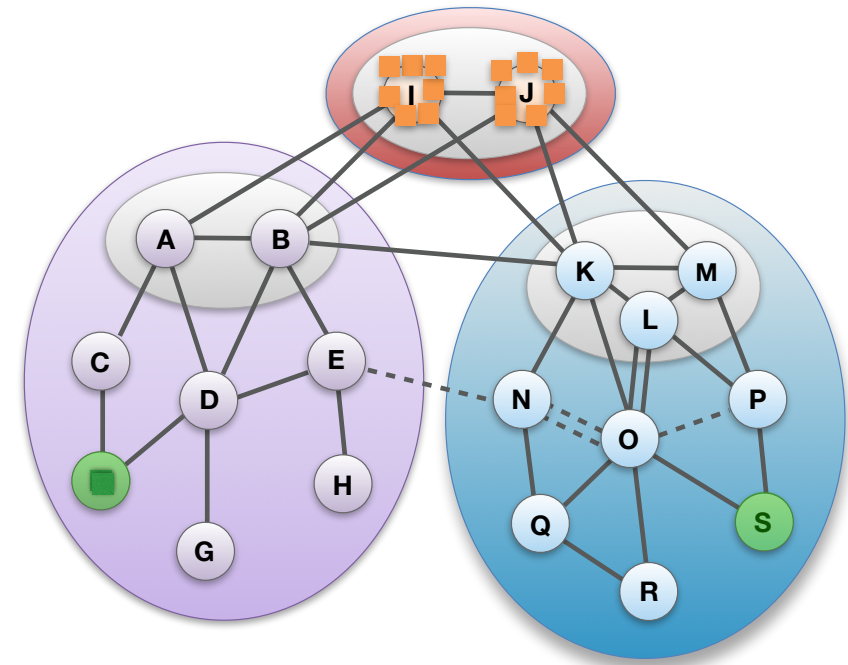


# Use Case: IoT Protection through Hidden Path



# Use Case: DDoS Defense

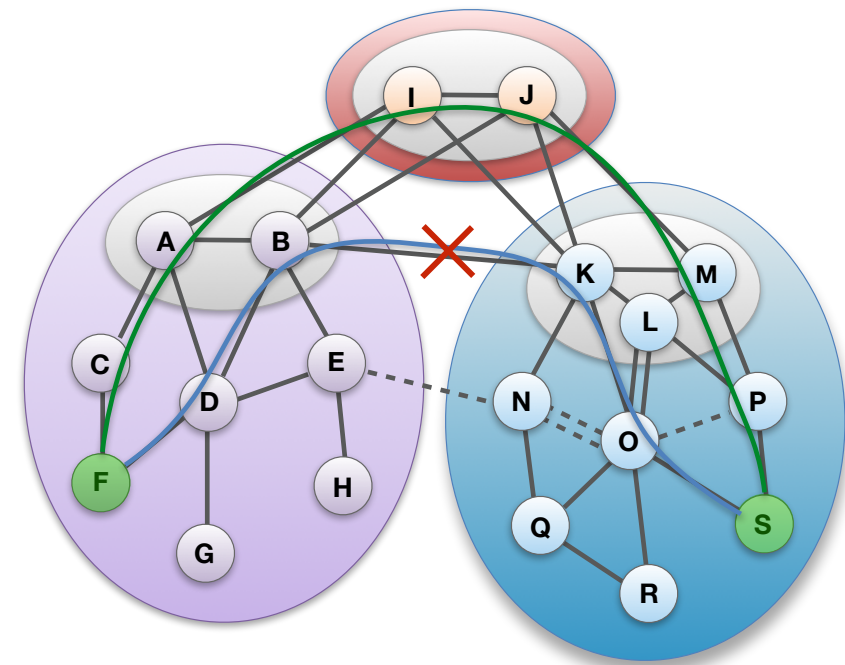
- Built-in mechanisms for DDoS defense
  - End-system high-speed source authentication
  - Multi-path communication enables circumventing congested areas
  - Hidden paths prevents flooding of last-mile links
  - COLIBRI global QoS system
- Property: guaranteed communication despite large-scale attacks



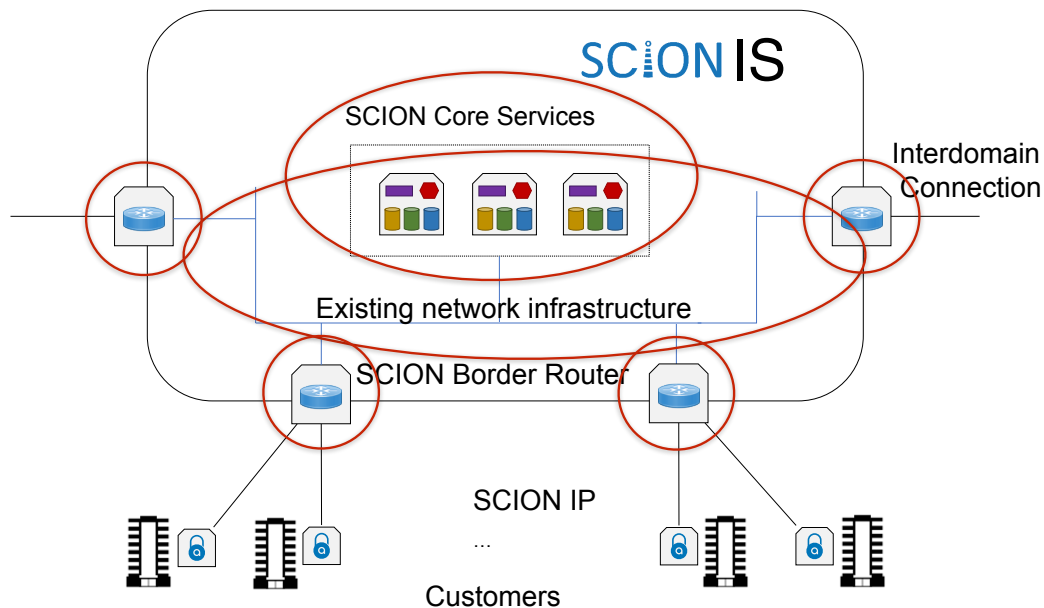


# Use Case: High-Speed Interdomain Failover

- Common failure scenarios in current Internet
  - Long-term failures (infrequent): large-scale failures require hours until BGP re-stabilizes
  - Intermediate-term failures (at each inter-domain router or link failure): 3-5 minutes until path is cleanly switched
  - Short-term failures (frequent): during BGP route change, routing loop during 5-10 seconds
- SCION: backup path is already set up and ready to be used when a link failure is observed
- Result: failover within milliseconds!

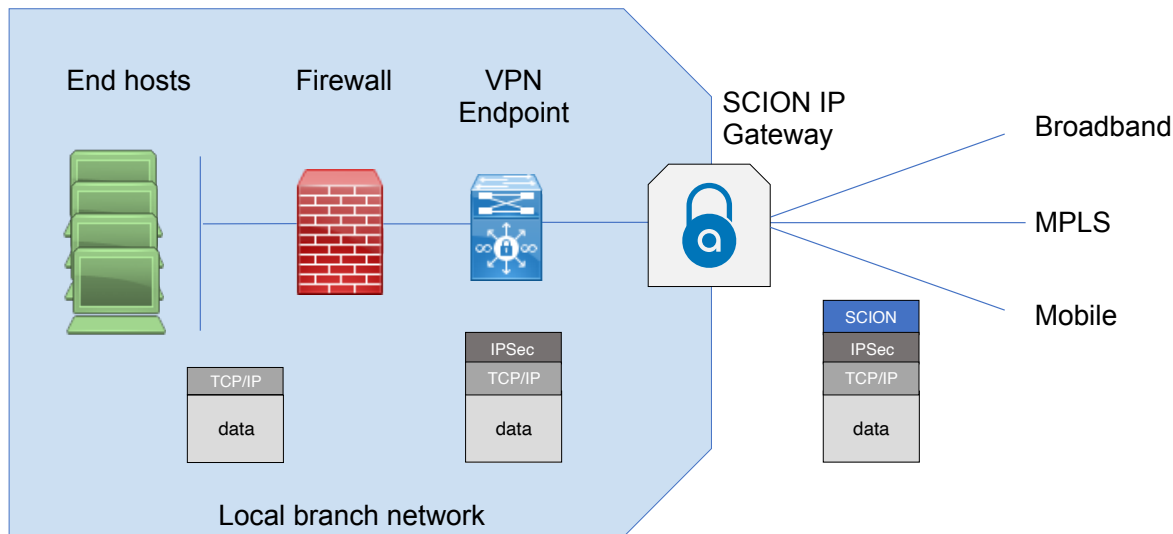


# How to Deploy SCION – Core Network



- Two components: SCION core services (control plane) and SCION border routers (data plane)
- SCION reuses existing intra-domain networking infrastructure—**no need to upgrade all networking hardware**

# How to Deploy SCION – End Domains



- SCION IP Gateway enables seamless integration of SCION capabilities in end-domain networks
- No upgrades of end hosts or applications needed
- SCION is transport-agnostic thus can work over many different underlying networks



## Recent Thrusts

- Main thrust: operationalize + drive deployment
- SCI-ED project
- SCIONLab
- Production network
- DRKey + control-plane PKI

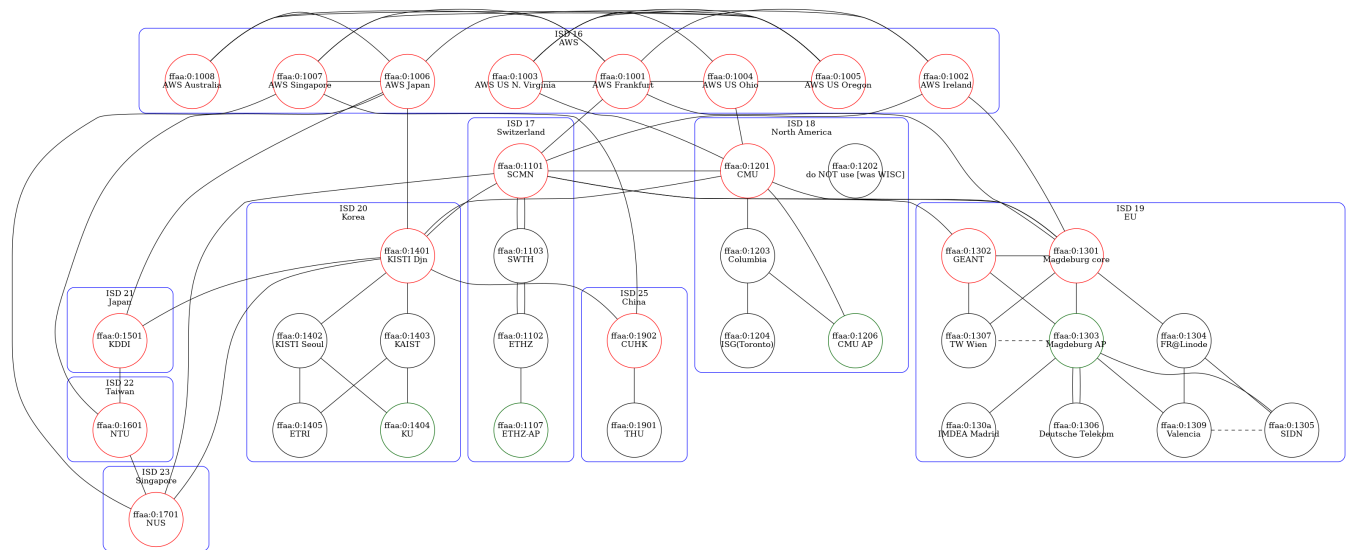
# SCI-ED: SCION for ETH Domain



- Goals
  - Large-scale real-world deployment: ETH, EPFL, PSI, CSCS, EMPA, EAWAG, WSL
  - Operationalize SCION in SWITCH network
  - Expand and demonstrate maturity of SCION on real-world use cases
- SCION use cases in the ETH Domain
  - High-performance data transmission
  - Secure communication of sensitive data
  - High availability for critical infrastructures
  - Platform for networking research


# SCIONLab

- Global SCION research testbed
- Open to everyone: create and connect your own AS within minutes
- ISPs: Swisscom, SWITCH, KDDI, GEANT, DFN
- Korea: GLORIAD, KISTI (KREONET), KU, KAIST, ETRI
- Deployed 35+ permanent ASes worldwide, 600+ user ASes





# SCION Production Network

- Led by Anapaya Systems  ANAPAYA
- Important point: BGP-free global communication
  - We need failure-independence from BGP protocol
- Discussions with domestic and international ISPs
  - Goal: First **inter-continental public secure** communication network
- Construction of SCION network backbone at select locations to bootstrap adoption
- Current deployment
  - ISPs: Swisscom, Sunrise, SWITCH, +others
  - Bank deployment: 4 major Swiss banks, some in production use
  - Swiss government has SCION in production use

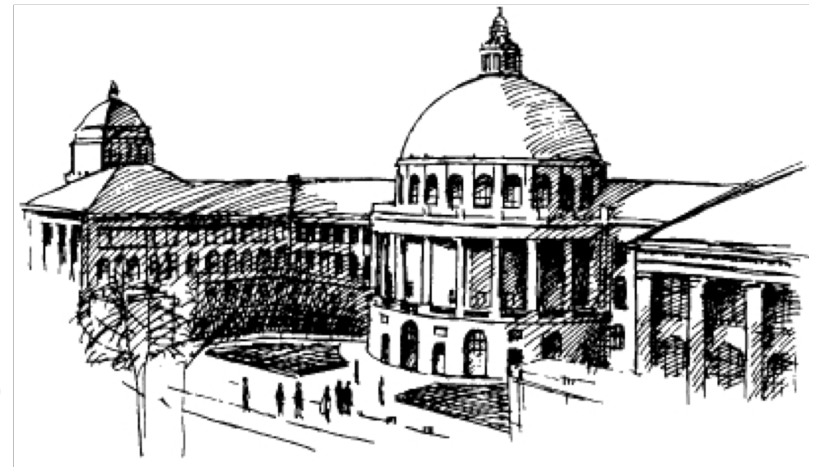


# LightningFilter: Traffic Filtering at 120 Gbps

Benjamin Rothenberger

*In collaboration with:*

Prof. Adrian Perrig, Juan García Pardo, Dominik Roos,  
Jonas Gude, Pascal Sprenger, Florian Jacky



# Project Goals

- High-speed packet processing requires nanosecond operations
  - Example: 64-byte packets @ 100Gbps: ~5ns processing time
- Nanosecond scale key establishment
- Nanosecond scale packet authentication
- Trivia: how “long” is a nanosecond?
  - Answer: light travels about 30cm in 1ns

# High-Speed Packet Processing

- Current high-speed Internet links: 400Gbit/s (Gbps)
- Arrival rate for 64-byte packets: one packet every 1.3 ns
- High-speed asymmetric signature implementation:  
Ed25519 SUPERCOP REF10:  $\sim 100\mu\text{s}$  per signature
- AES-NI instruction only requires 30 cycles:  $\sim 10\text{ns}$
- Memory lookup from DRAM requires  $\sim 200$  cycles:  $\sim 70\text{ns}$
- Only symmetric crypto enables high-speed processing through parallel processing and pipelining

# 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
- DRKey
  - High-speed key establishment (within 20 ns), enabling powerful DDoS defense



# 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  $SV_X$ 
    - $K_{X \rightarrow Y} = \text{PRF}_{SV_X}(\text{"Y"})$
    - Intel AES-NI instructions enable PRF computation within 30 cycles, or 70 cycles for CMAC
- Key computation is 3-5 times faster than DRAM key lookup!
- Any entity in AS X knowing secret value  $SV_X$  can derive  $K_{X \rightarrow *}$

# DRKey Performance



```
./fast-signing-eval
```

```
Authentication / Signing times averaged over 100000 runs:
```

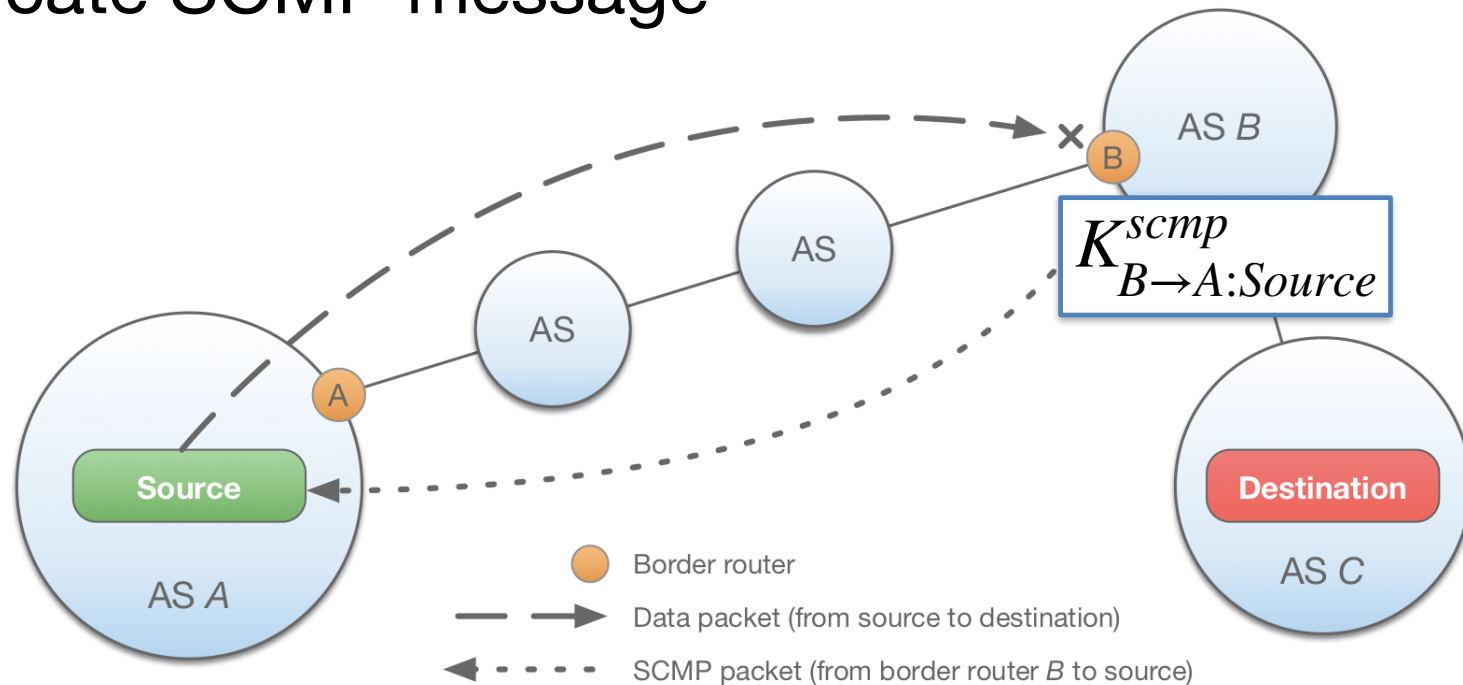
```
DRKey: 84.8 ns
```

```
Ed25519: 125.5 µs
```

Factor:  
~ 1450x

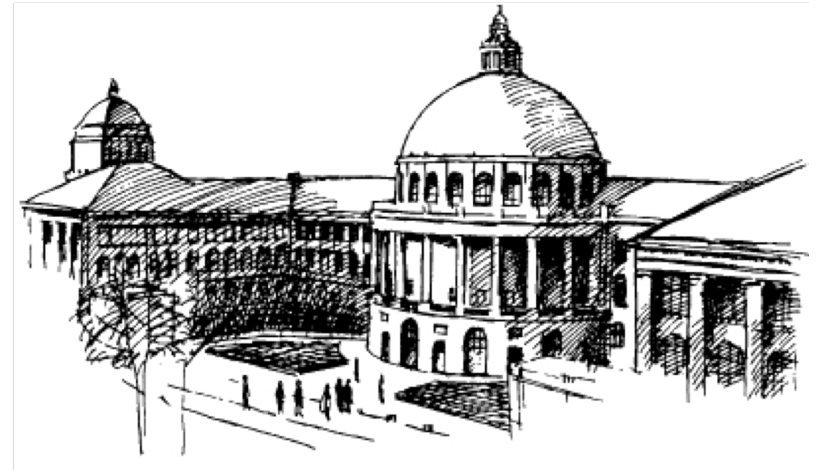
# DRKey Use Case: SCMP Authentication

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

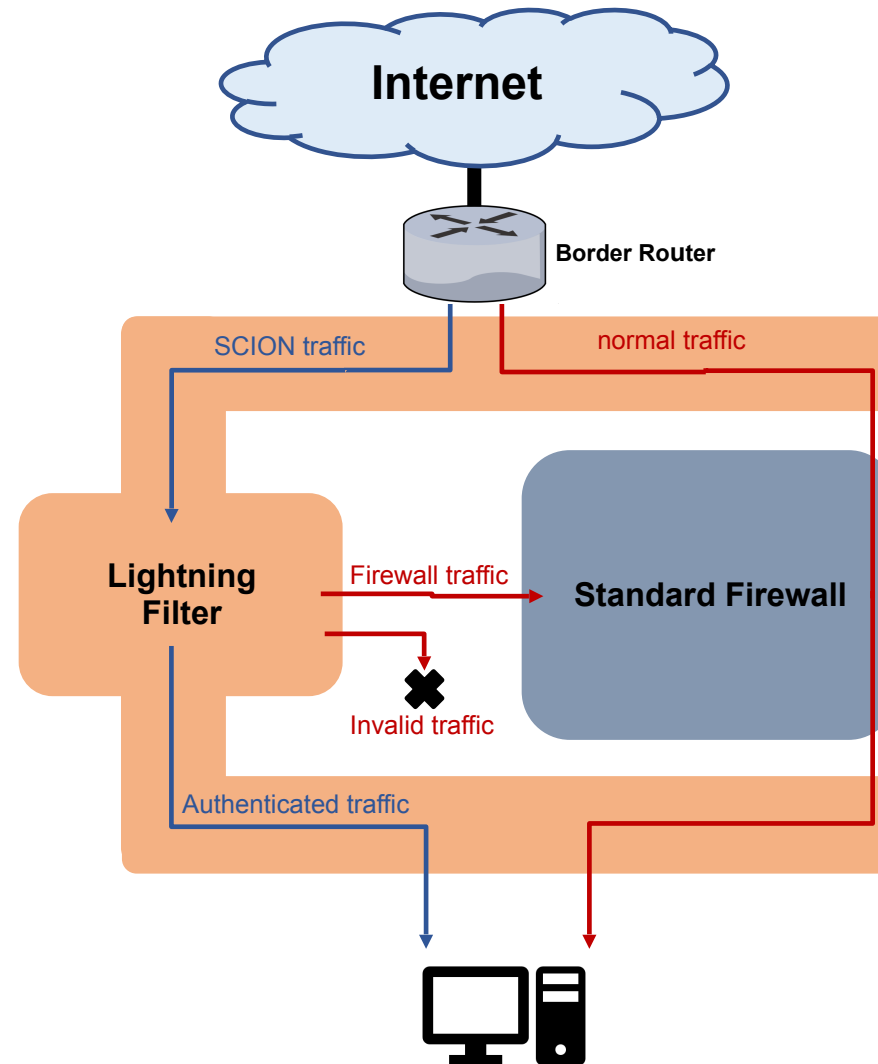


# Lightning Filter

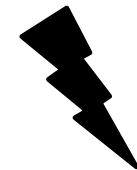
Traffic Filtering at 100 Gbps



# Overview

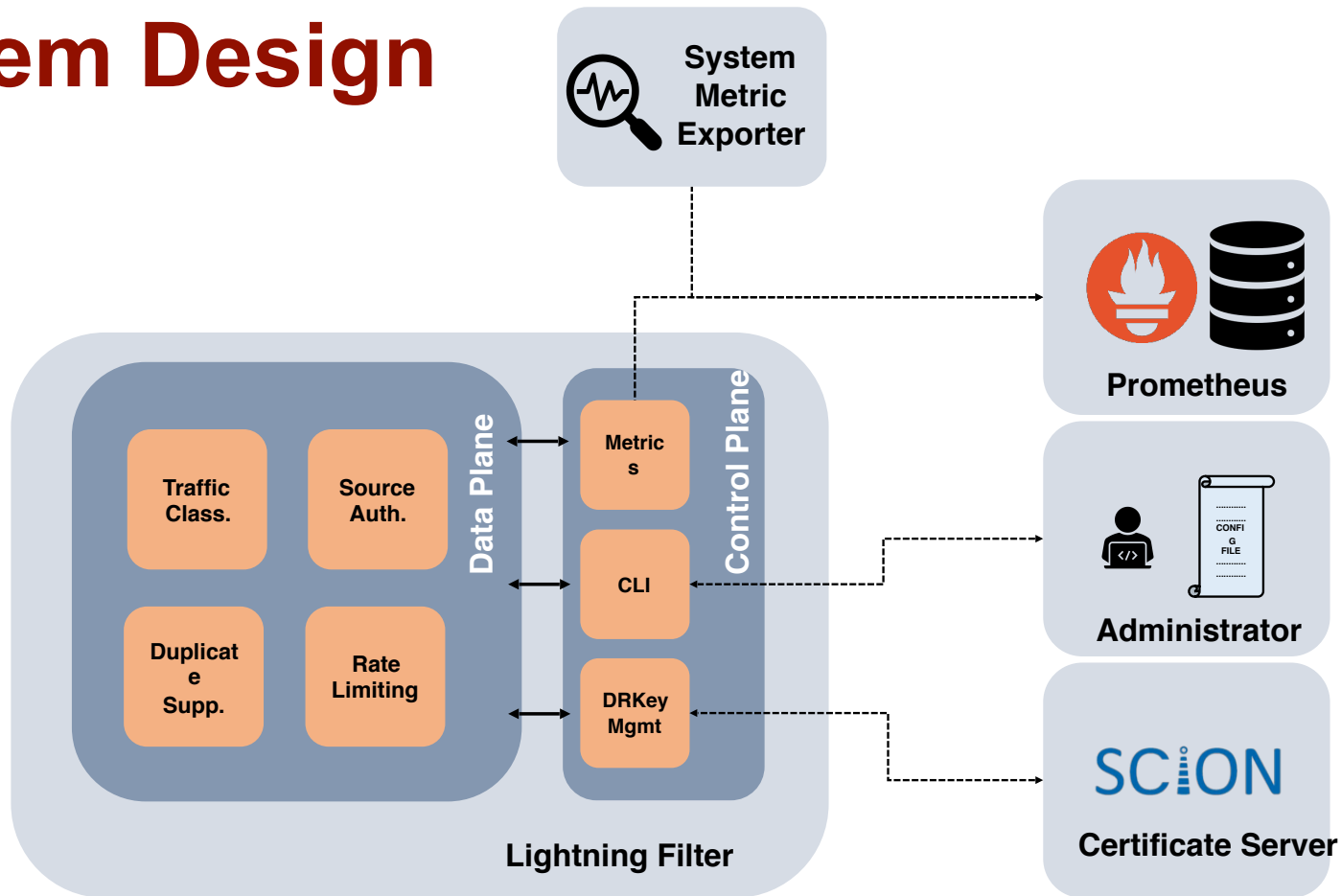


\$\$\$





# System Design

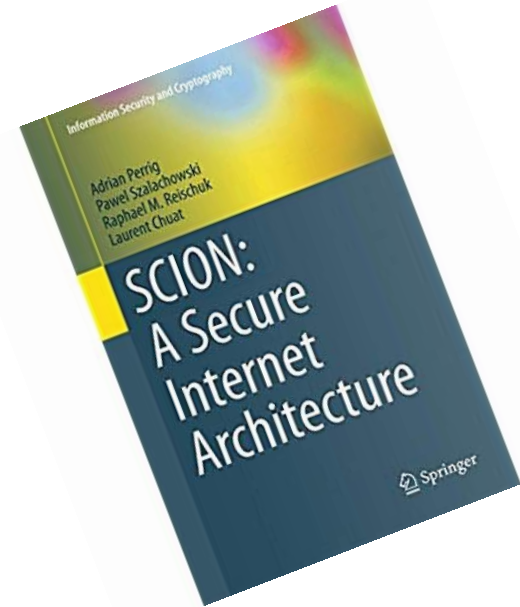


# Demo Outline

1. Attack scenario
  - Attacker located anywhere in Internet → Source authentication
2. Bandwidth capacity
  - 120 Gbps traffic volume
3. Filtering based on source authentication
  - Alternate between filtering and bypass every 30s
4. Duplicate suppression
  - 80 Gbps duplicates traffic, 40 Gbps legitimate traffic

# 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



# Summary

- Future Internet enables application-specific optimizations to provide **enhanced efficiency**
- **Path-aware networking + multi-path networks** are a promising direction to realize the future Internet vision
- **High security and availability** provide further benefits
- Join the effort, try out SCION today
  - SCIONLab research testbed
  - Production network

# Thank you for your attention!



SCION