SCION

SCALABILITY, CONTROL, AND ISOLATION
ON NEXT-GENERATION NETWORKS

A Secure Internet Architecture

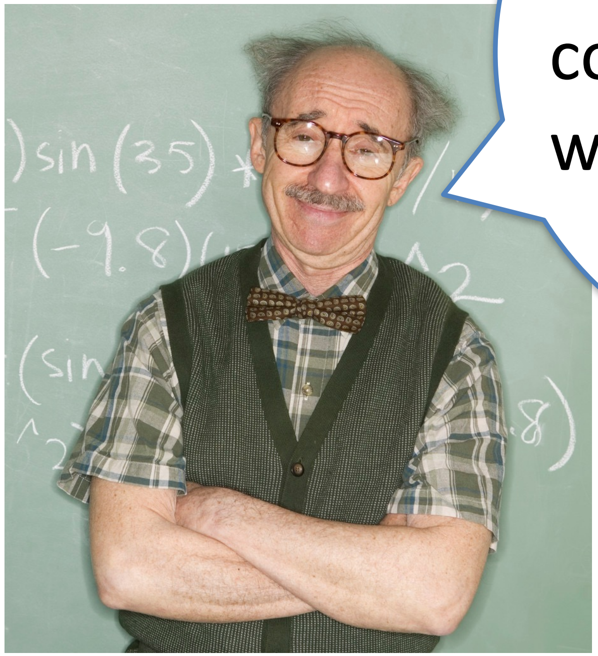
Adrian Perrig

Network Security Group, ETH Zürich
Anapaya Systems

My Early Days as a PhD Student

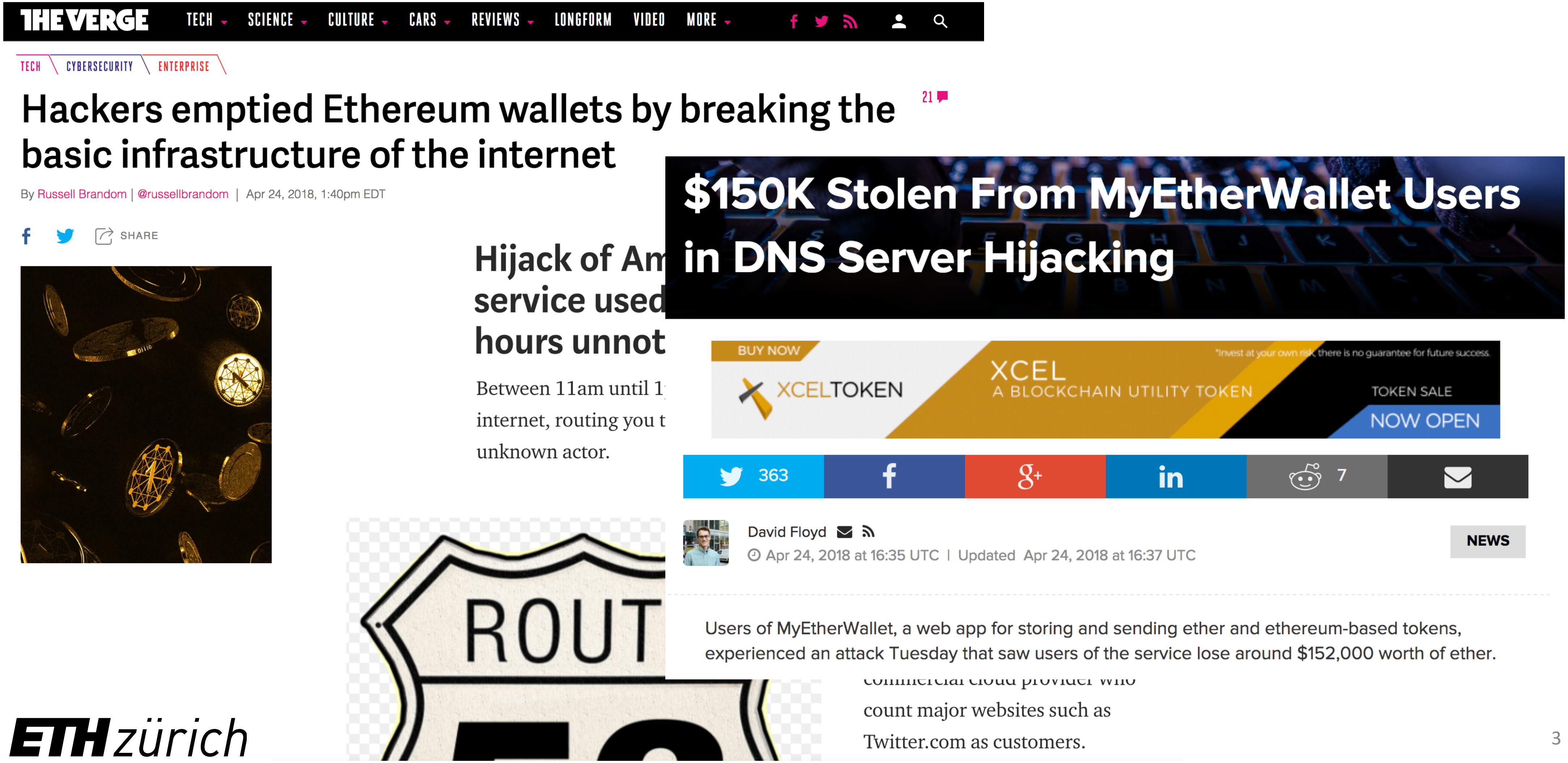
- NDSS Conference in San Diego, February 1998

I have an idea how to fix BGP prefix hijacking!



Don’t worry, kid. We have it under control. The problem will be fixed within 3 years.

Internet Security Issues



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

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

Hijack of Am
service used
hours unnot

Between 11am until 1
internet, routing you t
unknown actor.

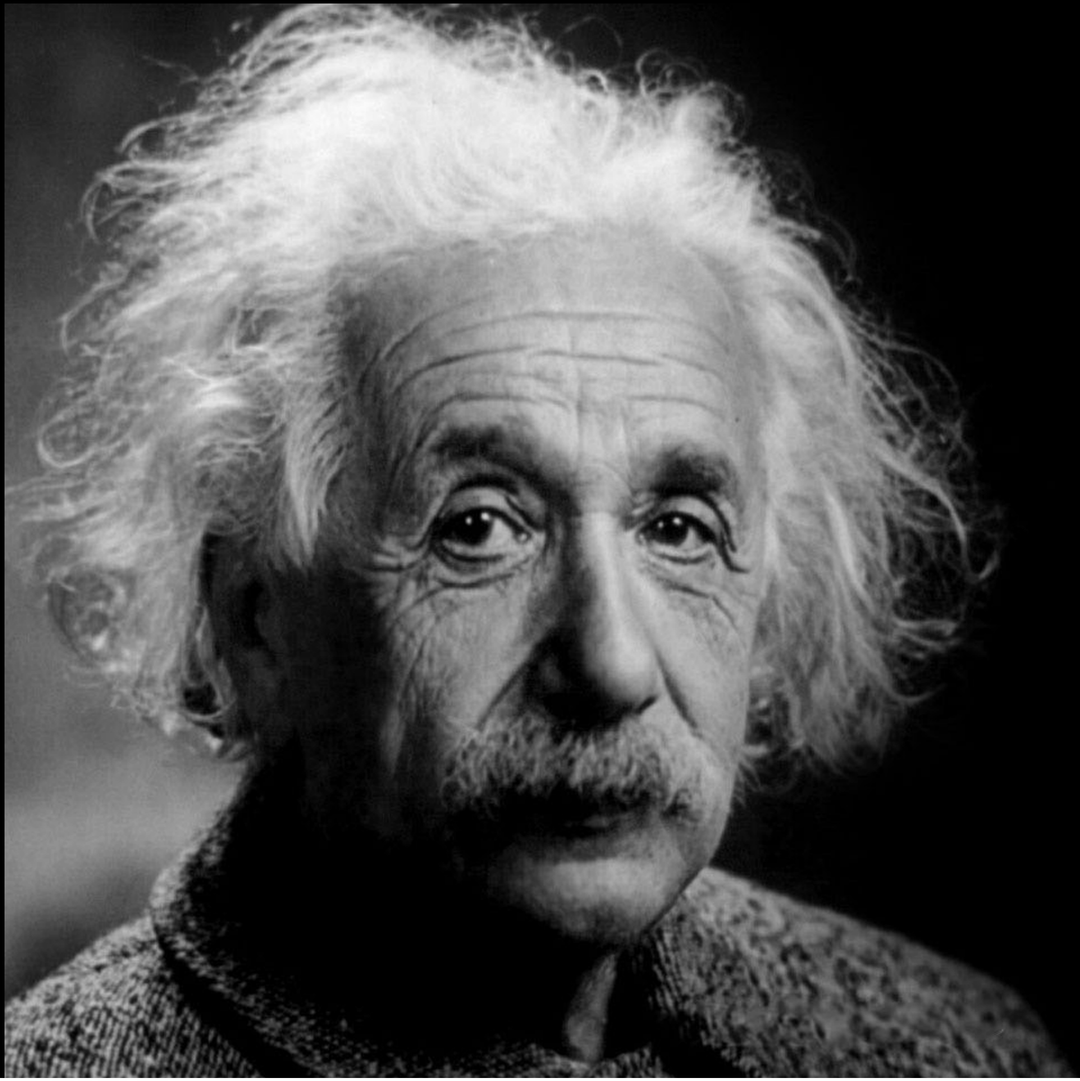
commercial cloud provider who
count major websites such as
Twitter.com as customers.

$150K Stolen From MyEtherWallet Users in DNS Server Hijacking

David Floyd

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

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.

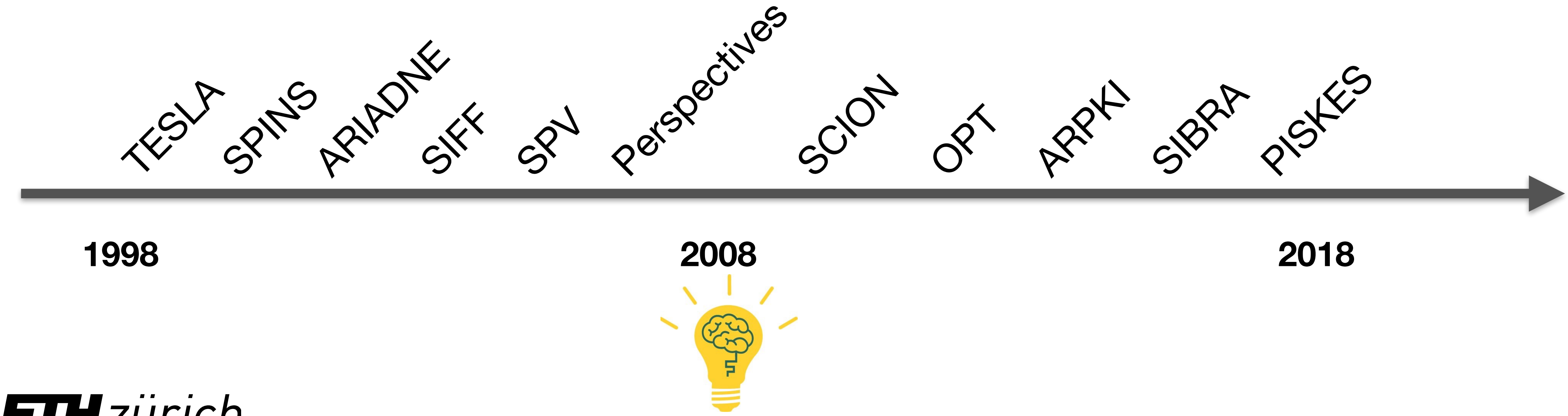


We cannot solve our problems with the same thinking we used when we created them.

Albert Einstein

Research Timeline

- First 10 years: attempt to fix current Internet
- Past 10 years: secure Internet by Design



TESLA SPINS ARIADNE SIFF SPV Perspectives SCION OPT ARPKI SIBRA PISKES

1998 2008 2018

New Internet Wish List

- Global communication guarantees
- High assurance for protocols and code
- High assurance for network paths
- Network sovereignty
- Differentiated trust

Global Communication Guarantees

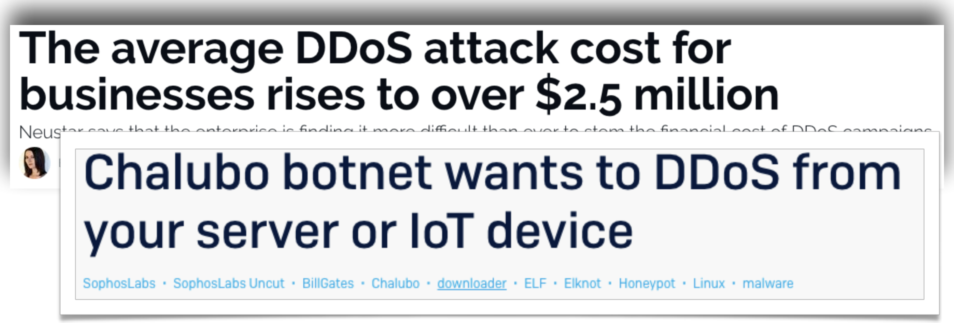
Current Status

- ✗ DDoS or routing attacks prevent communication
- ✗ No communication guarantees on today's Internet

New Approach

- ✦ Secure by Design
  - ▷ Most attacks are prevented by construction
  - ▷ E.g., built-in defense capabilities for DDoS and routing attacks

Consequences



The average DDoS attack cost for businesses rises to over $2.5 million

Neustar says that the enterprise is finding it more difficult than ever to stem the financial cost of DDoS campaigns

Chalubo botnet wants to DDoS from your server or IoT device

SophosLabs · SophosLabs Uncut · BillGates · Chalubo · downloader · ELF · Elknot · Honeypot · Linux · malware

Result

- ✓ Prevention of routing attacks
- ✓ Guaranteed communication despite DDoS attacks

ETH zürich

High Assurance for Protocols and Code

Current Status

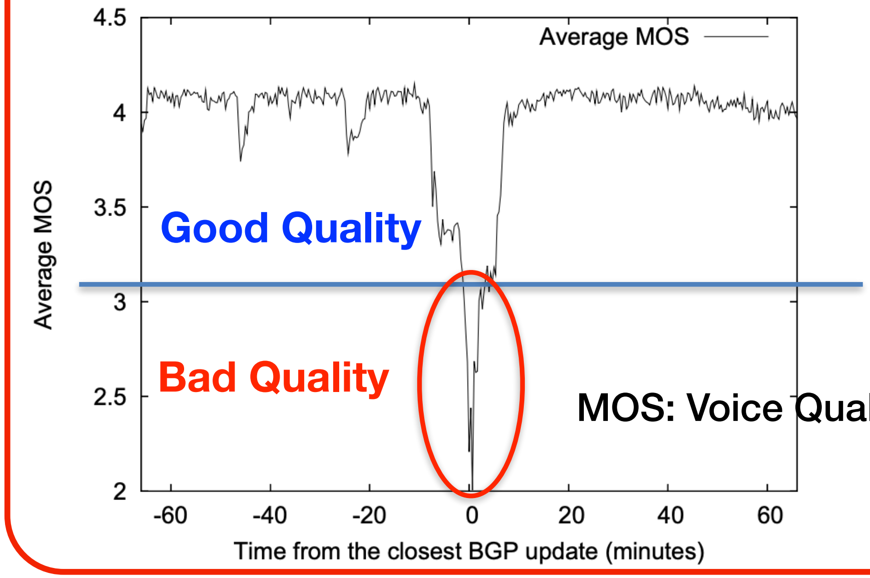
- ✘ BGP is slow to converge to stable state
- ✘ Complex router implementation

New Approach

- ✦ Provide convergence-free routing process
- ✦ Simple and stateless routers

Consequences

- E.g., Cannot assure VoIP quality [1]



Good Quality

Bad Quality

MOS: Voice Quality Index

Result

- ✓ Formally verified protocols and implementation
- ✓ Obtain high assurance for communication

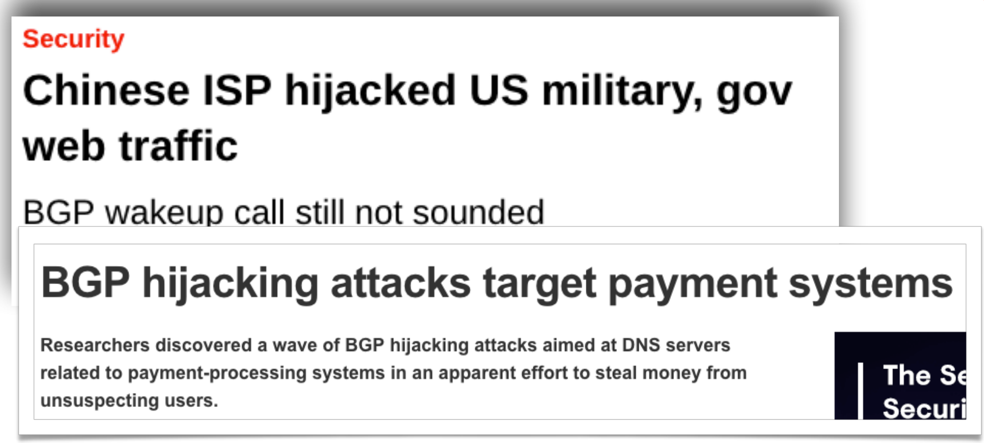
[1] N. Kushman et al., *Can you hear me now? It must be BGP, CCR 2007*

High Assurance for Network Paths

Current Status

- ✗ No assurance on and control over packets path across the Internet
- ✗ Frequent prefix hijacking

Consequences



Security

Chinese ISP hijacked US military, gov web traffic

BGP wakeup call still not sounded

BGP hijacking attacks target payment systems

Researchers discovered a wave of BGP hijacking attacks aimed at DNS servers related to payment-processing systems in an apparent effort to steal money from unsuspecting users.

New Approach

- ✦ Allow both sender and receiver to control the communication path
- ✦ Provide assurance on packet’s path by the network

Result

- ✓ Geo-Fencing
  - ▷ Ensure that packet stays within certain area
- ✓ Resilience against hijacking attacks

ETH zürich

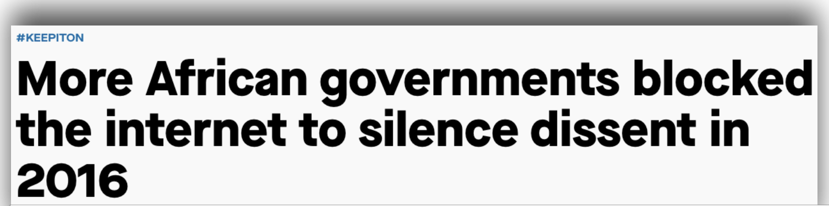
Network Sovereignty

Current Status

- ✗ Single root of trust for many (secure) Internet protocols
- ✗ External entities can control Internet in a region

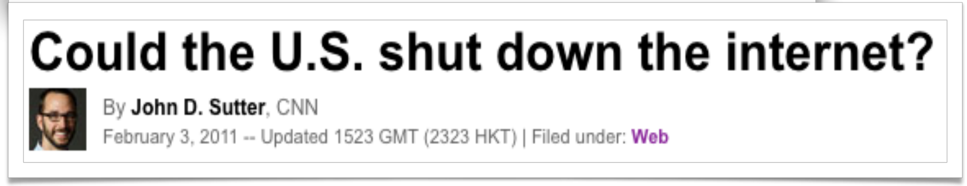
Consequences

- Internet Kill Switch



#KEEPITON

More African governments blocked the internet to silence dissent in 2016



Could the U.S. shut down the internet?

By **John D. Sutter**, CNN

February 3, 2011 -- Updated 1523 GMT (2323 HKT) | Filed under: Web

New Approach

- ✦ Isolation domains define sovereign Internet region
- ✦ Provide assurance on packet's path by the network

Result

- ✓ Global communication still possible
- ✓ Isolation domain defines who governs which region of the Internet

Differentiated Trust

Current Status

✘ Limited trust models

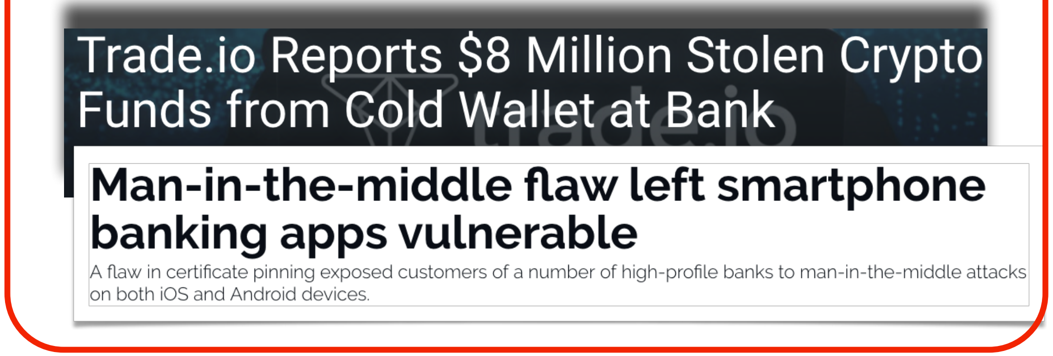
- Monopoly Model: Single trusted entity
- Oligarchy Model: Large # of trusted entities

New Approach

✦ Enable trust ranking by individuals and corporations

Consequences

- Man-in-the-Middle Attack



Trade.io Reports $8 Million Stolen Crypto Funds from Cold Wallet at Bank

Man-in-the-middle flaw left smartphone banking apps vulnerable

A flaw in certificate pinning exposed customers of a number of high-profile banks to man-in-the-middle attacks on both iOS and Android devices.

Result

✓ All entities can be authenticated

✓ Low trust entities cannot impersonate higher trust entities

SCION: Next-generation Internet Architecture

CAUTION: HIGHLY ADDICTIVE

SCION Architecture Design Goals

- High availability, even for networks with malicious parties
  - Communication guarantee if adversary-free path exists
- Secure entity authentication that scales to global heterogeneous (dis)trusted environment
- Flexible trust: enable selection of trust roots
- Transparent operation: clear what is happening to packets and whom needs to be relied upon for operation
- Balanced control among ISPs, senders, and receivers
- Scalability, efficiency

SCION Overview in One Slide

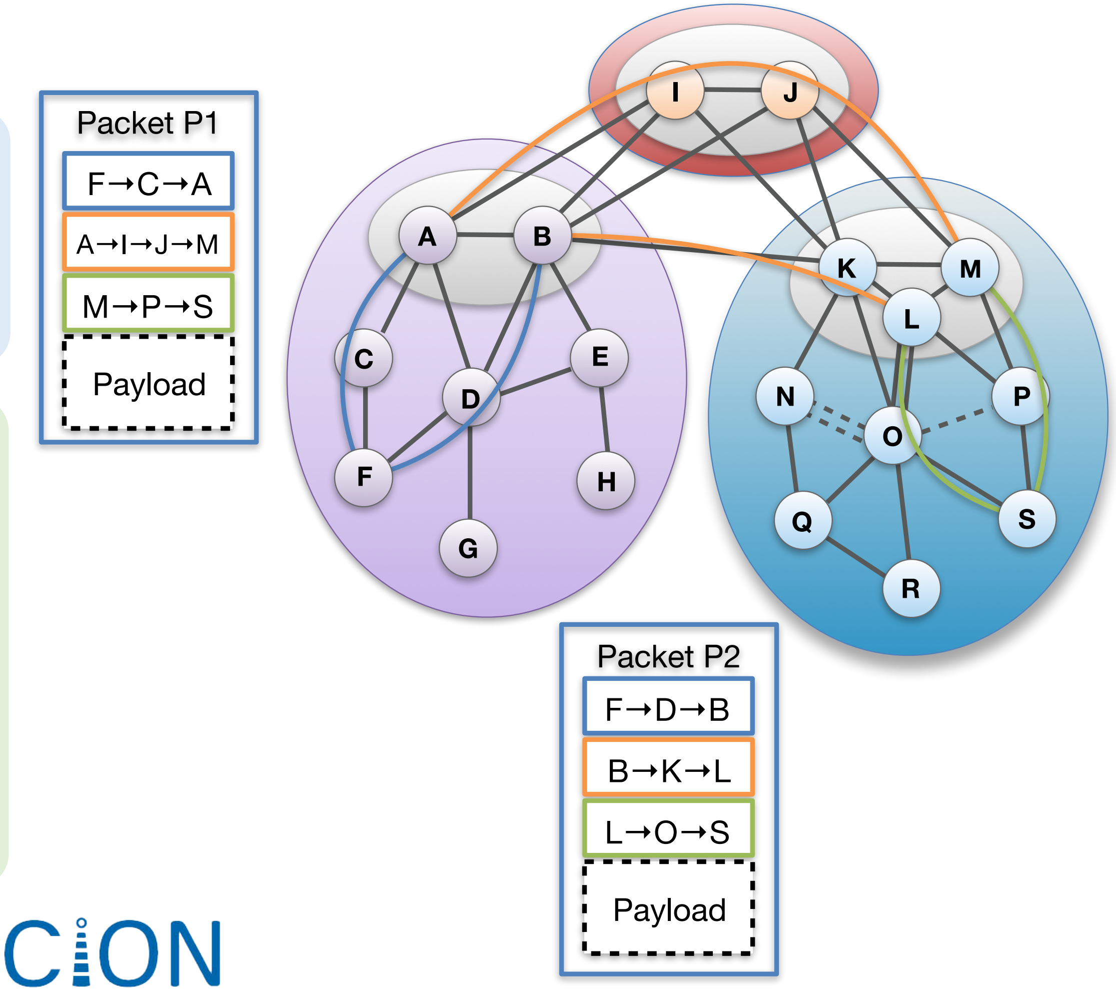
Path-based Network Architecture

Control Plane - Routing

- ❖ Constructs and Disseminates Path Segments

Data Plane - Packet forwarding

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



Packet P1

F→C→A

A→I→J→M

M→P→S

Payload

Packet P2

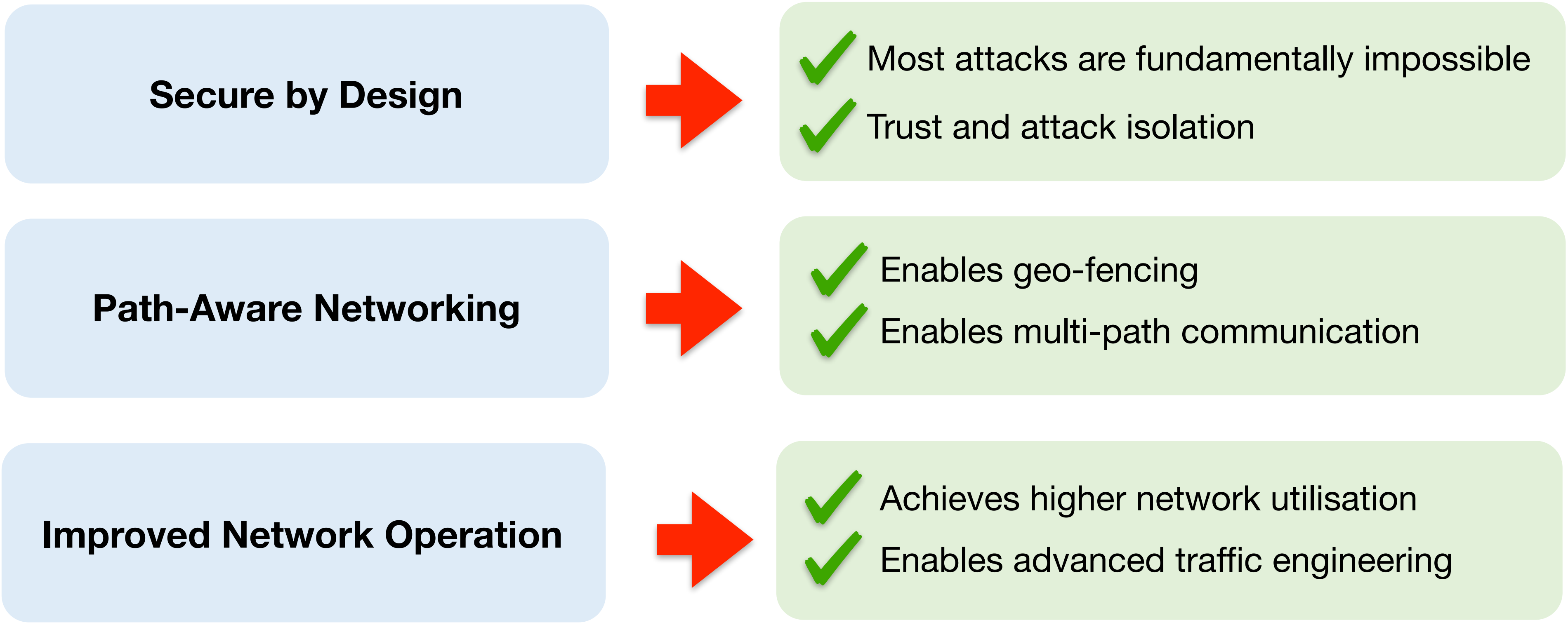
F→D→B

B→K→L

L→O→S

Payload

SCION: Fulfilling the Wish List



Secure by Design

- ✓ Most attacks are fundamentally impossible
- ✓ Trust and attack isolation

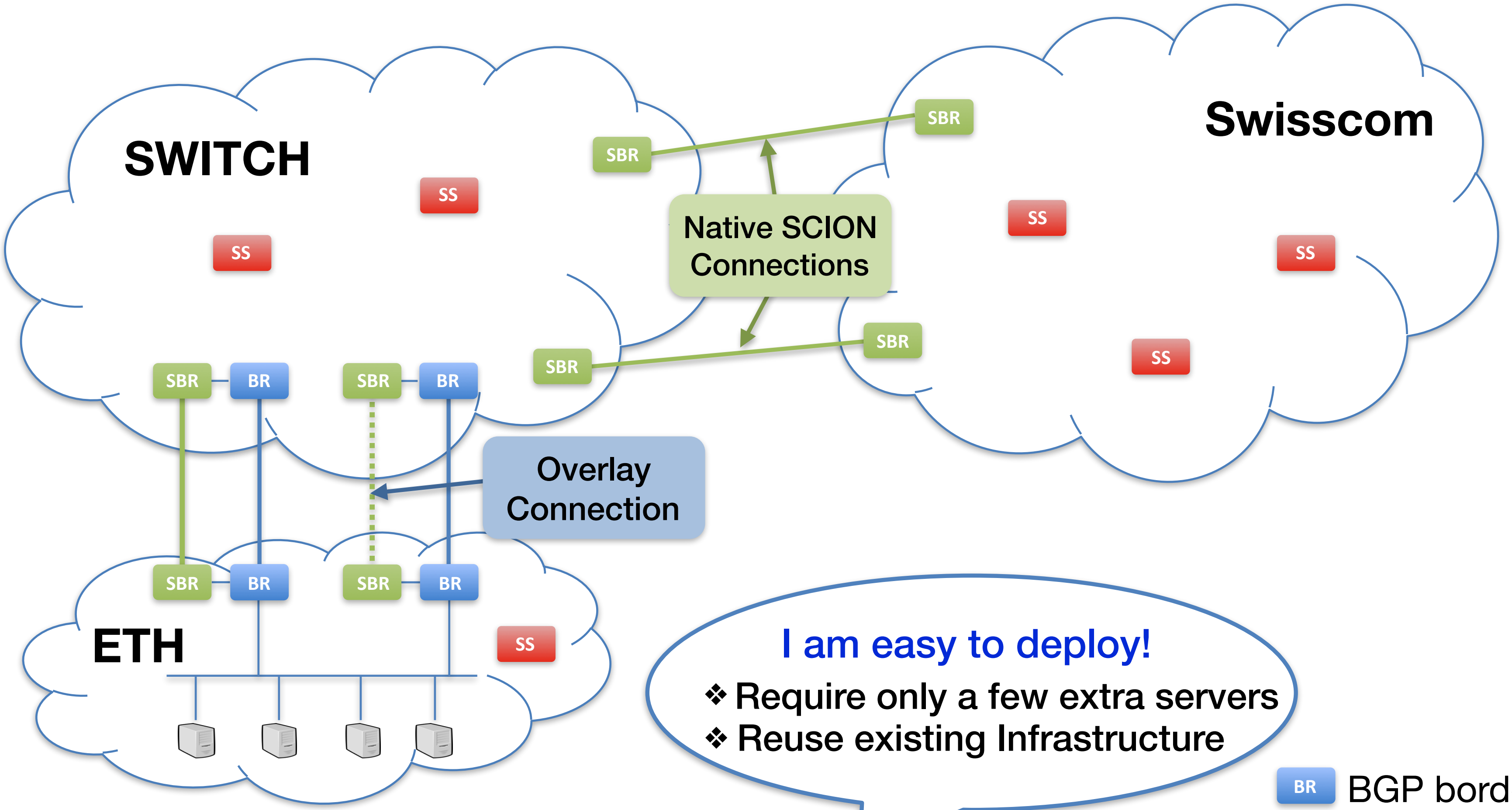
Path-Aware Networking

- ✓ Enables geo-fencing
- ✓ Enables multi-path communication

Improved Network Operation

- ✓ Achieves higher network utilisation
- ✓ Enables advanced traffic engineering

Deployment @ ETH, SWITCH, Swisscom



Native SCION Connections

Overlay Connection

I am easy to deploy!

❖ Require only a few extra servers
❖ Reuse existing Infrastructure

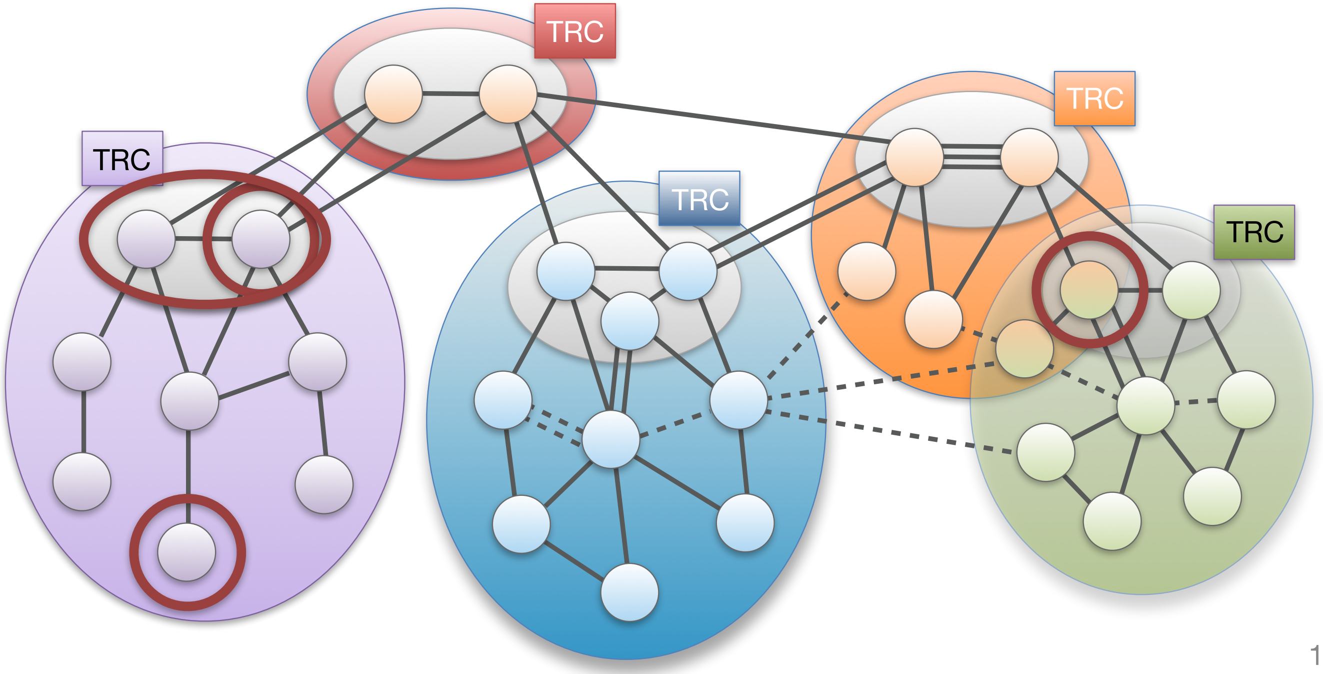
- BR BGP border router
- SBR SCION border router
- SS SCION services

ETH zürich

SCION

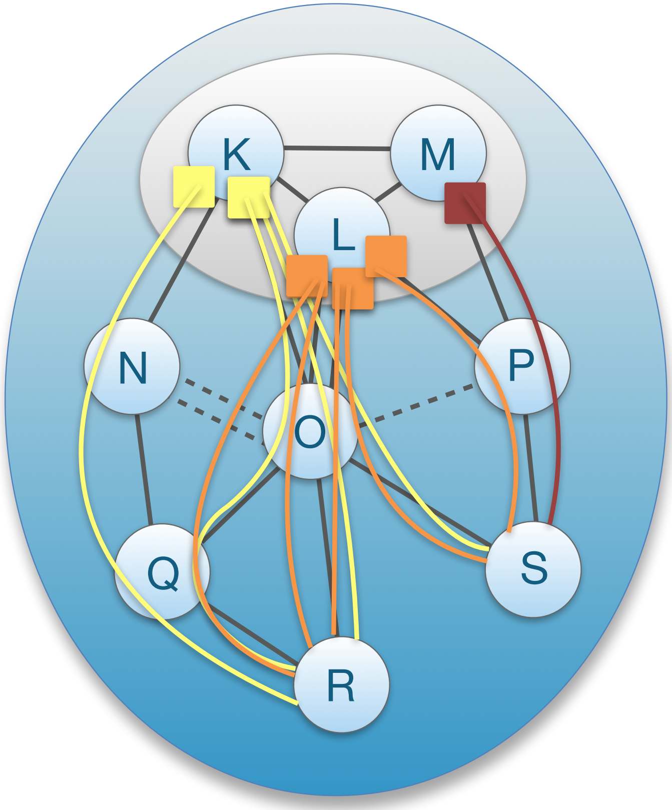
Approach for Scalability: Isolation Domain (ISD)

- Isolation Domain (ISD): grouping of ASes
- ISD core: ASes that manage the ISD
- Core AS: AS that is part of ISD core
- Control plane is organized hierarchically
  - Inter-ISD control plane
  - Intra-ISD control plane

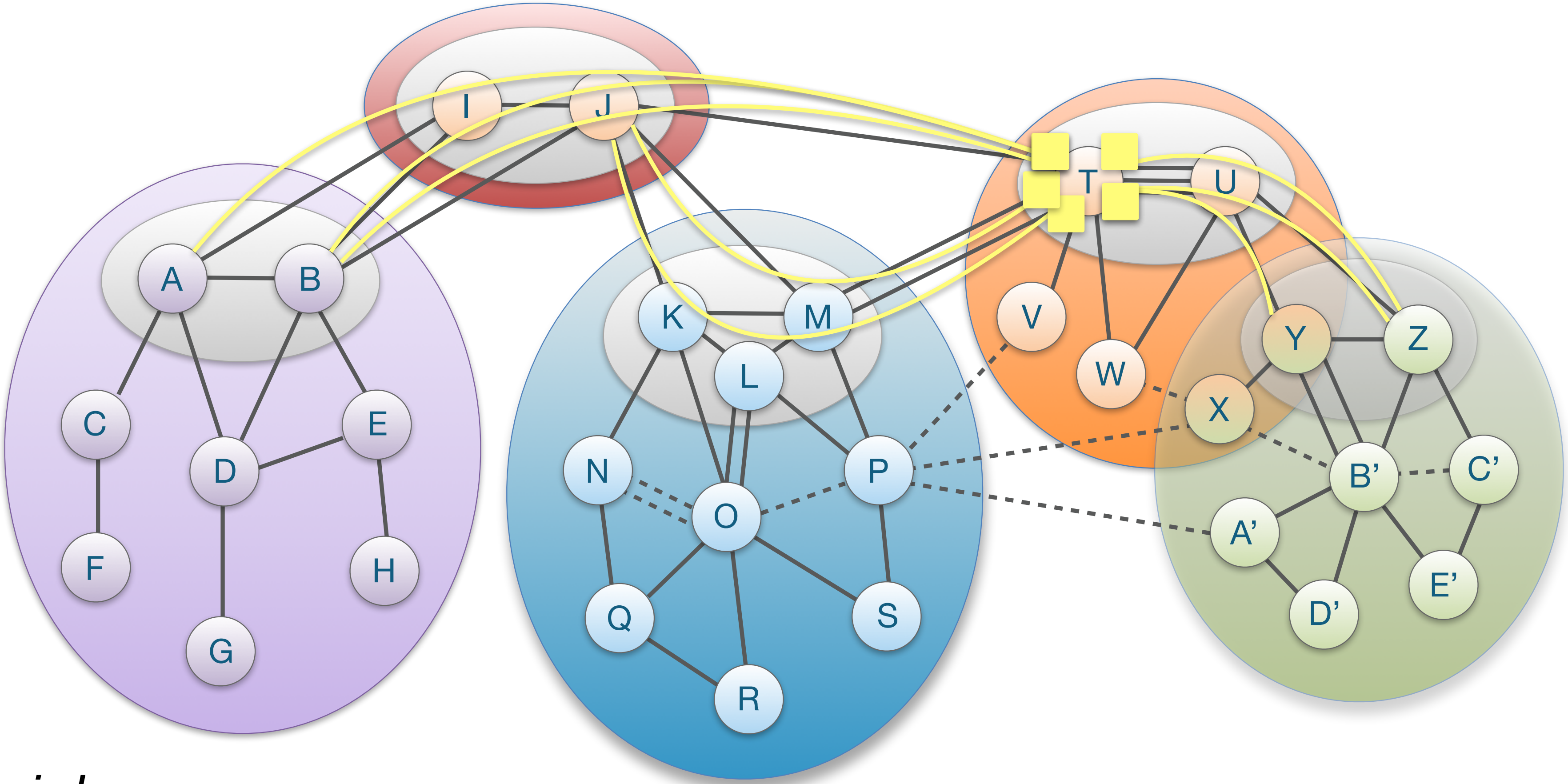


Intra-ISD Path Exploration: Beaconing

- Core ASes K, L, M initiate Path-segment Construction Beacons (PCBs), or “beacons”
- PCBs traverse ISD as a flood to reach downstream ASes
- Each AS receives multiple PCBs representing path segments to a core AS



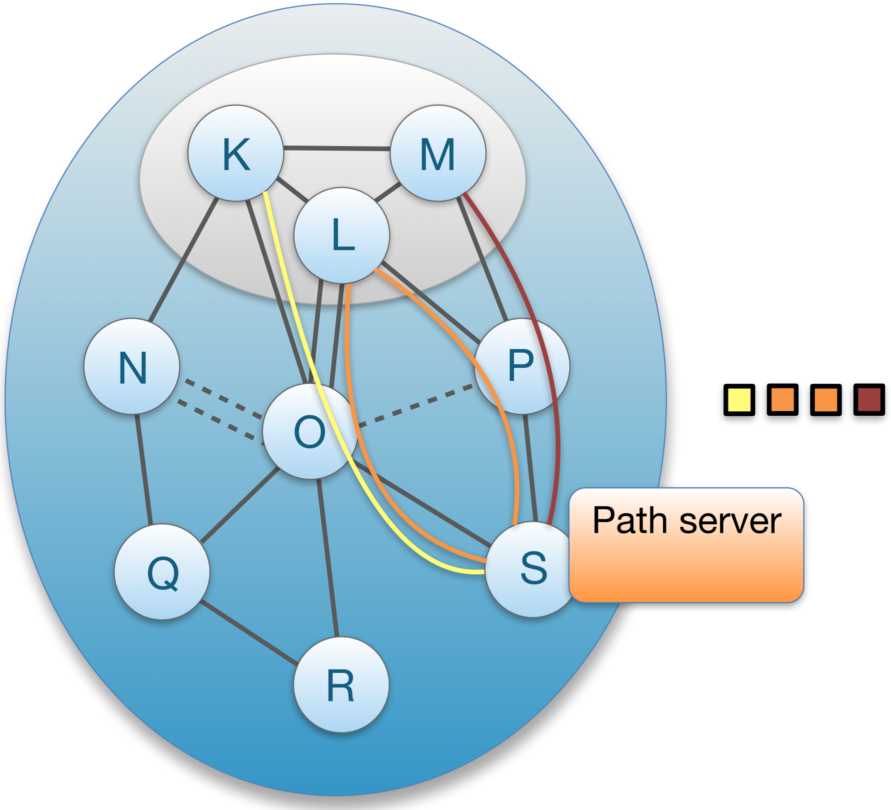
Inter-ISD Path Exploration: Sample Core-Path Segments from AS T



ETH zürich

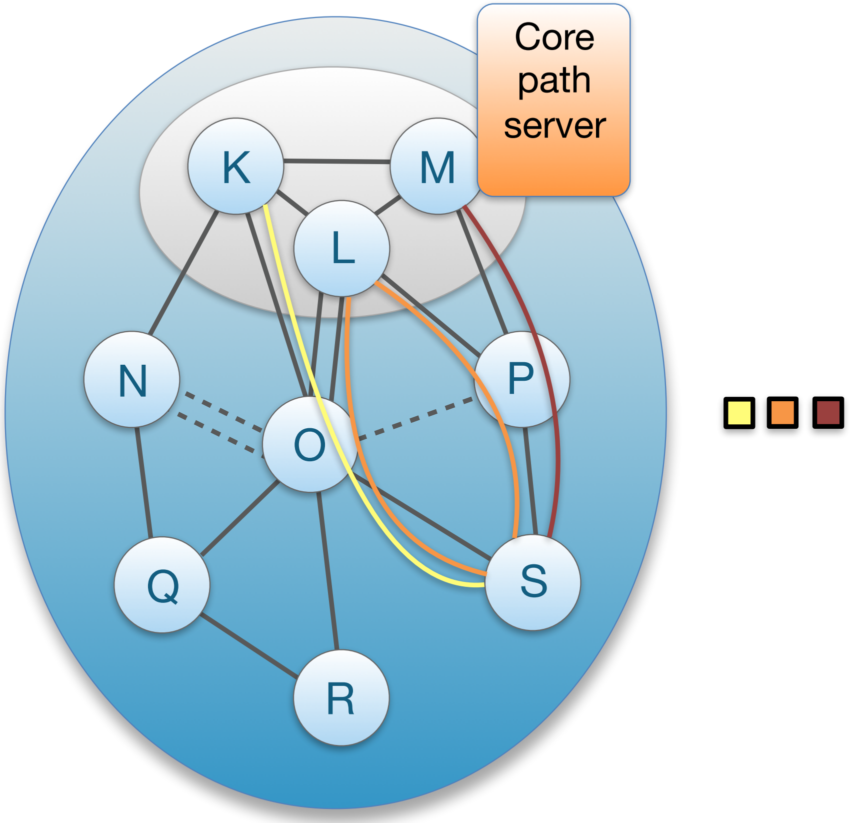
Up-Path Segment Registration

- AS selects path segments to announce as up-path segments for local hosts
- Up-path segments are registered at local path servers



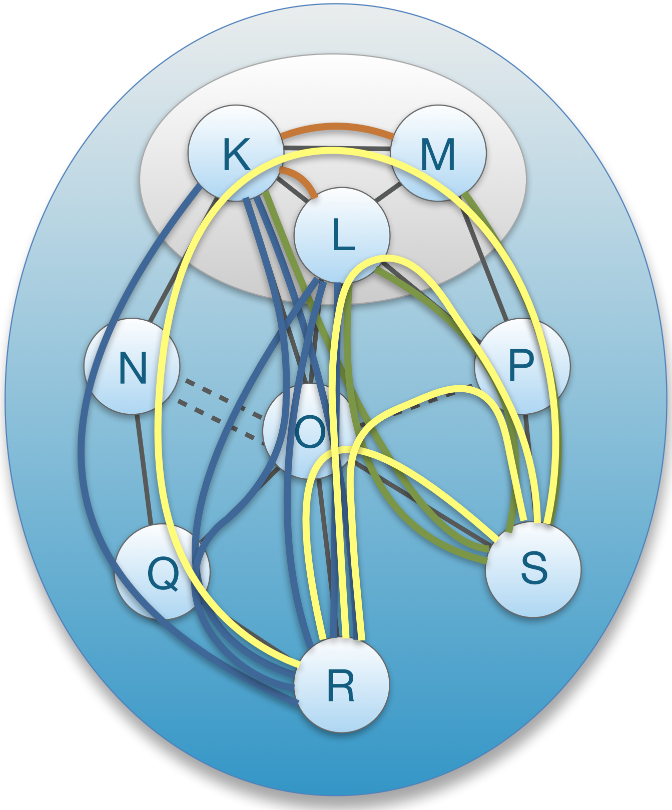
Down-Path Segment Registration

- AS selects path segments to announce as down-path segments for others to use to communicate with AS
- Down-path segments are uploaded to core path server in core AS



Communication within ISD

- Client obtains path segments
  - Up-path segments to local ISD core ASes (blue)
  - Down-path segments to destination (green)
  - Core-path segments as needed to connect up-path and down-path segments (orange)
- Client combines path segments to obtain end-to-end paths (yellow)



SCION Extensions

OPT
DRKey
COLIBRI
Multipath communication
Hidden paths
RAINS
SCION
PISKES
HORNET
TARANET
FAIR
ARPKI
CLEF
APNA

SCION Drawbacks

Initial Latency Inflation

❖ Additional latency to obtain paths

✓ BUT amortized by caching & path reuse

Bandwidth Overhead

❖ Due to paths in the packets

❖ About 80 additional bytes

✓ Enables path control, simpler data plane, etc

Increased Complexity in Key Mgmt.

❖ New certificates (e.g., TRC Certificates)

✓ High security design

Initial Set-up Cost

❖ Training network operators

❖ Installing new infrastructures

✓ Offers methods to facilitate deployment

SCION Use Cases

Use Case I

Highly Availability
Enterprise Connectivity

Use Case II

Secure Networks for
IoT Devices

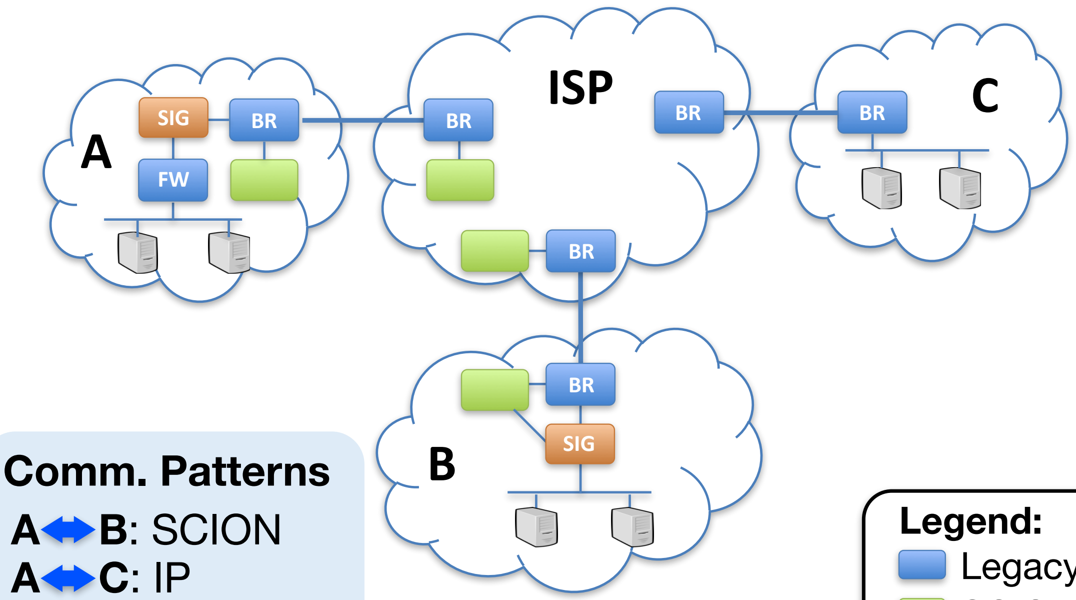
Use Case III

Gaming
Users

Important SCION Components and Concepts

❖ SCION-IP Gateway (SIG)

- Require no update to end hosts

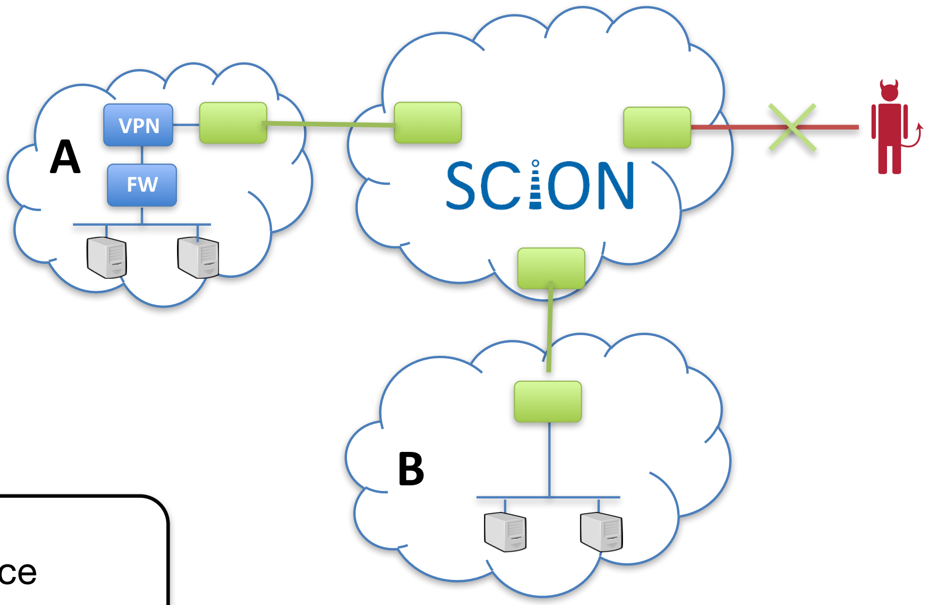


Comm. Patterns

A⟷**B**: SCION
A⟷**C**: IP
B⟷**C**: IP

❖ Hidden Paths

- Create a private link over the Internet

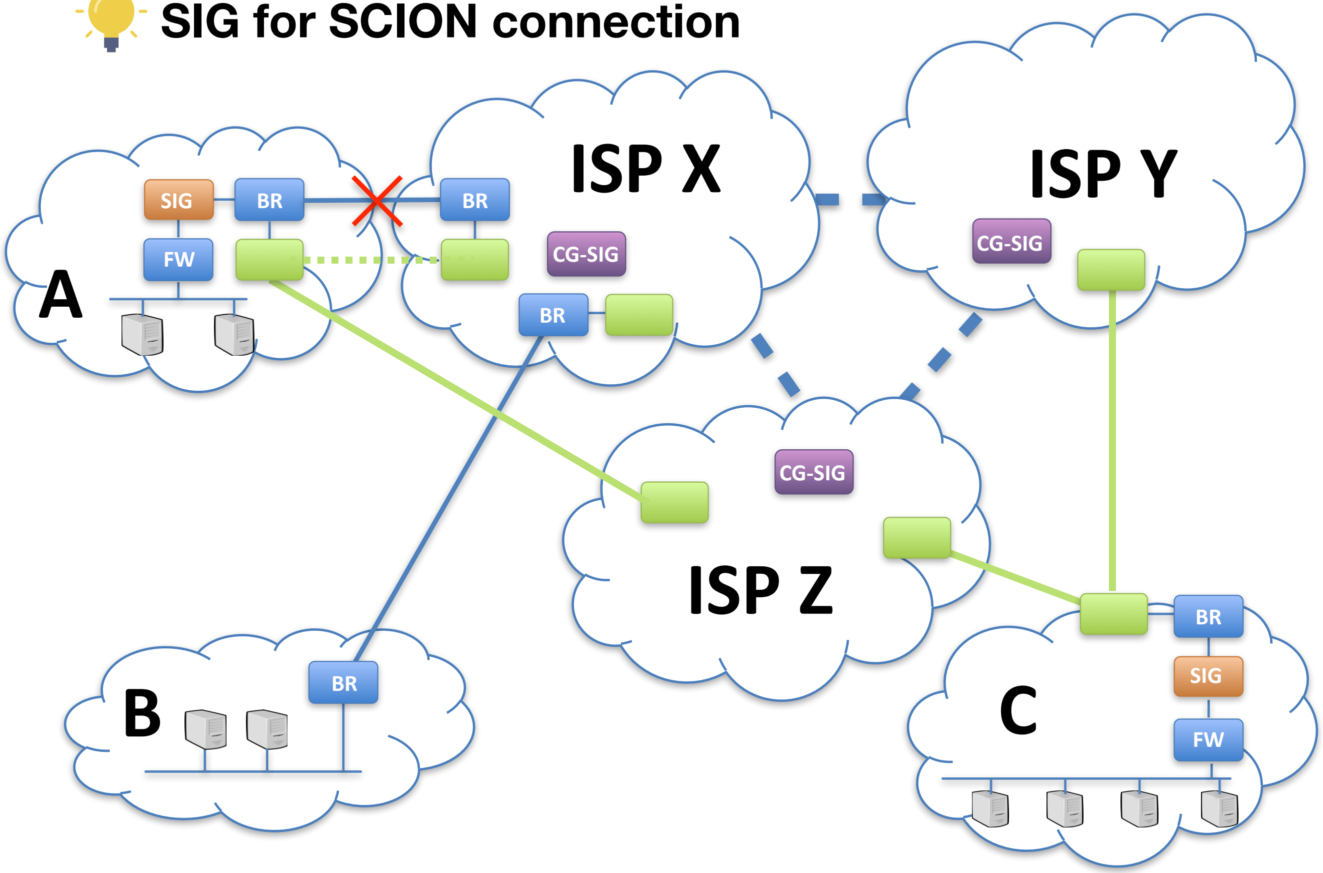


Legend:

🟦 Legacy device
🟩 SCION border router
🟧 SCION SIG

Use Case 1: High-Availability Enterprise Connectivity

💡 SIG for SCION connection



CG-SIG SCION Carrier-grade SIG (CG-SIG)

Deployment Scenario

- Site A has
  - IP connection to ISP X
  - Overlay SCION connection to ISP X
  - Dedicated SCION connection to ISP Z
- Site B has
  - IP connection to ISP X
- Site C has
  - Two dedicated SCION connections to ISPs Y and Z

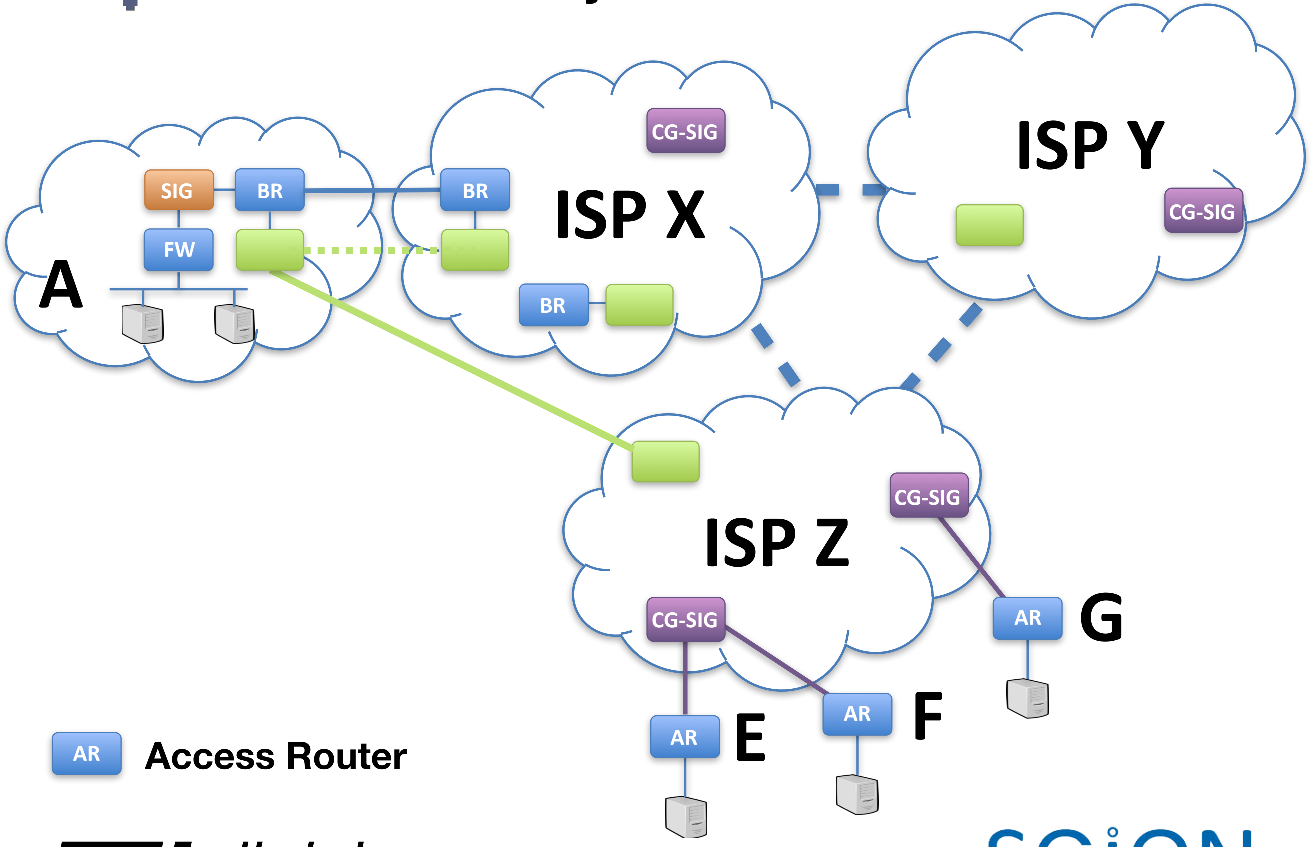
Benefits

✓ Site A has redundant connections
- Fast failover through ISP Z if the IP link between site A and ISP X fails

✓ Site B can benefit from SCION using the CG-SIG at ISP X

Use Case 2: Secure Networks for IoT Devices

- **Use Hidden Paths**
- **Default-off security model**



Deployment Scenario

- ✦ Site A is the monitoring site for IoT devices
- ✦ IoT Devices E, F, G are at ISP Z
  - Connected to SCION via CG-SIGs
  - Path Segments to the CG-SIGs are hidden and only given to site A

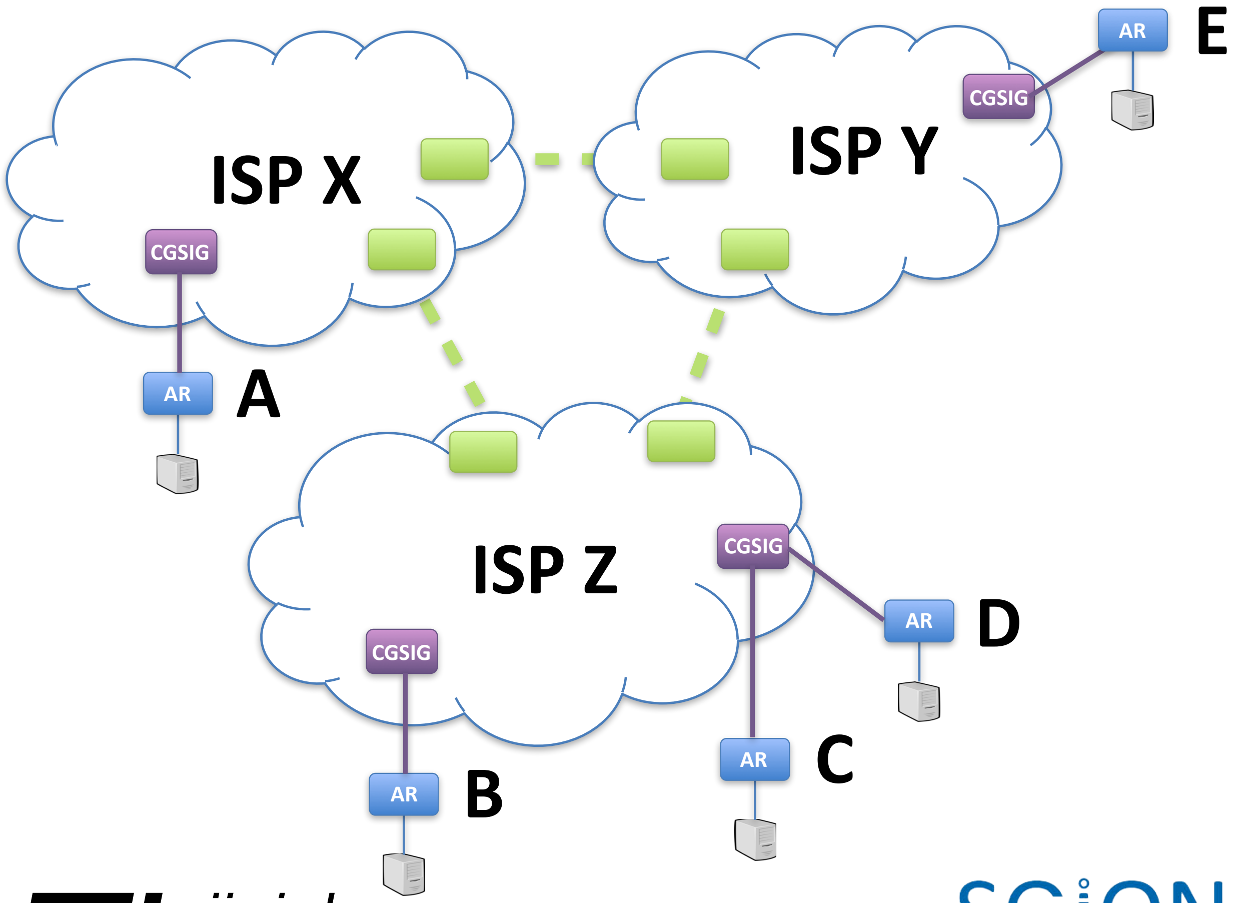
Benefits

- ✓ Secure network access
  - Only site A can access E, F, G
- ✓ High availability for the IoT network by using CG-SIG

ETH zürich

SCION

Use Case 3: Gaming Users



Deployment Scenario

- Gaming users A-E purchase SCION Internet Connection
  - Connected using CG-SIGs
  - Use hidden paths for communication between the participants

Benefits

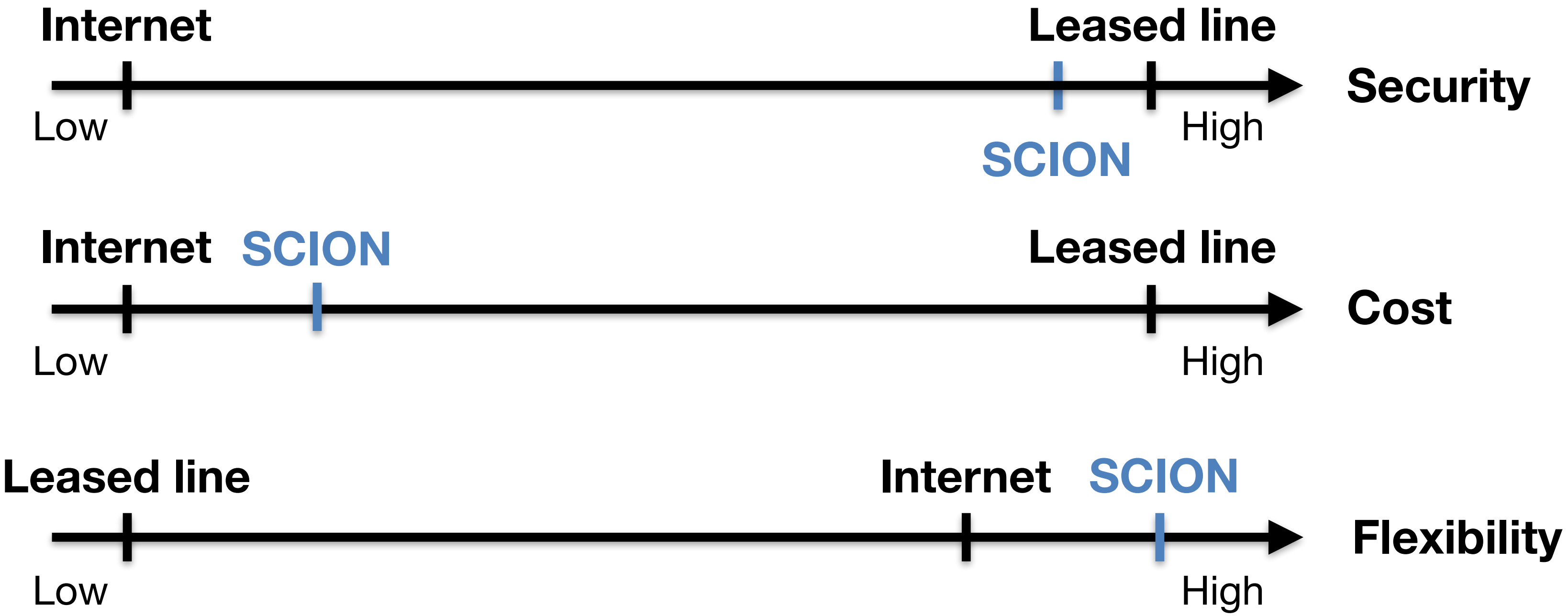
- ✓ Latency optimization by CG-SIG
  - Choose a path with the lowest latency
- ✓ DoS/DDoS protection using the hidden paths

ETH zürich

SCION

Value Proposition for Customers

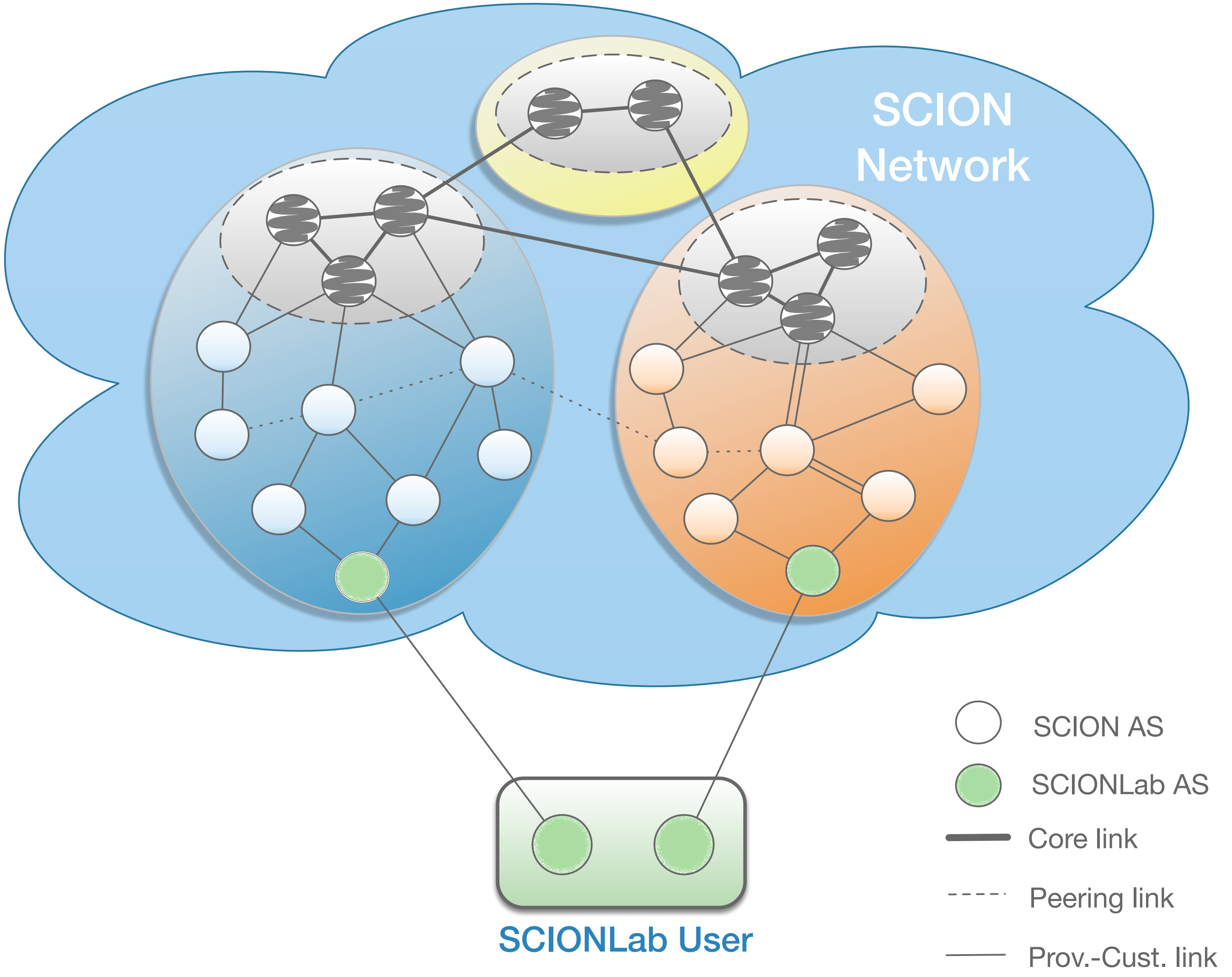
- SCION offers highly secure and available Internet communication with built-in DDoS defense



Value Proposition for ISPs

- New service offerings for customers
  - Premium link offerings
  - Geofencing, path choice
  - Business continuity (high availability / fast failover)
  - Pseudo-leased line at a fraction cost
- Lower network management overhead
- Increased network capacity utilization

SCIONLab



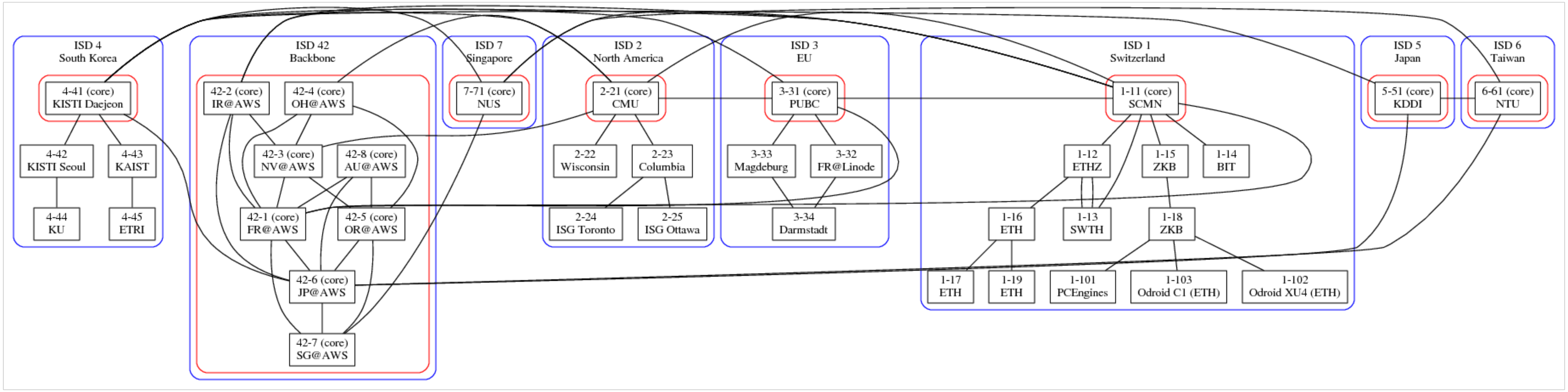
ETH zürich

Exciting SCIONLab Research Opportunities

- Next-generation Internet architecture research
- Users obtain real ASes with all cryptographic credentials to participate in the control plane
- ASes can use their own computing resources and attach at several points in the SCIONLab network
- Path-aware networking testbed
- Hidden paths for secure IoT operation
- Control-plane PKI in place, each AS has certificate
- Network availability and performance measurement (bandwidth and latency)
- Supported features (PKI, DDoS defense mechanisms, path selection support, end host / application support)
- (Security) Usability research
- Inter-domain routing scalability research
- Multi-path research
- Multi-path QUIC socket
- End-to-end PKI system that application developers can rely on to build highly secure TLS applications
- SIBRA inter-domain resource allocation system
- DDoS defense research using in-network defense mechanisms
- Next-generation routing architecture policy definitions

Global SCIONLab Network

- https://www.scionlab.org
- Collaboration with David Hausheer @ Uni Magdeburg



ISD 4
South Korea
4-41 (core)
KISTI Daejeon
4-42
KISTI Seoul
4-43
KAIST
4-44
KU
4-45
ETRI

ISD 42
Backbone
42-2 (core)
IR@AWS
42-4 (core)
OH@AWS
42-3 (core)
NV@AWS
42-8 (core)
AU@AWS
42-1 (core)
FR@AWS
42-5 (core)
OR@AWS
42-6 (core)
JP@AWS
42-7 (core)
SG@AWS

ISD 7
Singapore
7-71 (core)
NUS

ISD 2
North America
2-21 (core)
CMU
2-22
Wisconsin
2-23
Columbia
2-24
ISG Toronto
2-25
ISG Ottawa

ISD 3
EU
3-31 (core)
PUBC
3-33
Magdeburg
3-32
FR@Linode
3-34
Darmstadt

ISD 1
Switzerland
1-11 (core)
SCMN
1-12
ETHZ
1-15
ZKB
1-14
BIT
1-16
ETH
1-13
SWTH
1-18
ZKB
1-17
ETH
1-19
ETH
1-101
PCEngines
1-103
Odroid C1 (ETH)
1-102
Odroid XU4 (ETH)

ISD 5
Japan
5-51 (core)
KDDI

ISD 6
Taiwan
6-61 (core)
NTU

SCION Commercialization

- Founded Anapaya Systems in June 2017
- 4 founders: David Basin, Sam Hitz (CEO), Peter Müller, Adrian Perrig
- Several banks and ISPs are customers
- https://www.anapaya.net

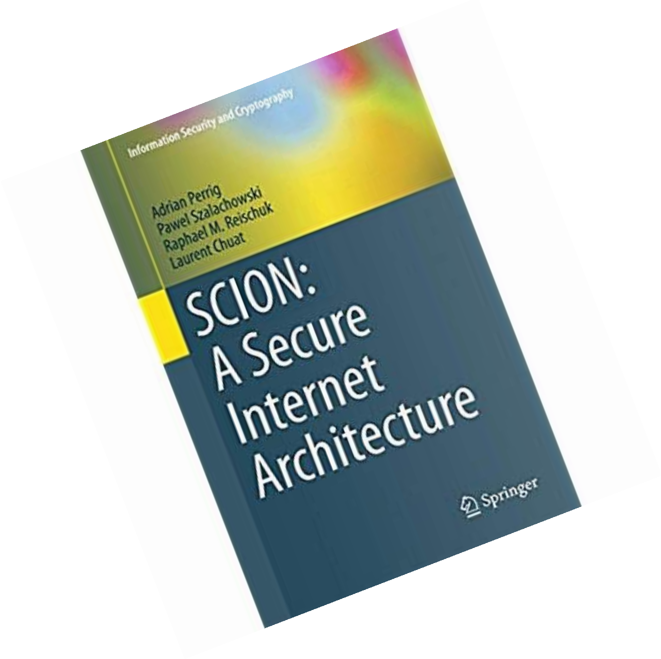
ANAPAYA SYSTEMS

Securing and Optimizing Internet Communication

anapaya systems

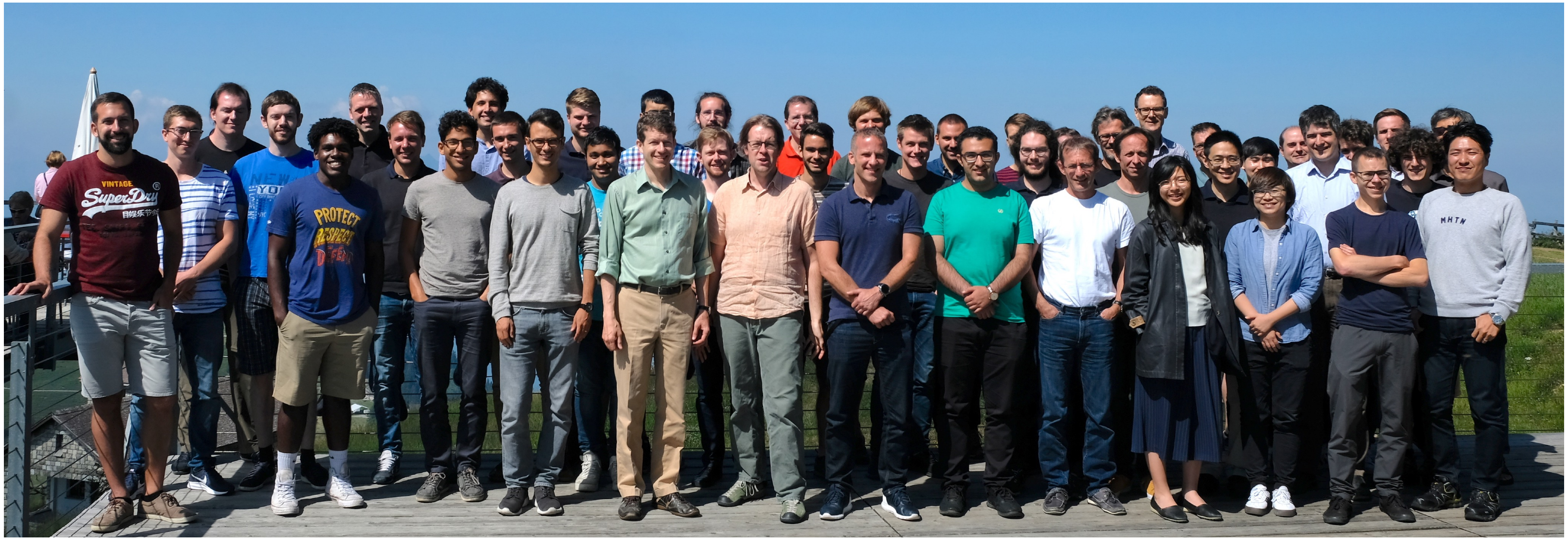
Online Resources

- 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


Information Security and Cryptography
Adrian Perrig
Pawel Szalachowski
Raphael M. Reischuk
Laurent Chuat
SCION: A Secure Internet Architecture
Springer

SCION Core Project Team

- Netsec: Daniele Asoni, Laurent Chuat, Sergiu Costea, Piet De Vaere, Sam Hitz, Mike Farb, Matthias Frei, Giacomo Giuliari, Tobias Klausmann, Cyrill Krähenbühl, Jonghoon Kwon, Tae-Ho Lee, Sergio Monroy, Chris Pappas, Juan Pardo, Adrian Perrig, Benjamin Rothenberger, Stephen Shirley, Jean-Pierre Smith, Brian Trammell, François Wirtz
- Infsec: David Basin, Tobias Klenze, Ralf Sasse, Christoph Sprenger, Thilo Weghorn
- Programming Methodology: Marco Eilers, Peter Müller
- Uni Magdeburg: David Hausheer, UIUC: Yih-Chun Hu, NTU: Hsu-Chun Hsiao



Conclusion: SCION is a Disruptive Technology

- Network attacks are made impossible by design
  - SCION offers communication guarantees in spite of DDoS attacks, BGP prefix hijacking, etc.
- New security properties
  - Geofencing
  - Path verification
- Improved communication efficiency
  - Increased bandwidth thanks to multi path communication
  - Decreased latency thanks to path optimization
  - Fast failover provides business continuity

Thanks to our Sponsors!

ETH zürich

ZISC Zurich Information Security & Privacy Center

erc

NSF

SIX

swisscom

Zürcher Kantonalbank

NEC

INFOSEC GLOBAL

Google

SWITCH

KDDI

T Deutsche Telekom