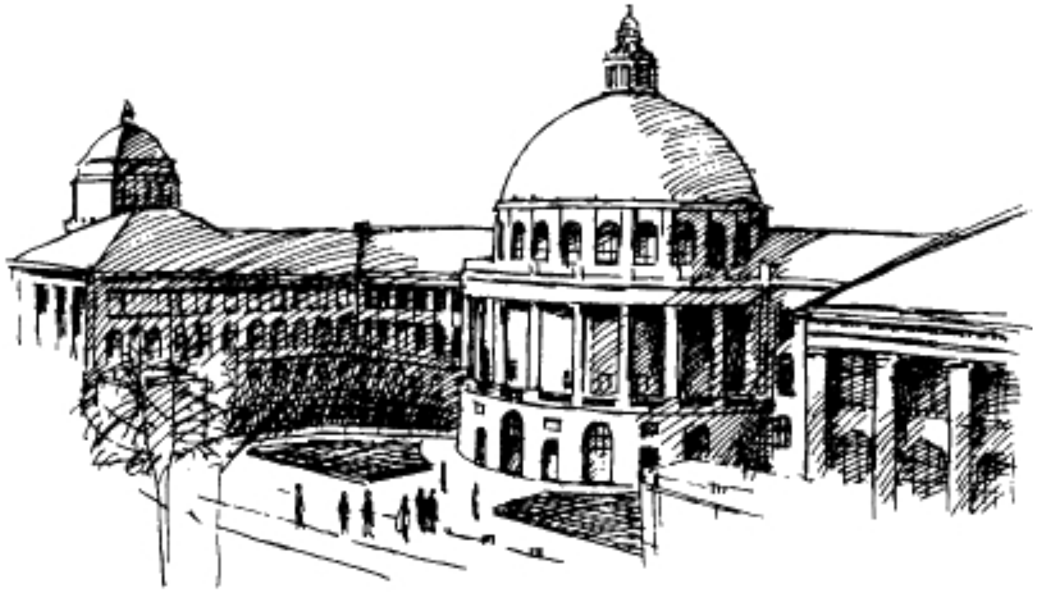
SCION:
A Secure Internet Architecture

Markus Legner

Network Security Group

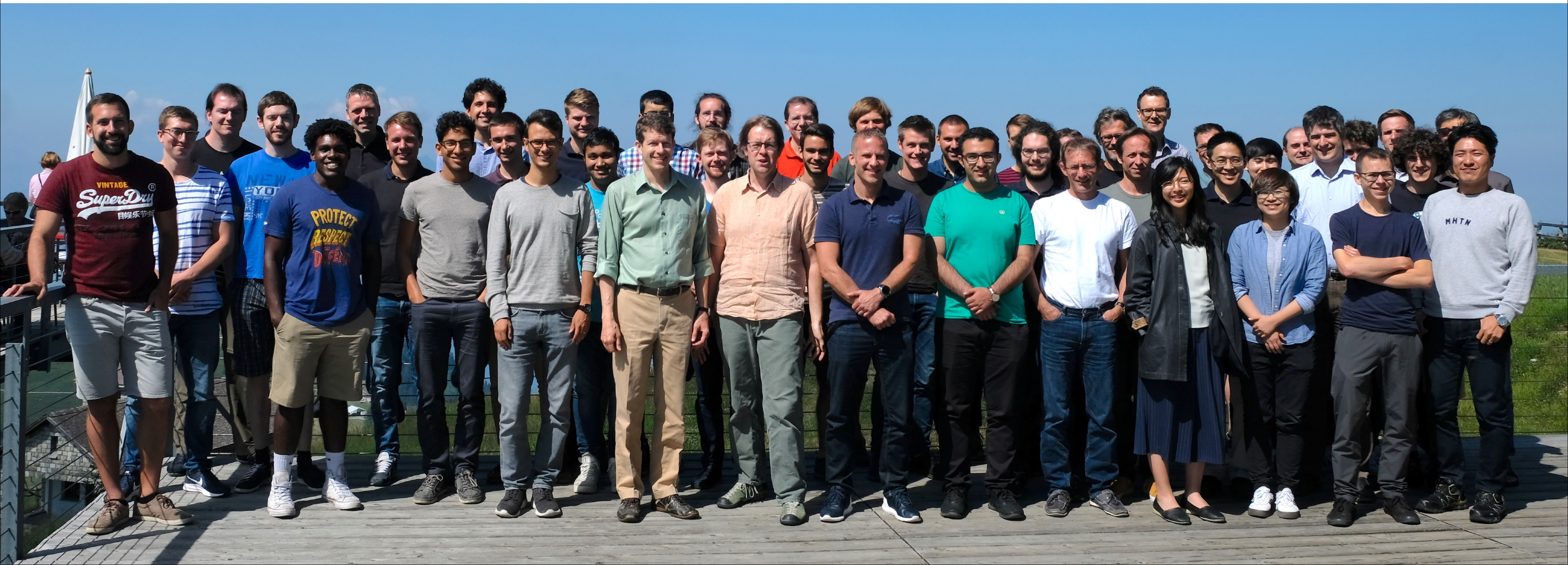
ETH Zürich

SiNOG 6.0, May 2019

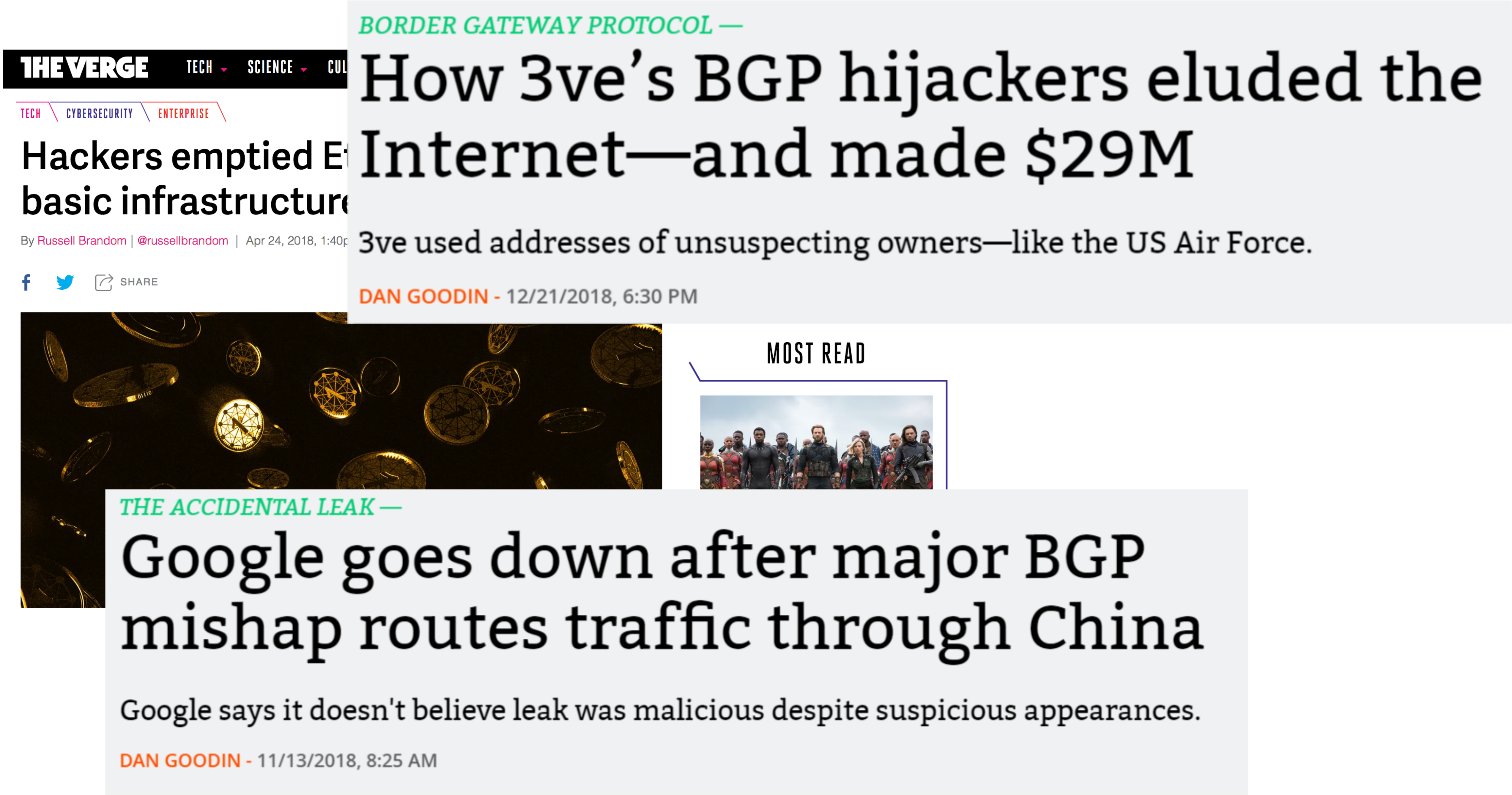


SCION Core Project Team

- Netsec: Daniele Asoni, Laurent Chuat, Sergiu Costea, Piet De Vaere, Samuel Hitz, Mike Farb, Matthias Frei, Giacomo Giuliari, Mateusz Kowalski, Cyrill Krähenbühl, Jonghoon Kwon, Markus Legner, Sergio Monroy, Juan Pardo, Adrian Perrig, Benjamin Rothenberger, Simon Scherrer, Stephen Shirley, Jean-Pierre Smith, Joel Wanner, François Wirz
- 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



Internet Security Issues



TECH CYBERSECURITY ENTERPRISE

Hackers emptied Et
basic infrastructur

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

BORDER GATEWAY PROTOCOL —

How 3ve's BGP hijackers eluded the Internet—and made $29M

3ve used addresses of unsuspecting owners—like the US Air Force.

DAN GOODIN - 12/21/2018, 6:30 PM

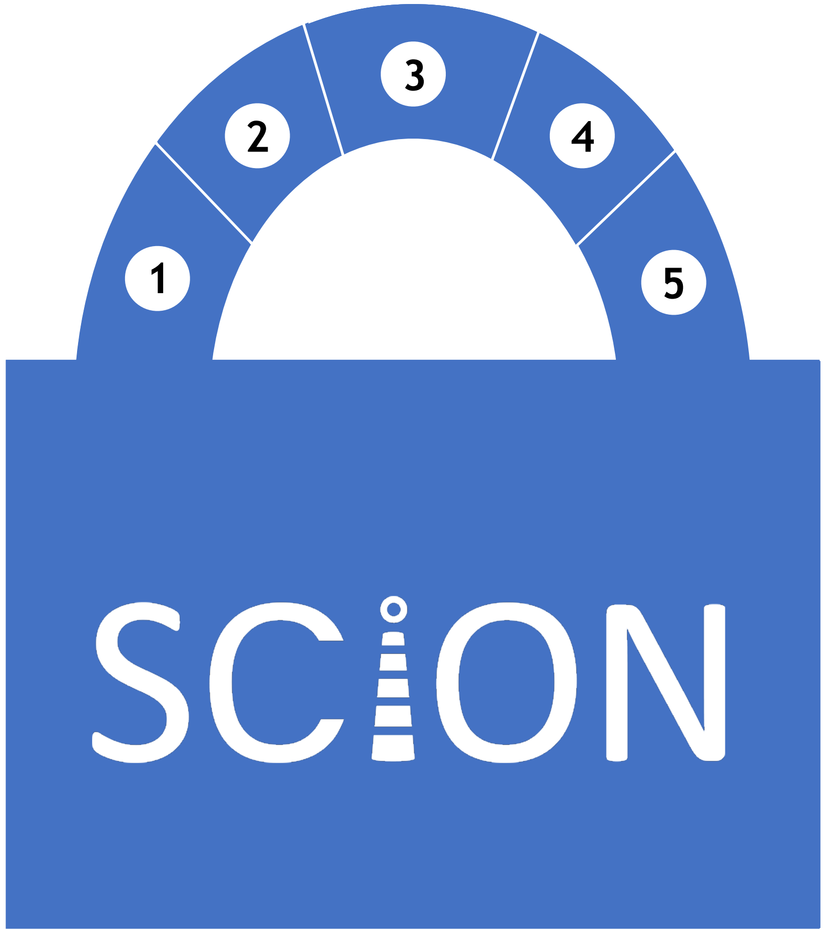
THE ACCIDENTAL LEAK —

Google goes down after major BGP mishap routes traffic through China

Google says it doesn't believe leak was malicious despite suspicious appearances.

DAN GOODIN - 11/13/2018, 8:25 AM

What is different in SCION?



1 Path-aware networking

2 New routing and forwarding architecture

3 Provable security: Protocol + Code

4 Heterogeneous trust model

5 Built-in DDoS defense mechanisms

Path-aware Networking

1 Path-aware networking

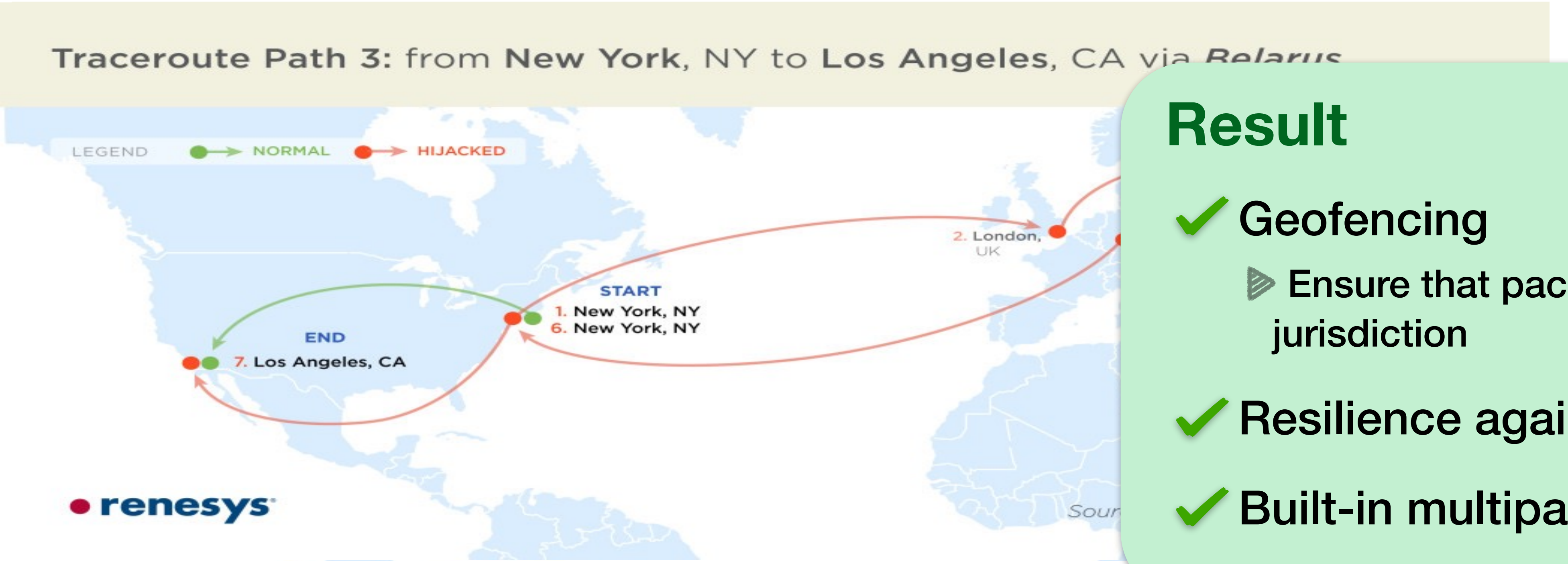
High Assurance for Network Paths

Current Internet

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

New Approach

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



Traceroute Path 3: from New York, NY to Los Angeles, CA via Belarus

Result

- ✓ Geofencing
  - Ensure that packet stays within certain jurisdiction
- ✓ Resilience against hijacking attacks
- ✓ Built-in multipath support

New Routing and Forwarding Architecture

2 New routing and forwarding architecture

1 Path-aware networking

High Assurance for Routing and Forwarding

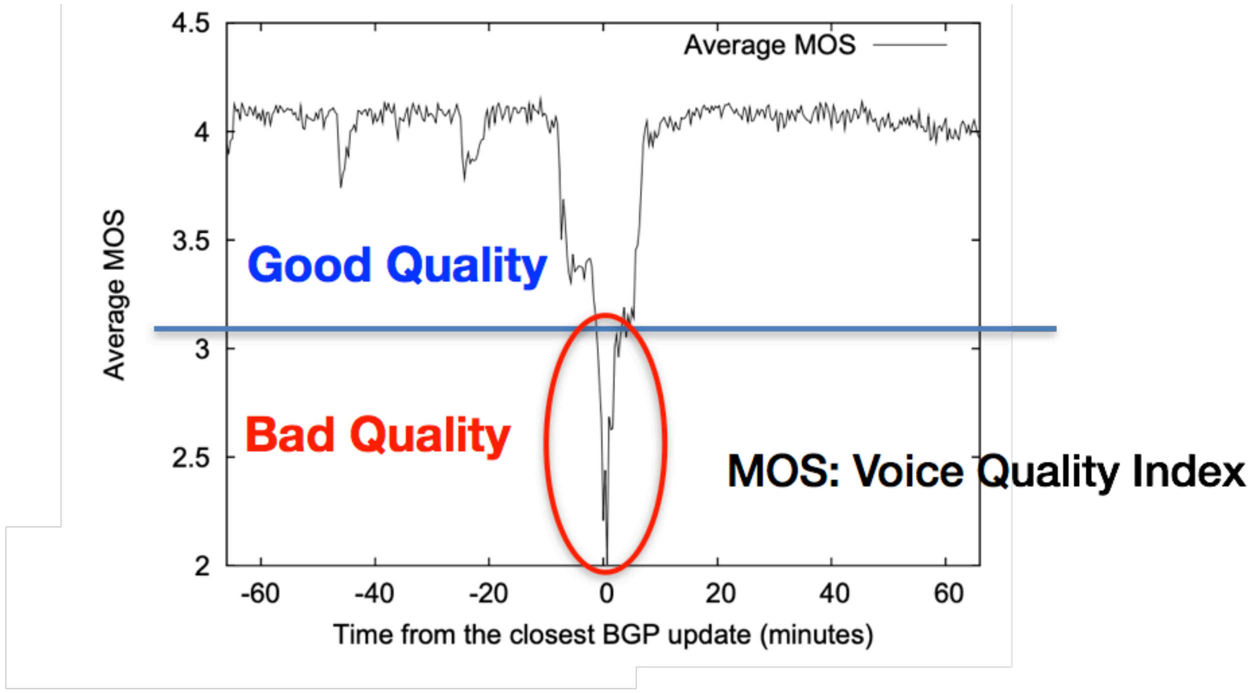
Current Internet

- ✗ BGP slow to converge to stable state
- ✗ Lack of separation between control and data plane leads to outages

New Approach

SCION

- ✦ **Fast converging** routing process
- ✦ **Authenticated** routing messages
- ✦ Simple and **stateless** routers



MOS: Voice Quality Index

Result

SCION

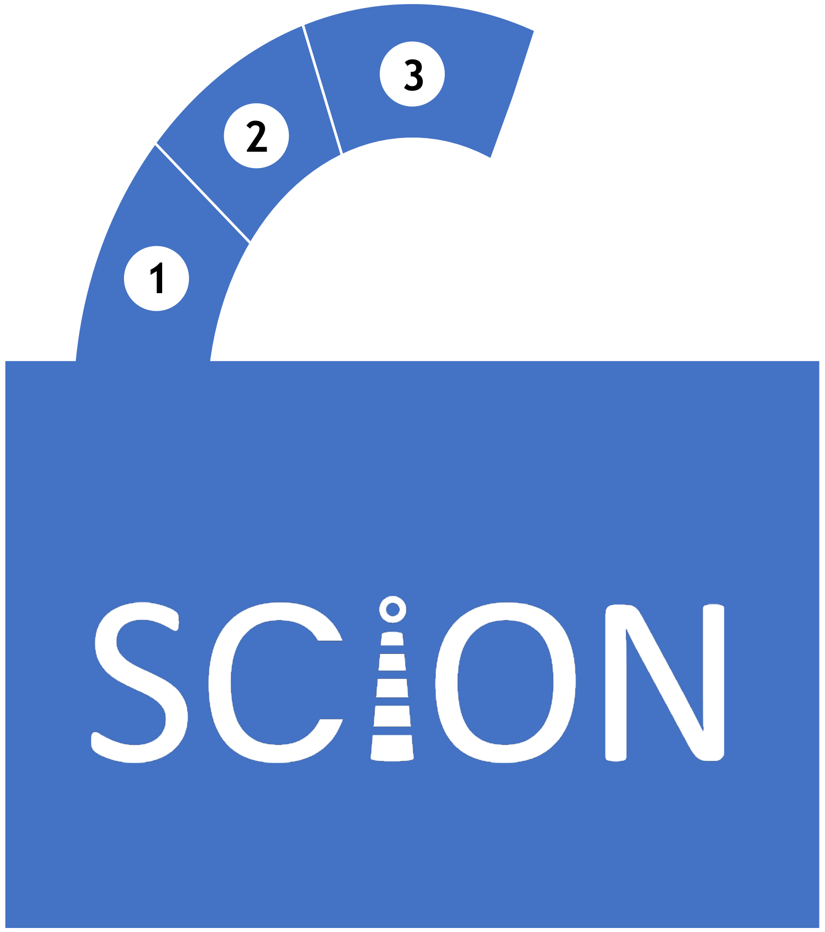
- ✓ Increases availability of the Internet
- ✓ Increases Quality of Experience (QoE)

Provable Security: Protocol + Code

3 Provable security: Protocol + Code

2 New routing and forwarding architecture

1 Path-aware networking



High Assurance for Protocols and Code

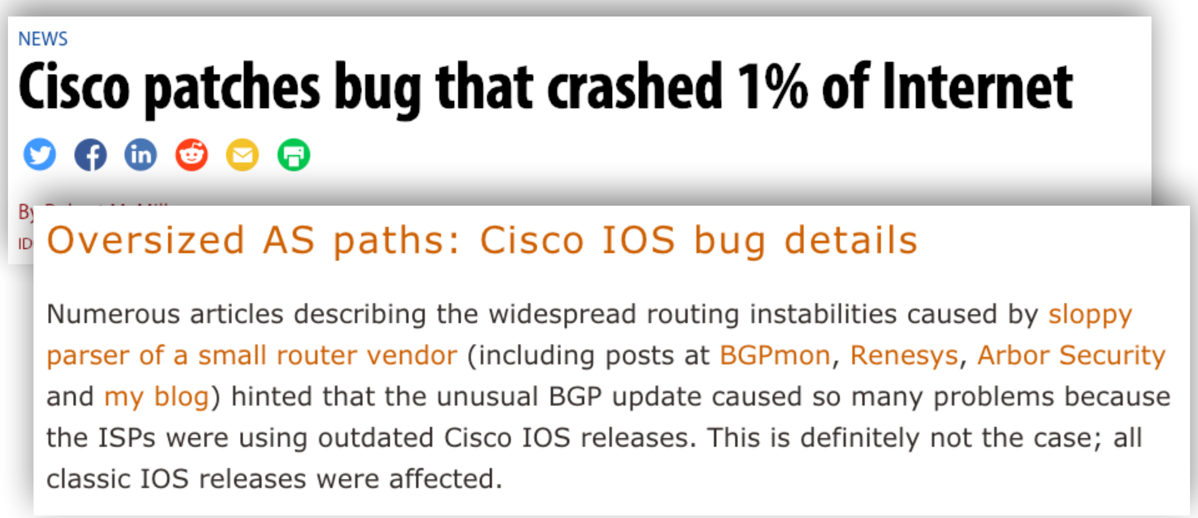
Current Internet

- ✗ Problems with BGP protocol
- ✗ Faulty router implementations

New Approach

SCION

- ✦ Formally modeled and **verified protocols**
- ✦ Formally **verified implementations**



NEWS

Cisco patches bug that crashed 1% of Internet

Oversized AS paths: Cisco IOS bug details

Numerous articles describing the widespread routing instabilities caused by sloppy parser of a small router vendor (including posts at BGPmon, Renesys, Arbor Security and my blog) hinted that the unusual BGP update caused so many problems because the ISPs were using outdated Cisco IOS releases. This is definitely not the case; all classic IOS releases were affected.

Result

SCION

- ✓ **Increase resiliency** against failures due to faulty design and implementation
- ✓ Obtain high assurance for communication

Heterogenous Trust Model

1 Path-aware networking

2 New routing and forwarding architecture

3 Provable security: Protocol + Code

4 Heterogeneous trust model

Heterogeneous Trust Models & Network Sovereignty

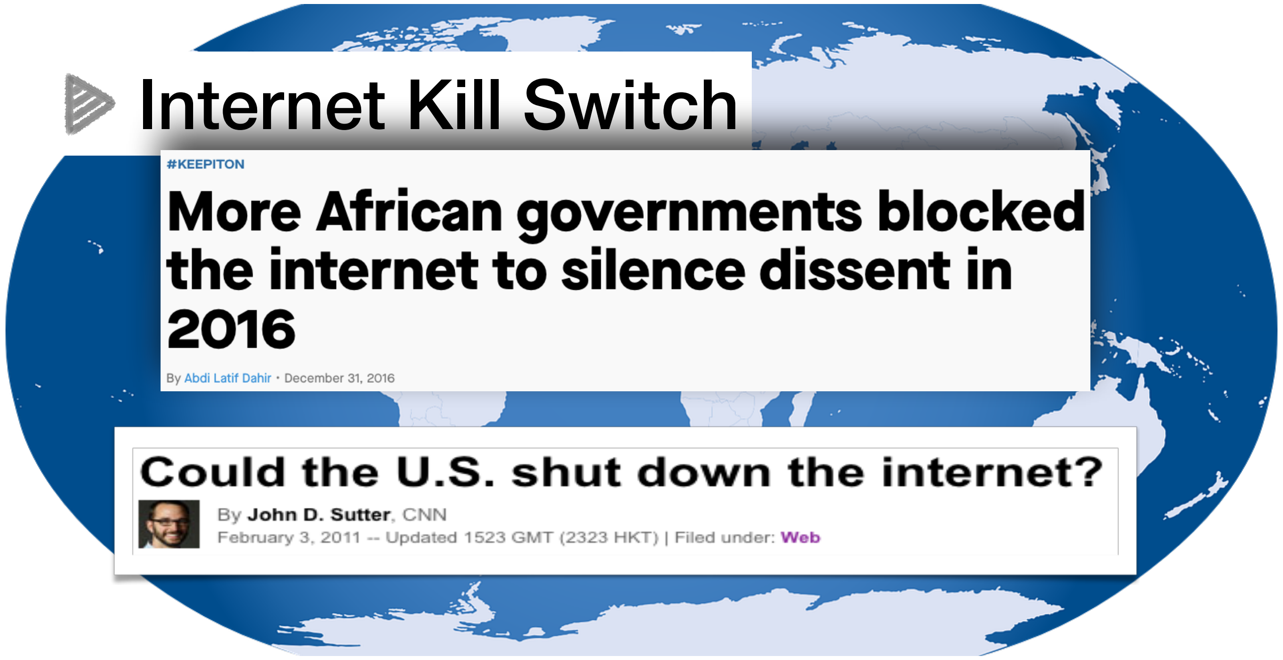
Current Internet

- ✗ Either no trust model or global roots of trust
- ✗ Whoever controls the global root of trust can shut down parts of the Internet

New Approach

SCION

- ✦ Isolation domains define **sovereign Internet region**
- ✦ Each isolation domain can choose its own trust roots



Internet Kill Switch

#KEEPITON

More African governments blocked the internet to silence dissent in 2016

By Abdi Latif Dahir · December 31, 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**

Result

SCION

- ✓ Autonomy/Sovereignty for infrastructure, e.g., at national level
- ✓ No kill switches

Built-in DDoS Defense Mechanisms

3 Provable security: Protocol + Code

2 New routing and forwarding architecture

4 Heterogeneous trust model

1 Path-aware networking

5 Built-in DDoS defense mechanisms

1
2
3
4
5
SCION

Built-in DDoS Defense Mechanisms

Current Internet

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

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

New Approach

SCION

- ✦ Secure by design
  - Most attacks are prevented by construction
- ✦ **Multipath** communication and source authentication
- ✦ Dynamic global bandwidth-reservation system

Result

SCION

- ✓ Reduce malicious traffic on the Internet
- ✓ Guaranteed communication despite DDoS attacks

SCION in a Nutshell

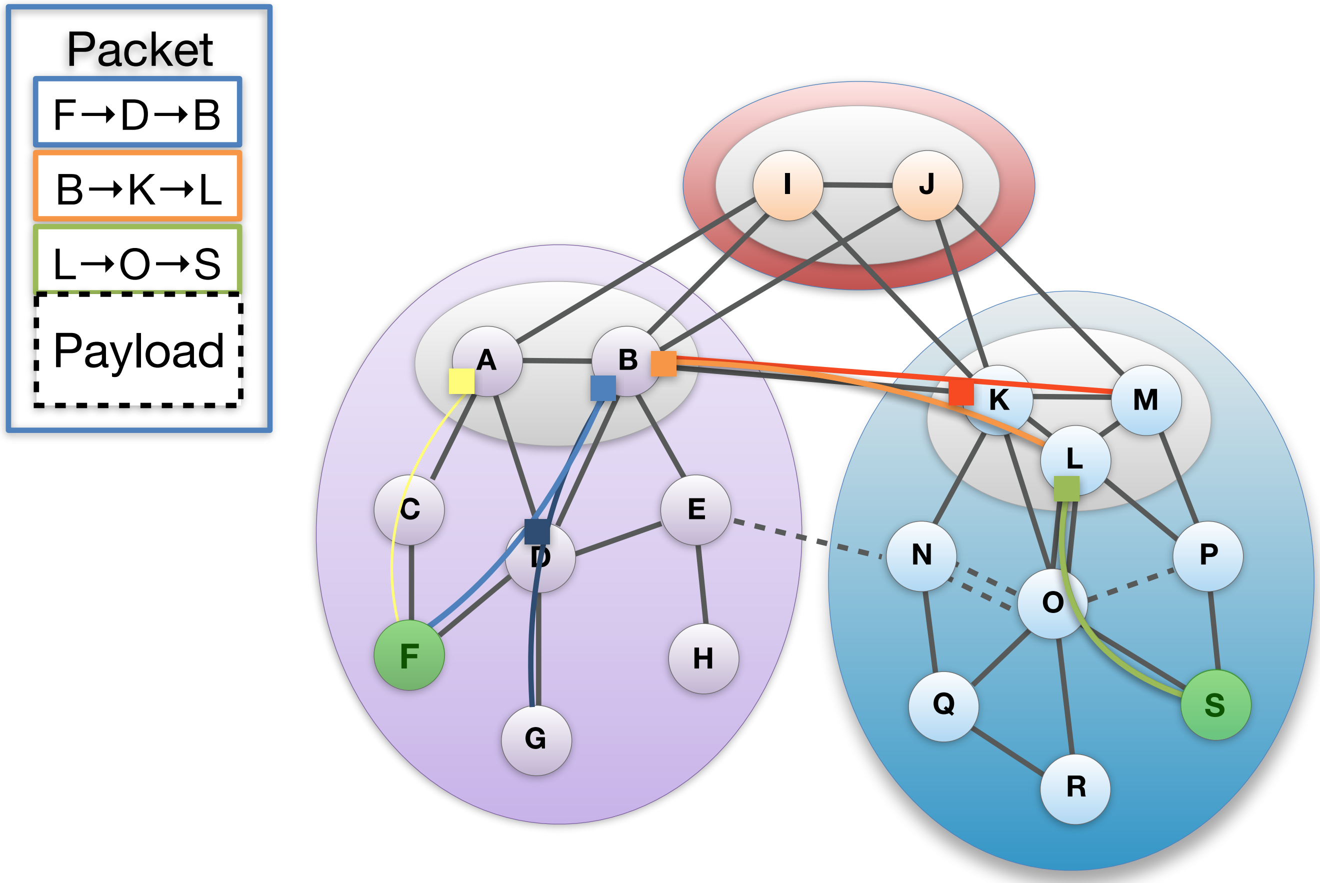
Path-based Network Architecture

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



Packet

F→D→B

B→K→L

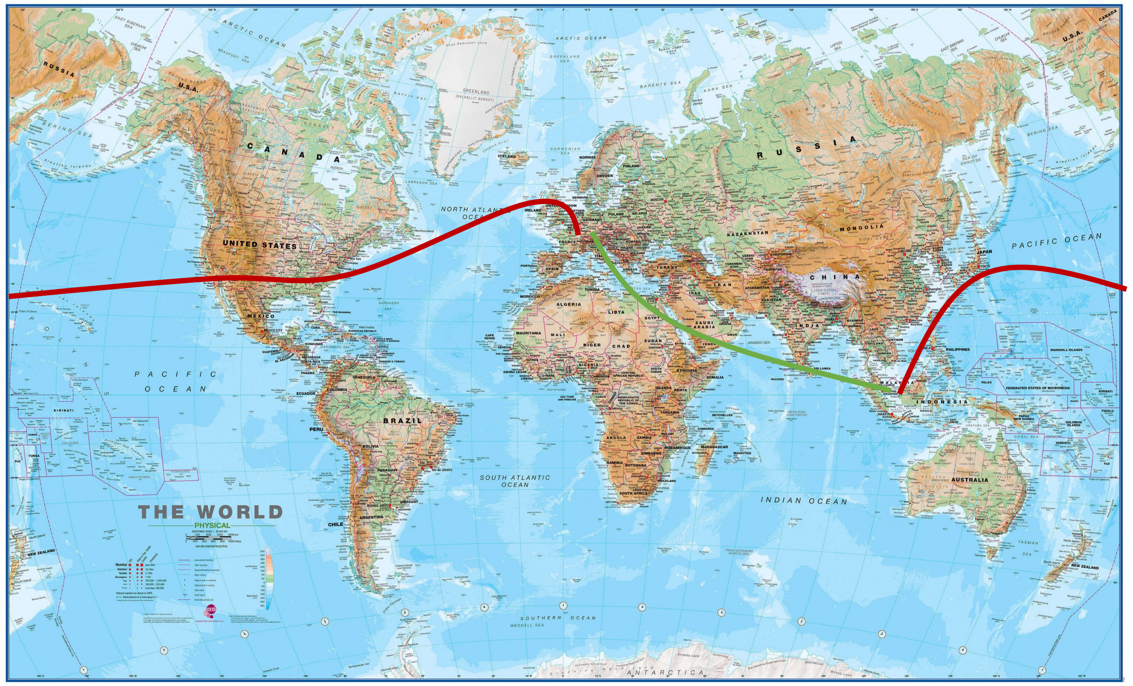
L→O→S

Payload

Isolation Domains (ISDs)

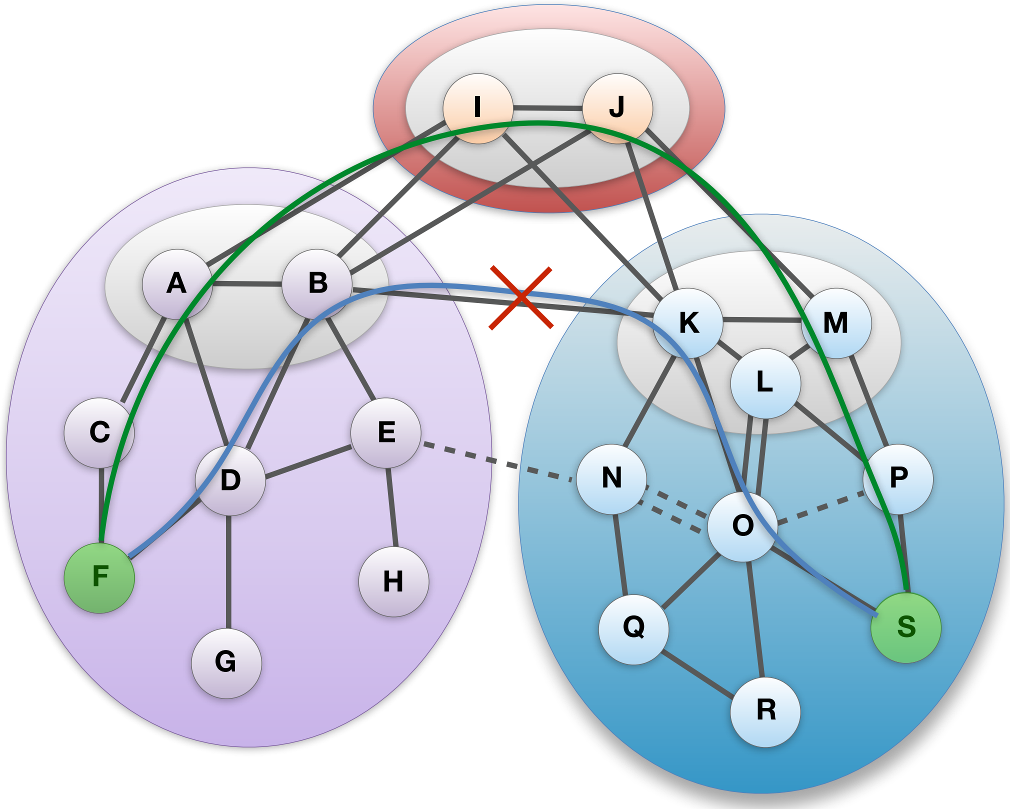
Use Case: Low-Latency Connectivity

- 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!



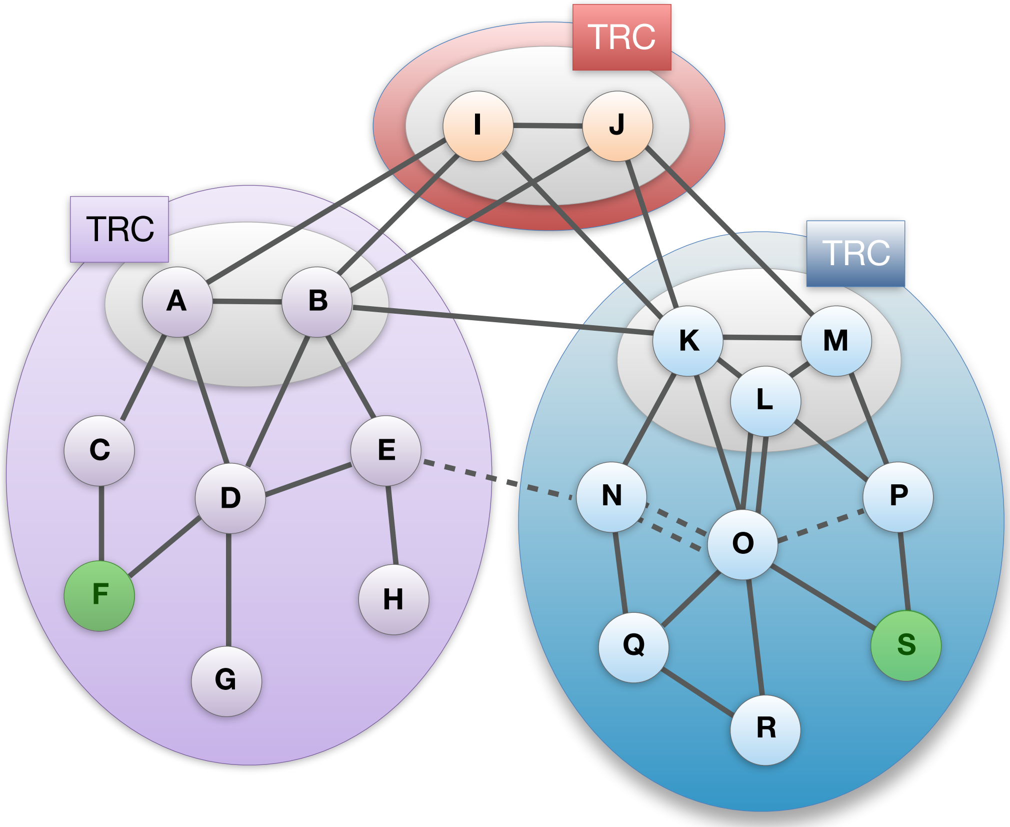
Use Case: High-Speed Interdomain Failover

- 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: multiple paths available to end hosts
- Backup path is already set up and ready to be used when a link failure is observed
- Result: failover within milliseconds!

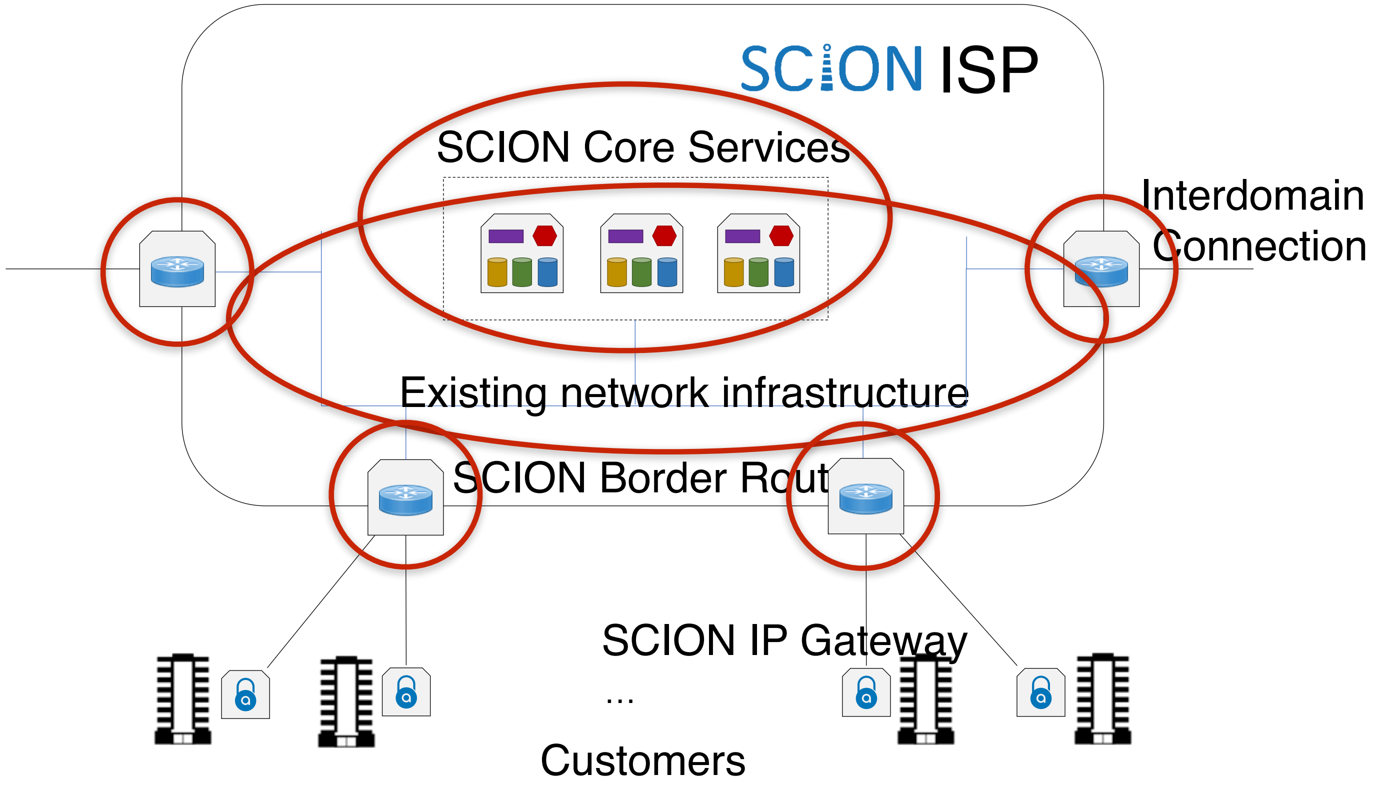


Use Case: Internet Sovereignty

- Isolation Domains (ISD) guard Internet against external influence
- Per-ISD trust roots remove dependence on external roots of trust
- Enables clean trust scoping
- Provides transparency on which entities need to be trusted in any verification

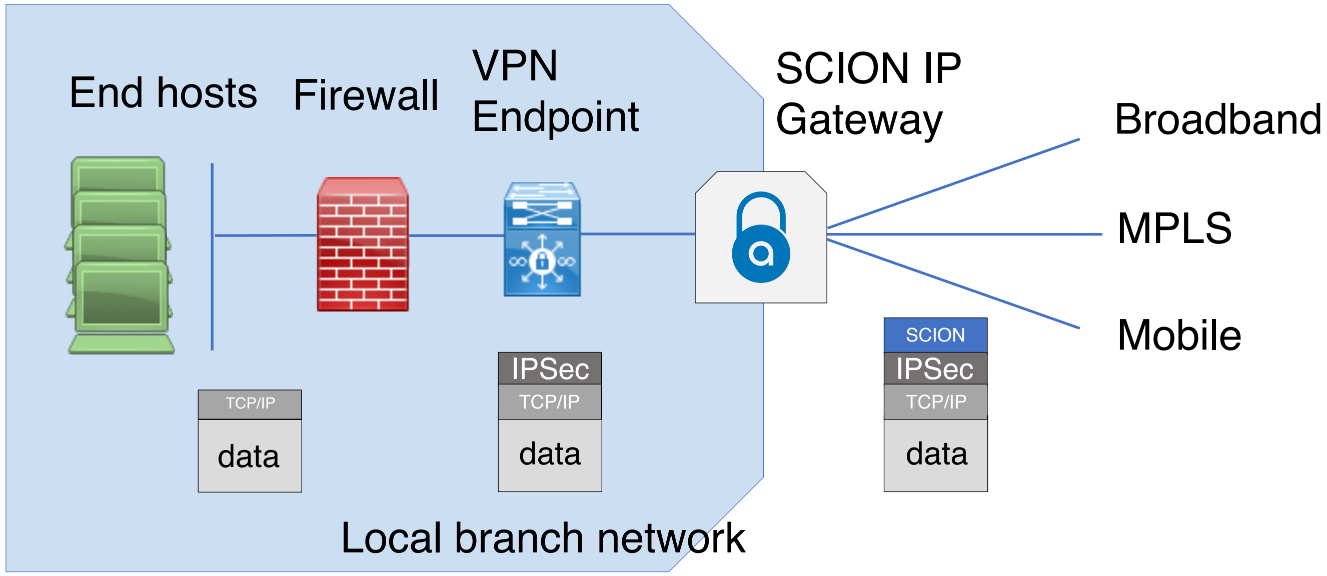


How to Deploy SCION – Core Network



- 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

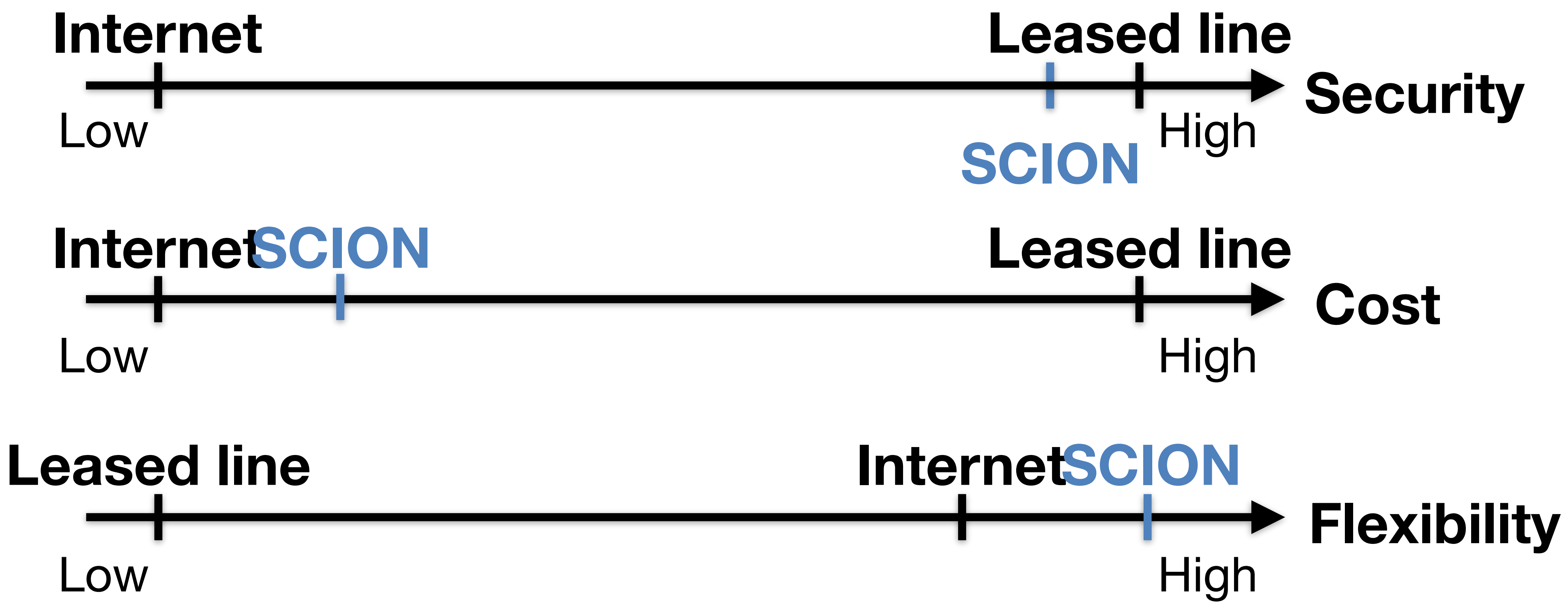
How to Deploy SCION – End Domains



- 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 underlaying networks

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
- Lower network management overhead
- Increased network capacity utilization

Current Deployment Status

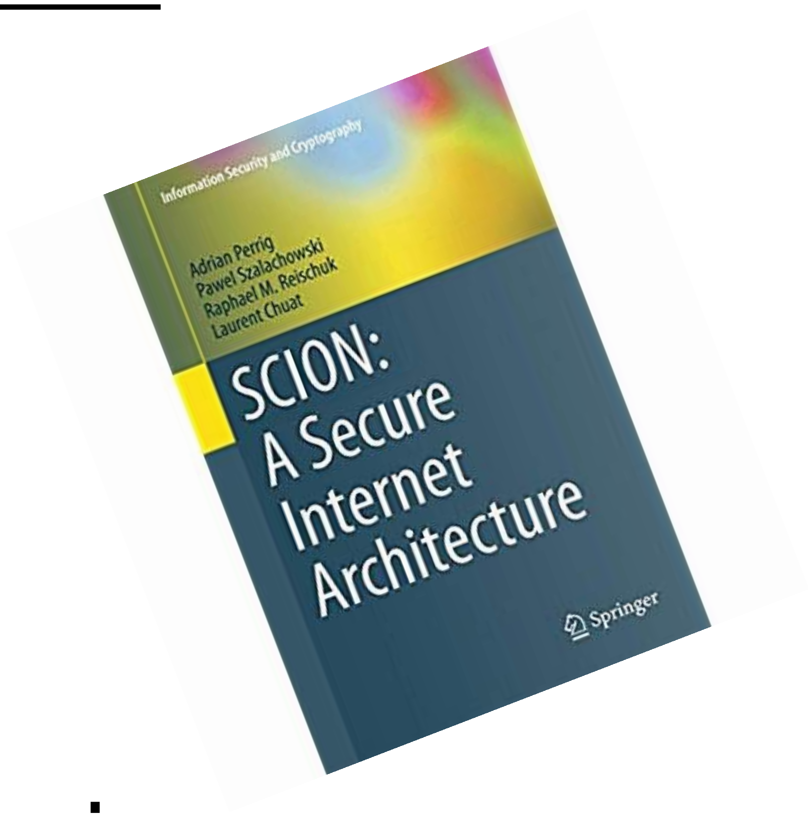
- Commercial Network (Anapaya)
  - ISPs: Deutsche Telekom, Swisscom, SWITCH, Init7
  - Bank deployment: 4 major Swiss banks, some in production use
  - Swiss government has SCION in production use

BGP FREE

- Research Network (SCIONLab)
  - ISPs: Swisscom, SWITCH, KDDI, GEANT, DFN
  - Korea: KISTI (KREONET), KU, KAIST, ETRI
  - Deployed 50 ASes worldwide
  - Global interest, e.g., ESA

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



Conclusion: SCION is a disruptive technology that we can use today

- Clean-slate Internet architecture built on solid security foundations
- New security properties:
  - Geofencing
  - Verified protocols and code
- Improved communication efficiency
  - Increased bandwidth via multipath communication
  - Decreased latency thanks to path optimization
  - Fast failover using backup paths

SCION

Scalability, Control, and Isolation on Next-Generation Networks