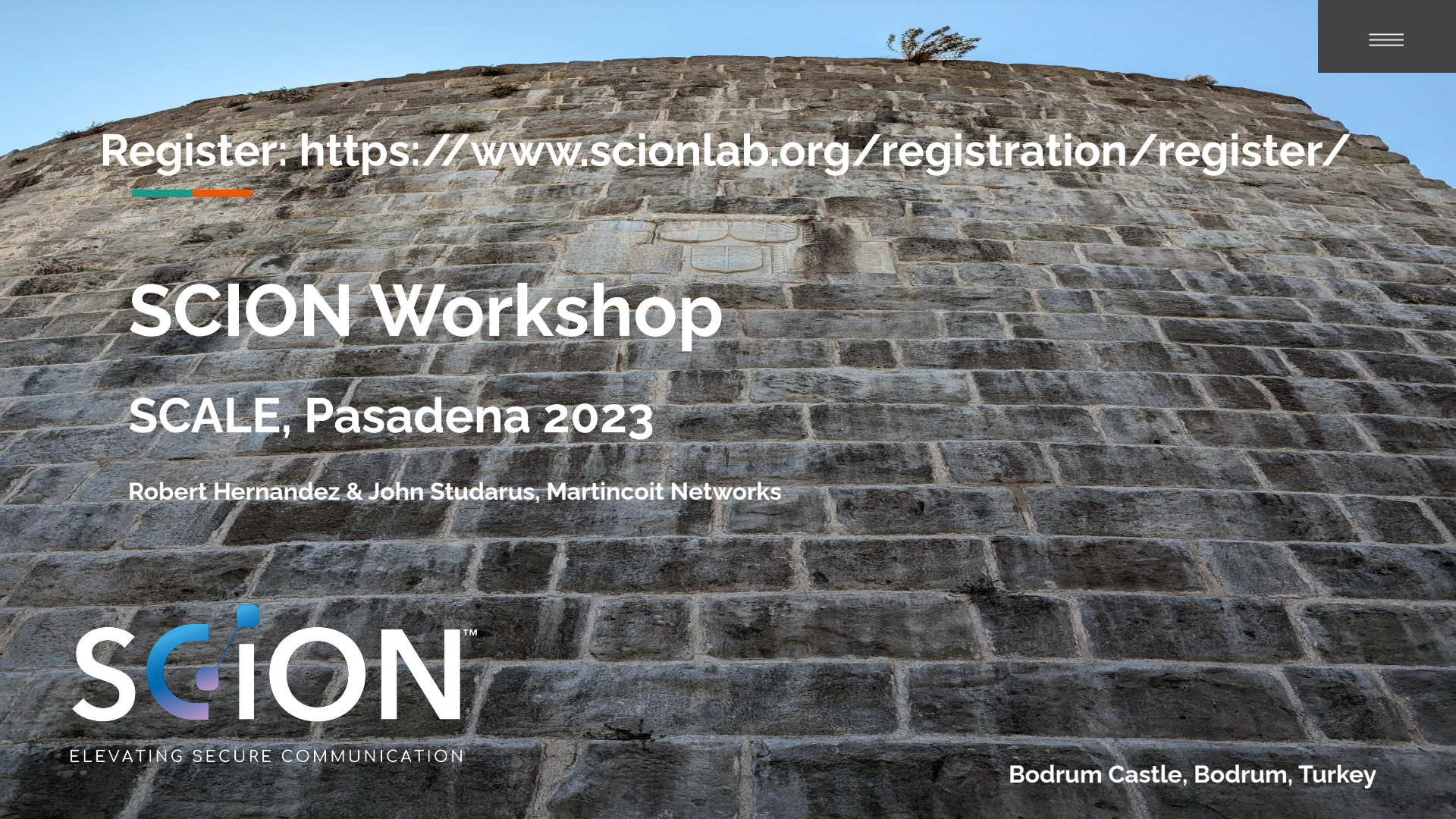

Register: https://www.scionlab.org/registration/register/
SCION Workshop
SCALE, Pasadena 2023
Robert Hernandez & John Studarus, Martincoit Networks
SCION™
ELEVATING SECURE COMMUNICATION
Bodrum Castle, Bodrum, Turkey

Workshop Agenda

SCION Brief

- Technology/Benefits/Addressing
- Deployments

Hands On - SCIONLab

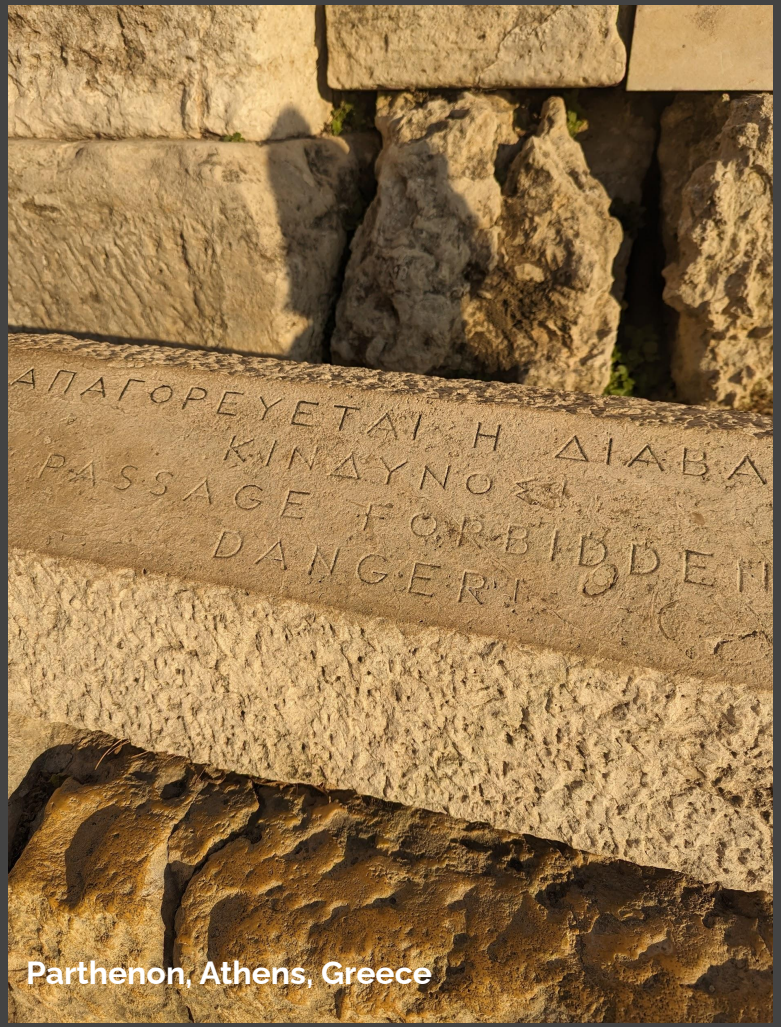
- Your own “AS” on a larger global network
- Play with path selection and sample applications

Hands On - “Free Standing”

- A complete 5 AS self-contained ecosystem

Forward Looking

- Platform for future productions and solutions



Parthenon, Athens, Greece

Martincoit Networks

Next Gen Network Engineering

- Utilizing secure network protocols
- Network design
- System engineering (Linux/VM)
- Application porting (Go)

Our Customers

- Data Centers & ISPs
- Financial Services
- Crypto/Blockchain

Our Technology

- SCION (replaces BGP)
- Path Aware Networking (PAN)
- Network Analysis

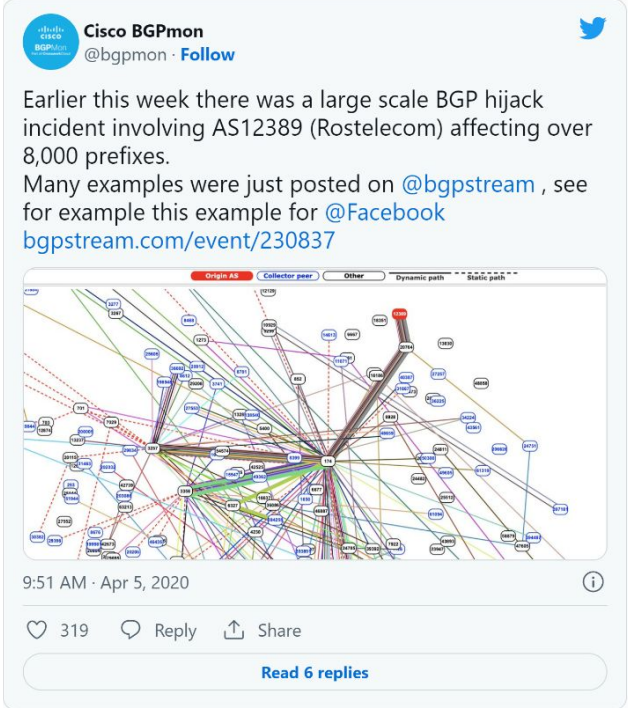
BGP Hijacking

Network Control Threat

"Russia And China 'Hijack' Your Internet Traffic: Here's What You Do", Forbes, April 2020

"Who's reading your email?", Design World, June 2022. China intercepted traffic via BGP hijacking 2010, 2016, and 2017 (6 weeks) in Netherlands, Sweden, Italy and Denmark.

Implications:
Network traffic hijacking is real and has been happening for years. BGP has long been a weak point of the Internet.



Malicious TLS CA

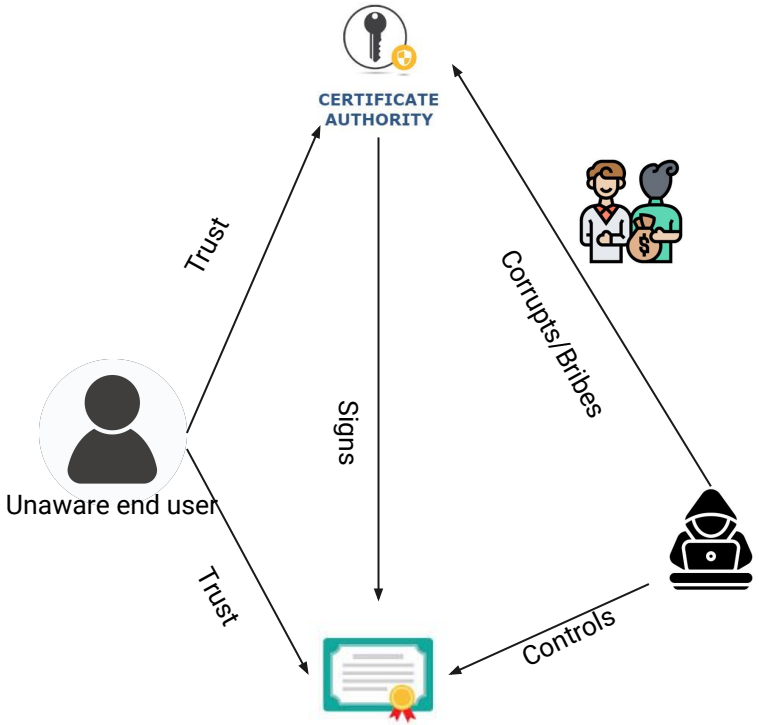
Trust of Certificate Authorities

A Certificate Authority (CA) issue a digital certificate (TLS).

Corrupt CAs have been used by hackers to generate bogus digital certificates. Since the end users trust the CA and the certificate is signed by the CA, the end user thus trust these bogus certificates.

KlaySwap crypto users lost **$1.9M** funds after a combined BGP hijack and bogus TLS certificate issued by malicious Certificate Authority.

Implications:
Organizations should no longer trust arbitrary DNS registrars and TLS Certificate Authorities across the Internet. SCION allows the users to determine which CAs to trust.



Bogus certificate trusted by user installed on malicious website.

Digital Sovereignty through SCION

Digital sovereignty is a key idea in the internet age — **the idea that parties must have sovereignty over their own digital data**.

Given today's geopolitical conflicts, nations would like a whole ecosystem of products to promote digital sovereignty which can be accomplished SCION connectivity.

SCION: Addressing Internet Issues of today

1. **Control**. Who controls which networks your data will traverse? Untrusted entities control your packets destiny. Owners of data must be able to control where data flows.

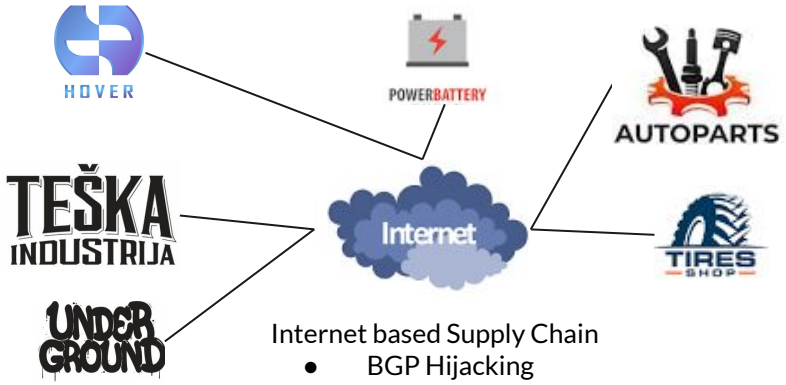
2. **Transparency**. Do you know which path your data has traversed? Packet Carried State cryptographically guarantees the route data traverses.

3. **Availability**. BGP route convergence, misconfiguration, single route options, and hijacking impact WAN availability. Path Aware Networking allows for path resiliency reducing outages.

4. **Trust**. DNS and TLS PKS rely upon over 1000 roots of trust. Do you want to trust them all? SCION ISD (Isolation Domains) allow users and domains to select who they trust.

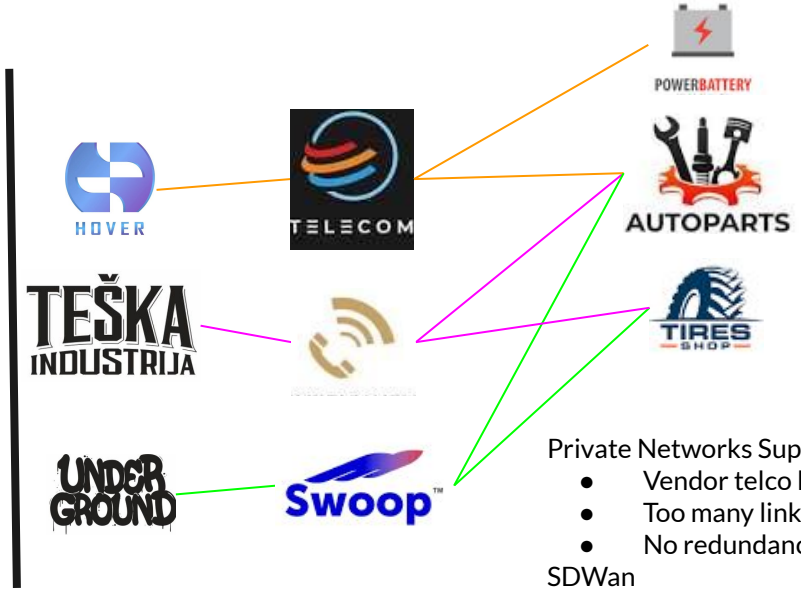
Manufacturing Cyber Security Nightmare

Factories are dependent on their parts suppliers! Network security & resilience is key.



Internet based Supply Chain

- BGP Hijacking
- DDoS attacks
- Limited resilience
- Slow failure recovery
- No isolation



Private Networks Supply Chain (MPLS)

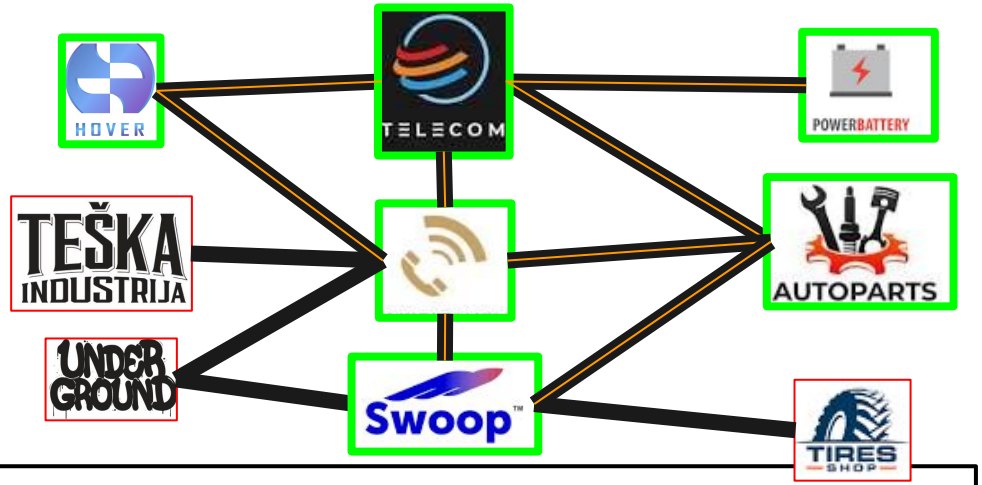
- Vendor telco lockin
- Too many links $$
- No redundancy to edge

SDWan

- Above + Internet risks!

Cloud Methodology to Global Networking

Imagine applying cloud principles to global networking.



- Purchase connectivity from any telco! Just like an Internet connection.
- Purchase multiple for resilience. SCION protocol intelligently routes across all paths.
- No vendor lock-in! Select your SCION connect from multiple ISPs.

Global VPC - Virtual Private Cloud
- Segment to just trusted business partners

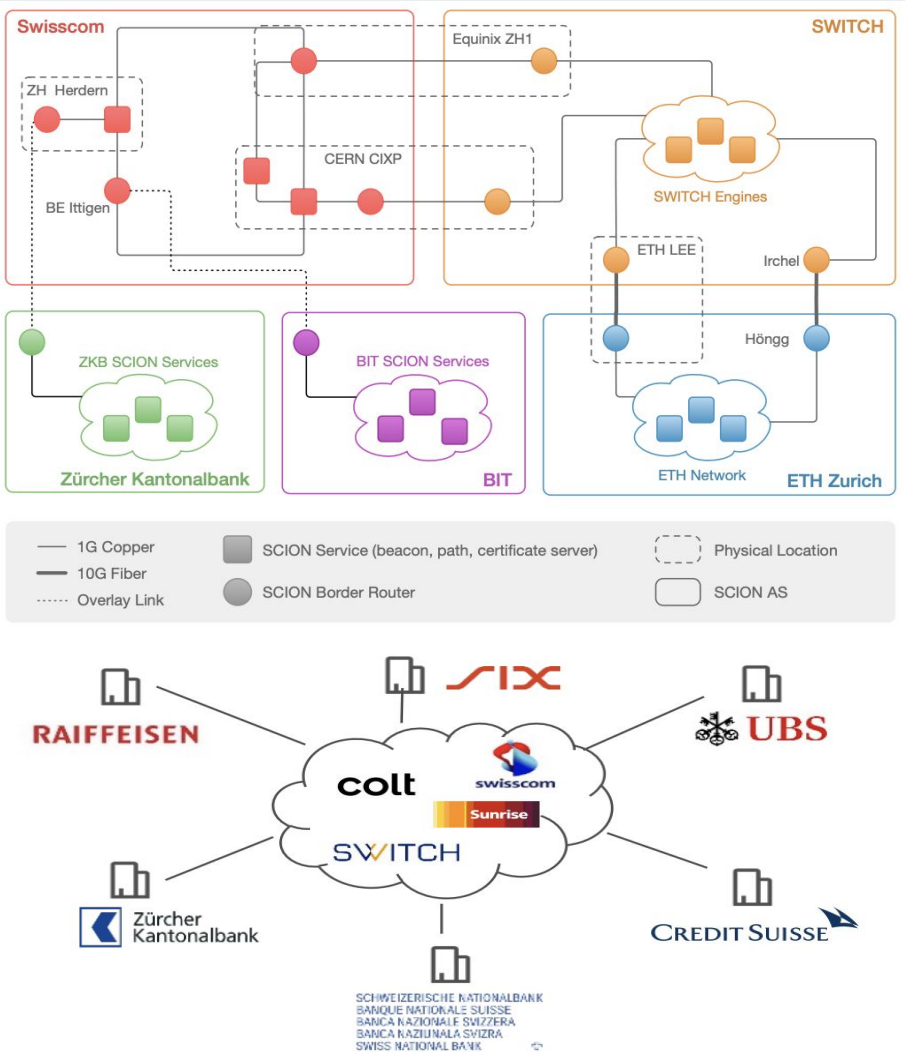
Multiple ISP Selection
- Improved reliability
- Removes provider lockin

Per socket path selection by:
- Region - Geopolitical
- Performance - Latency, Packet loss, Bandwidth
- Price

Modern Protocols. Immunity from:
- BGP Hijacking
- DDoS attacks

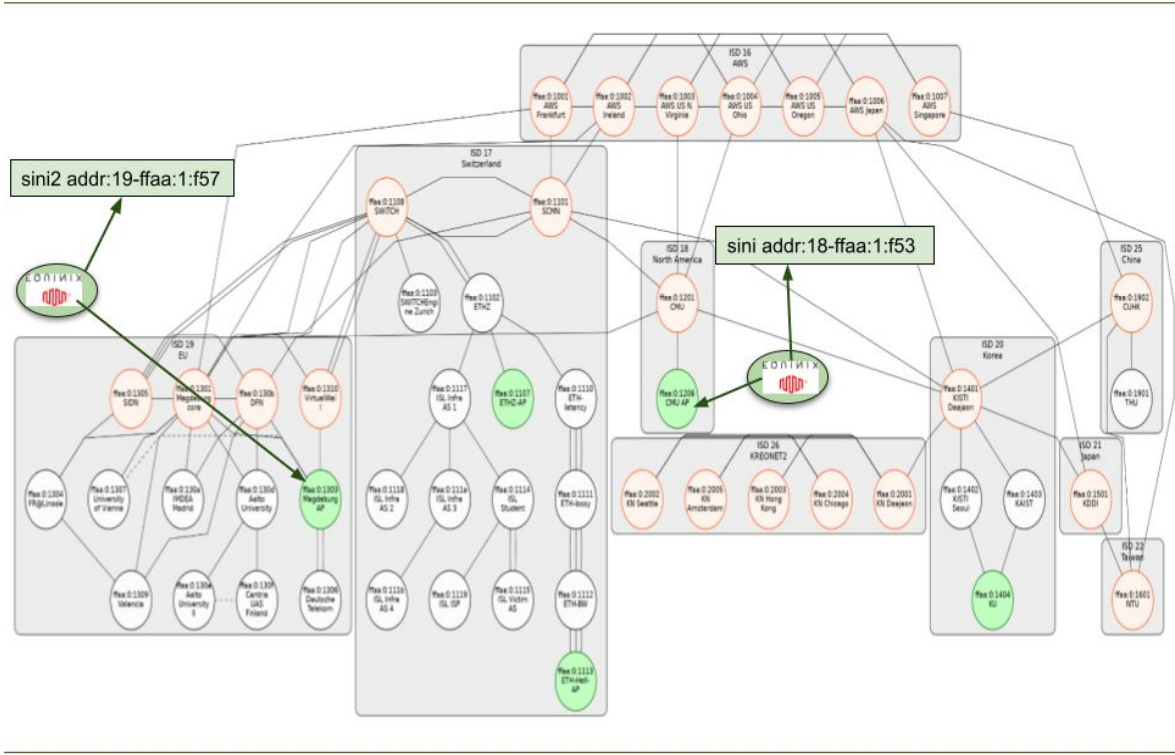
SCION in Production

- SCION in production use since August 2017
- ISPs
  - Swisscom
  - SWITCH
  - Colt
  - Sunrise
- Customers (Banking)
  - SIX
  - RAIFFEISEN
  - UBS
  - CREDIT SUISSE,
  - Zürcher Kantonalbank



SCIONLab for Research

- SCION-Lab
  - Global testbed available for all
- INI on SCION-Lab
  - sini.martincoit.net 19-ffaa:1:f57
  - sini2.martincoit.net 18-ffaa:1:f53
- Equinix Infra
  - Hardware provided by Equinix Metal
  - Utilizing data centers in FRA & IAD
  - Connected to NA & EU ISDs



Hands On Workshop - SCION Lab

http://bit.ly/SCALE21X-SCION

Which of these is a valid SCION address?

A) A:24-5
B) #8,404
C) 17-4:0:2b
D) +9-505
E) 867-5309

What is an ISD?

A) Information Security Digest
B) Isolation Domain
C) Isovalent System Delivery
D) Insecure Solution Division

What does an ISD represent?

A) High Level Geo Political Trust Domain
B) Low Level Government Entity
C) Self Funded Government Group
D) Commercially Funded Organization

What is one preference that would not make sense for path selection?

A) Latency
B) Color
C) Energy Use
D) Bandwidth

Making Applications “SCION Aware”

```
flag.BoolVar(&interactive, "i", false, "Interactive path selection, prompt to ch
flag.StringVar(&sequence, "sequence", "", "Sequence of space separated hop predi
flag.StringVar(&preference, "preference", "", "Preference sorting order for path
        "Comma-separated list of available sorting options: "+
        strings.Join(pan.AvailablePreferencePolicies, "|"))

flag.Parse()
policy, err := pan.PolicyFromCommandline(sequence, preference, interactive)
```

pan.PolicyFromCommandLine() : Choose path interactively based on route sequence, preference.

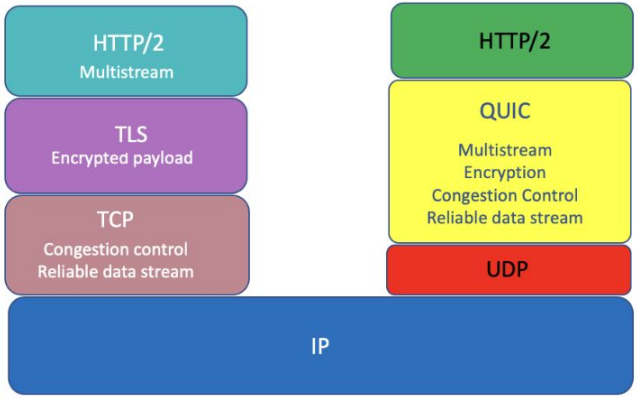
```
addr, err := pan.ResolveUDPAddr(serverAddress)
if err != nil {
        fmt.Println("server address error")
        return
}
//Select path to control connection
pathSelector := pan.NewDefaultSelector()
// garnish connect to the server
conn, err := pan.DialUDP(context.Background(), netaddr.IPPort{}, addr, policy, pathSelector)
if err != nil {
```

pan.ResolveUDPAddr() : resolve server’s SCION address (e.g. 17-ffaa:1:1,[127.0.0.1]:12345)

Default Selector will keep using the current path, starting with the first path chosen by the policy.

Set a connection between Garnish and Origin Server based on the path selection policy set by the user

Code examples/diff enabling SCION QUIC



QUIC is a reliable transport protocol that refines the basic operation of IP's TCP.

```
session, err := pan.DialQUIC(context.Background(), netaddr.IPPort{}, addr, nil, selector, "", tlsCfg, nil)
if err != nil {
        return err
}
for i := 0; i < count; i++ {
        stream, err := session.OpenStream()
```

pan.DialQUIC() : Establish a new QUIC connection (session) to a server at the remote address.

OpenStream(): use streams of bytes that can be read from or written to

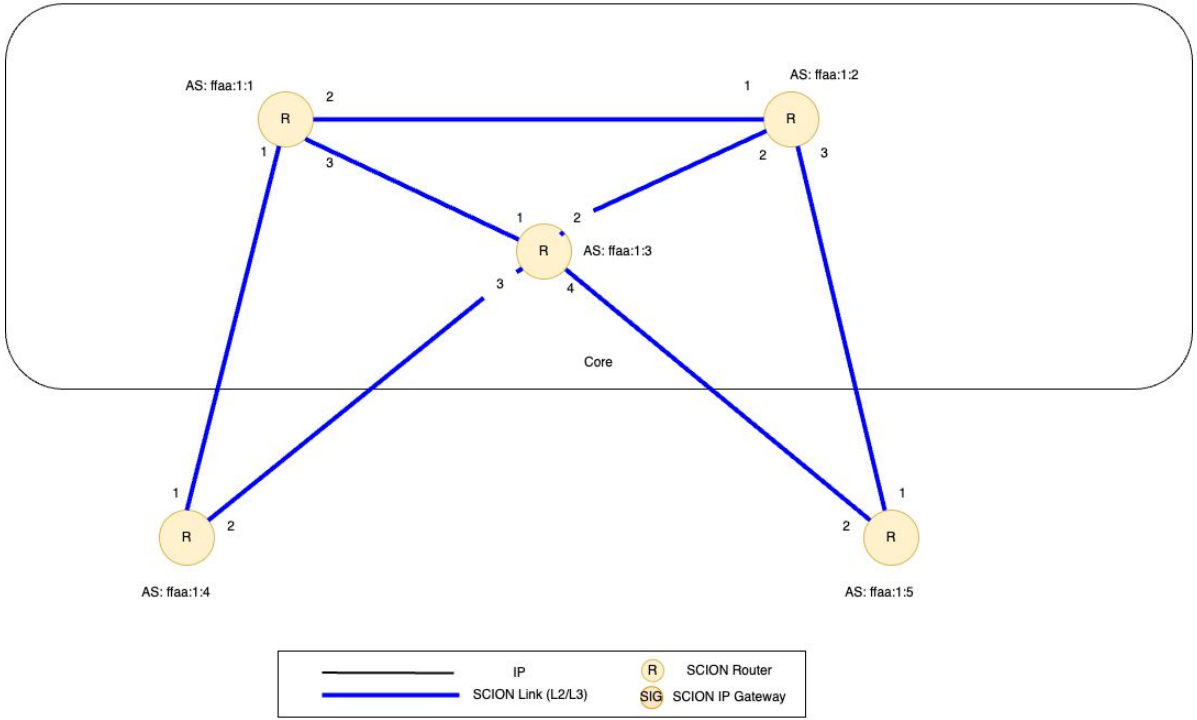
```
func runServer(listen netaddr.IPPort) error {
        tlsCfg := &tls.Config{
                Certificates: quicutil.MustGenerateSelfSignedCert(),
                NextProtos:   []string{"hello-quic"},
        }
        listener, err := pan.ListenQUIC(context.Background(), listen, nil, tlsCfg, nil)
```

MustGenerateSelfSignedCert(): generates private key and a self-signed certificate. // certificate usable for TLS with InsecureSkipVerify: true.

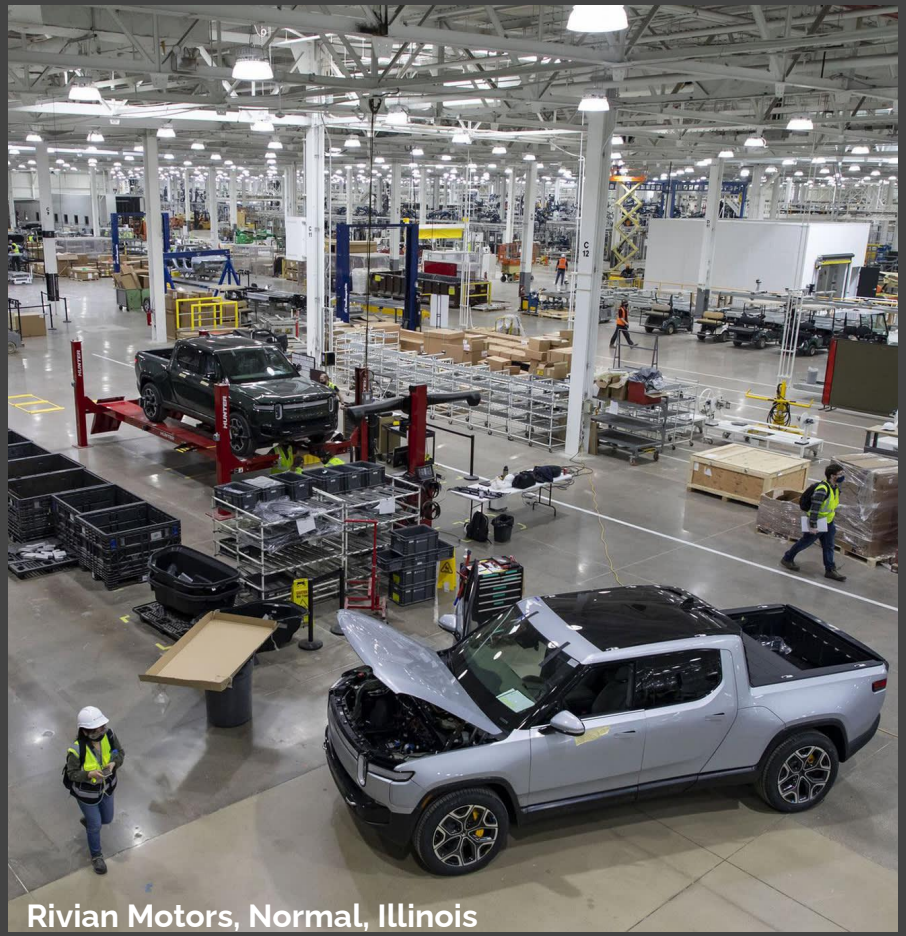
Tutorial: Freestanding Deployment

Full “Stand Alone” environment.
5 “AS” - 3 Core & 2 Child.
Can be VM, bare metal, etc…

See Worksheet for tech details.




MARTINCOIT
Networks


Rivian Motors, Normal, Illinois

Manufacturing Case Study

Global Supplier Networks

Global addressing cross networks
Single global point of failure (business & operationally)
SCION networks around trade associations

NATS Project Goal

Port an existing open source message bus over to SCiON to explore the benefits of Path-aware Networking (PAN) using SCiON.

Realm of the Possible

Network policy aware NATS message bus queues
Data security policies applied to network via NATS

Results

Improved NATS network reliability
Data security policies implementable in NATS

Thank you.