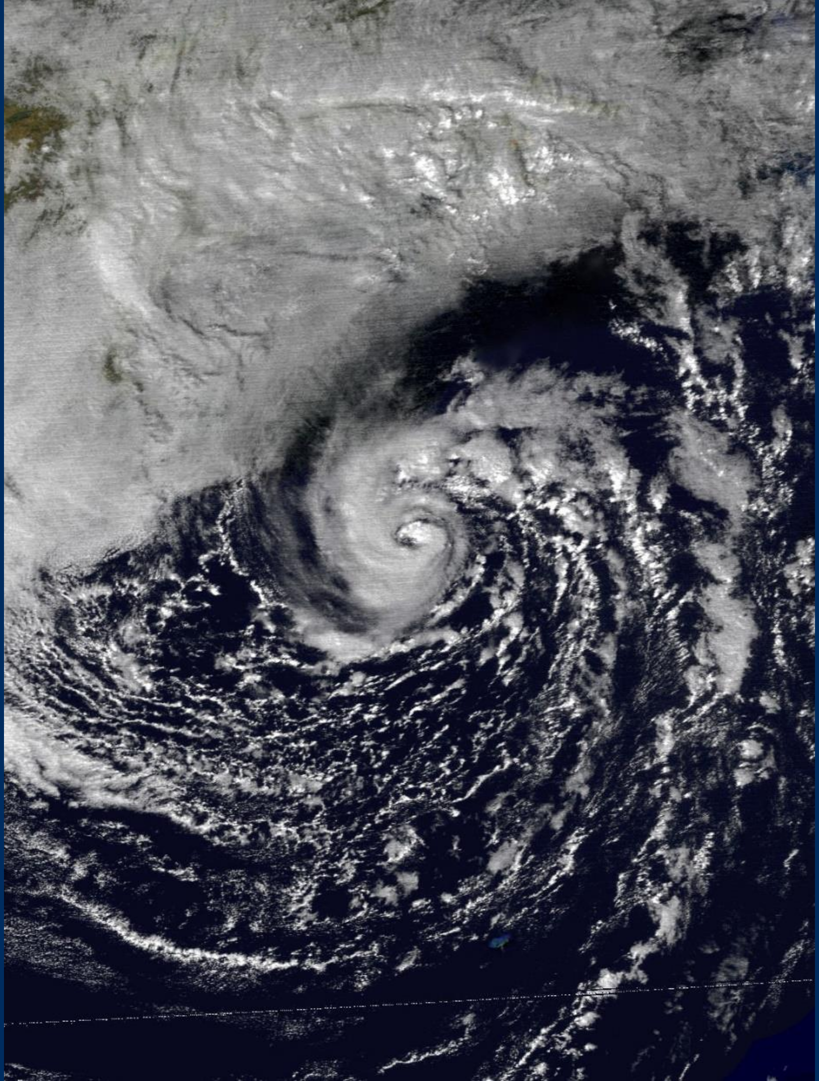
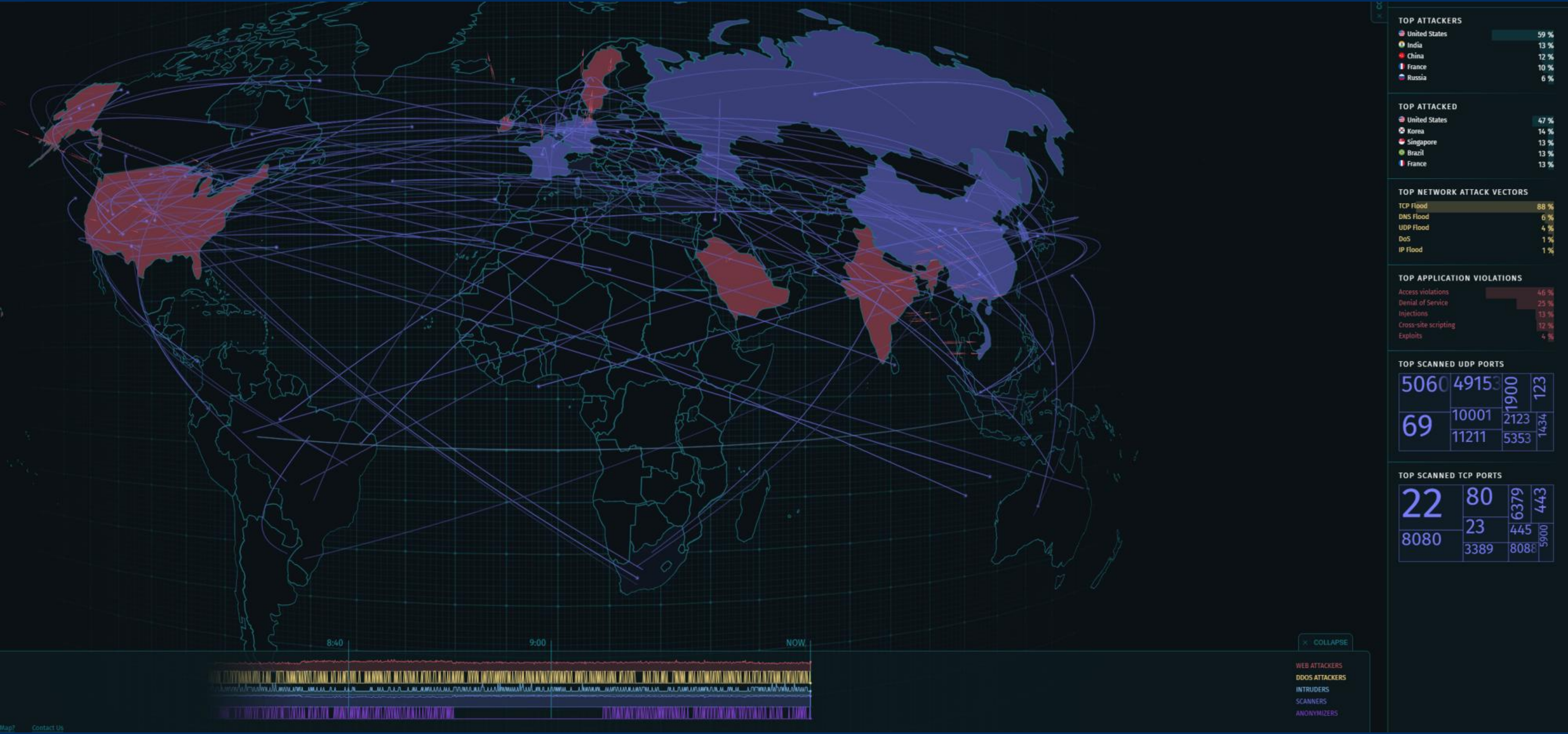
Weathering The Cyber Security Storm

Fritz Steinmann, SIX
07 September 2022





TOP ATTACKERS

United States	59 %
India	13 %
China	12 %
France	10 %
Russia	6 %

TOP ATTACKED

United States	47 %
Korea	14 %
Singapore	13 %
Brazil	13 %
France	13 %

TOP NETWORK ATTACK VECTORS

TCP Flood	88 %
DNS Flood	6 %
UDP Flood	4 %
DoS	1 %
IP Flood	1 %

TOP APPLICATION VIOLATIONS

Access violations	46 %
Denial of Service	25 %
Injections	13 %
Cross-site scripting	12 %
Exploits	4 %

TOP SCANNED UDP PORTS

5060 49153 1900 123 69 10001 11211 2123 5353 1434

TOP SCANNED TCP PORTS

22 80 6379 443 8080 23 445 5900 3389 8088

IRAN
AFGHANISTAN
PAKISTAN
Baluchistan
Quetta
Faisalabad
Lahore
Ludhiana
Multan
Delhi
New Delhi
Jodhpur
Jaipur
Agra
Karachi
Hyderabad
Rann of Kutch
Gwalior
Kanpur
Lucknow
Allahabad
Varanasi
Patna
Ahmadabad
Jabalpur
Indore
Surat
Nagpur
Nashik
Mumbai
Pune
Raipur
Ranchi
Asansol
Jamshedpur
Kolkata
Dhaka
BANGLADESH
BHUTAN
Guwahati
Dibrugarh
Chittagong
MYANMAR (BURMA)
INDIA
CHINA
Chengdu
Neijiang
Chongqing
Nanchong
Guiyang
Lanzhou
Xining
Qamdo
Dubai
Abu Dhabi
U.A.E.
Muscat (Masqat)
Gulf of Oman
OMAN
Arabian Sea
Bandar-e'Abbas
Shiraz
Kerman
TURKMENISTAN
SE
SW
W
NW
N
NE
E
S
140
160
180
200
220
240
260

Top Five Cyber Security Risks

Source: Swiss NCSC Semi-annual report 2021/2

Vulnerabilities

Phishing

Fraud

DDoS

Malware

SCION

Scalability, Control and Isolation on Next-Generation Networks

Cyber Security – Three Risks Prevail When Using the Internet for Communication

DoS and DDoS Attacks

- Expensive and difficult to protect against DoS und DDoS attacks
- Despite large investments, attacks continue to be successful

Communication Path Hijacking

- Sender und receiver have limited control over routing
- Attacks can hijack and relay paths

Kill Switch ruptures Sovereignty

- Current Internet suffers from several "Kill Switches", which can halt communication within a geographical area
- Several attack avenues exist
- Revocation of certificates is also possible

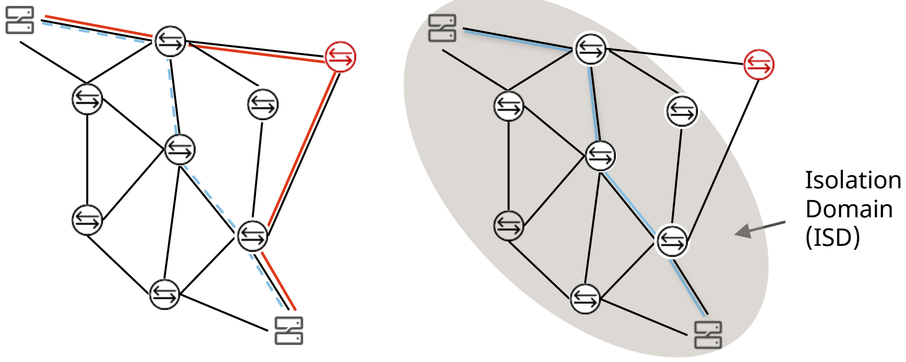
SCION – a Network Architecture for Safe and Reliable Data Communication

Avoiding undesired network paths

- Internet at present: Impossibility to avoid certain networks or geographic regions due to lack of route controls
- SCION architecture: Path defined by end-users; cryptographic path protection prevents re-routing

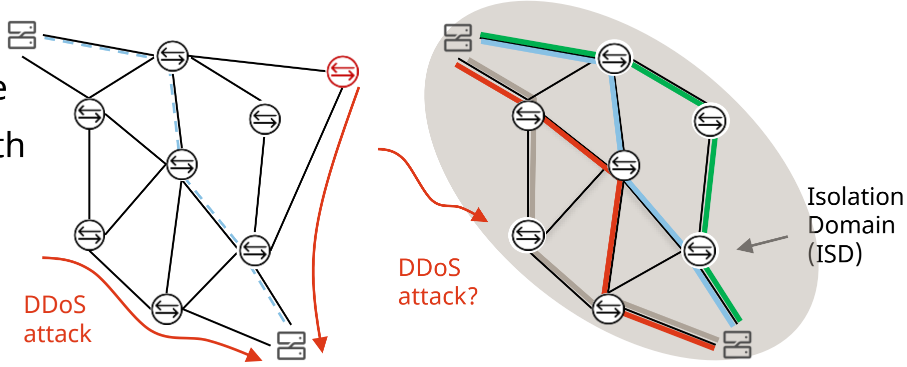
Internet at present

SCION architecture



Preventing DDoS with isolation domains (ISDs)

- Internet at present: End points are vulnerable
- SCION architecture: Addresses are shared with selected communications partners only;
  a DDOS attack from the internet can thus no longer penetrate through to these addresses



SSFN

Secure Swiss Finance Network

Together with partners, SIX introduced SSFN as the new financial communication network

Under the leadership of SIX the project brought together a dedicated team of **partners**

- **SIX** (Project Lead)
- **SNB** (Manager Swiss Interbank Clearing [SIC])
- **Anapaya** (Commercial SCION Technology)
- **Sunrise, Swisscom & SWITCH** (Partners for **connectivity**)

Three banks actively participated in the **pilot**

Active **collaboration** in the project

- Set-up a pilot network and performed testing using test traffic
- Defined governance principles
- Identified and partially tested use cases for SSFN or SCION-based networks beyond SIC / euroSIC
  - SSFN: Most SIX services
  - SSFN: "Secure" connection between banks
  - SCION: Working from home or eBanking

SSFN went live in November 2021, SIC uses SSFN productively since June 2022. SSFN will replace the current network in the medium term due to its superior flexibility and functionality

SCION / SSFN Benefits

- High “native” resilience and availability
- Fast failover
  - Current routing setup and protocols can take seconds to minutes to failover
  - Due to known health states on each network path segment failover in SCION is in the milliseconds
- Identified participants due to cryptographically signed path elements
- Vendor and carrier agnostic
- Overall network policy enforcement possible

ETHZ – SCION + SIX – SSFN = Private-Public Partnership

Joint efforts and exchange

- SIX became an ETH Zurich Information Security Center (ZISC) partner in 2016
- First SCION workshop in April 2017
- Pilot SCION setup at SIX in 2018
- SSFN project start in 2019
- SSFN pilot with banks in 2020
- SSFN go-live in 2021
- Swiss Interbank Clearing production traffic in 2022

Resources

SIX

Hardturmstrasse 201
CH-8021 Zürich

www.six-group.com

SCION:
www.scion-architecture.net
www.scionlab.org
www.github.com/netsec-ethz

SSFN:
www.six-group.com/ssfn
www.six-group.com/en/newsroom/magazines/pay.html