2STiC programme

Security, stability and transparency of inter-networking communication

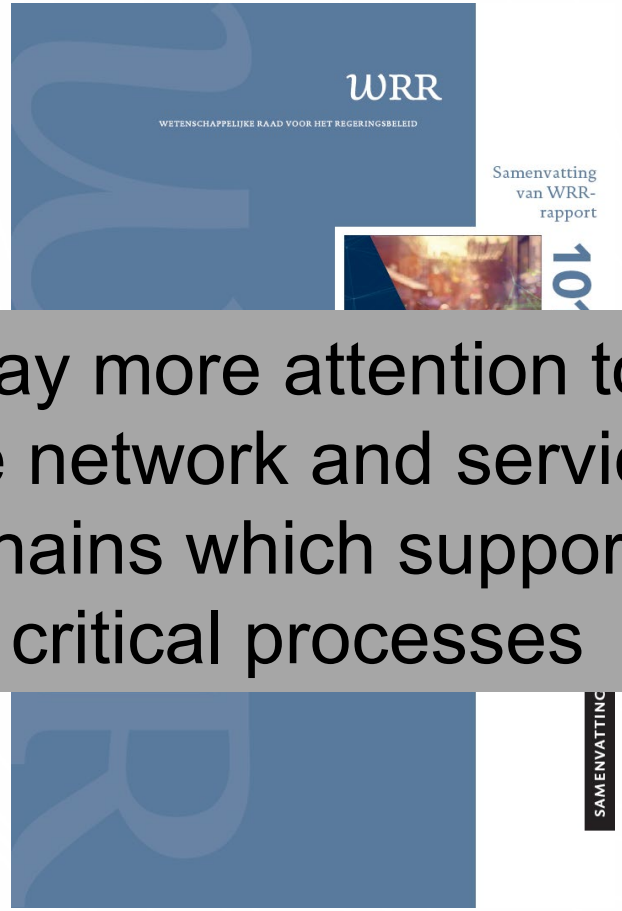
Victor Reijs (SIDN Labs) and Caspar Schutijser (SIDN Labs)

WWW.2STiC.NL

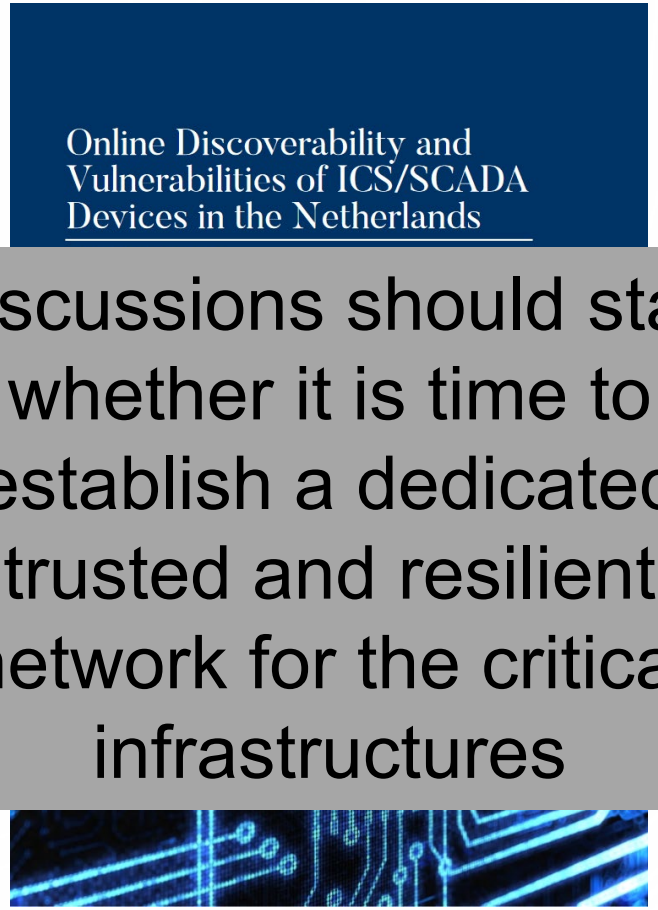
Outline

- General
  - Lessons learnt from present IP environment
  - 2STiC programme
- 2STiC activities
- Q&A and discussion

Recent reports



Pay more attention to the network and service chains which support critical processes



Discussions should start whether it is time to establish a dedicated trusted and resilient network for the critical infrastructures

Threat examples

Stability

Security

Distributed malware attacks Dyn DNS, takes down websites in US

Written by Wikinews, Oct

Monday, October 24, 2016

The third attack distribution as
provided by downdetector.com
and OpenStreetMap.

On Friday, a network of diverse
domain registration service pr
several popular websites such
Times, and *Wired*.

The attack involved targeting

'Nog eens honderden bedrijven onbeveiligd door lek in VPN-netwerk'

edenen niet bekendgemaakt. Het
beursgenoteerd bedrijf.

For two hours, a large chunk of European mobile traffic was rerouted through China

It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western countries."

By Catalin Cimpanu for Zero Day | June 7, 2019 -- 19:41 GMT (20:41 BST) | Topic: Security

MORE FROM CATALIN CIMPANU

Security
Bitpoint cryptocurrency exchange hacked for $32 million

Security
US mayors group adopts resolution not to pay any more ransoms to hackers

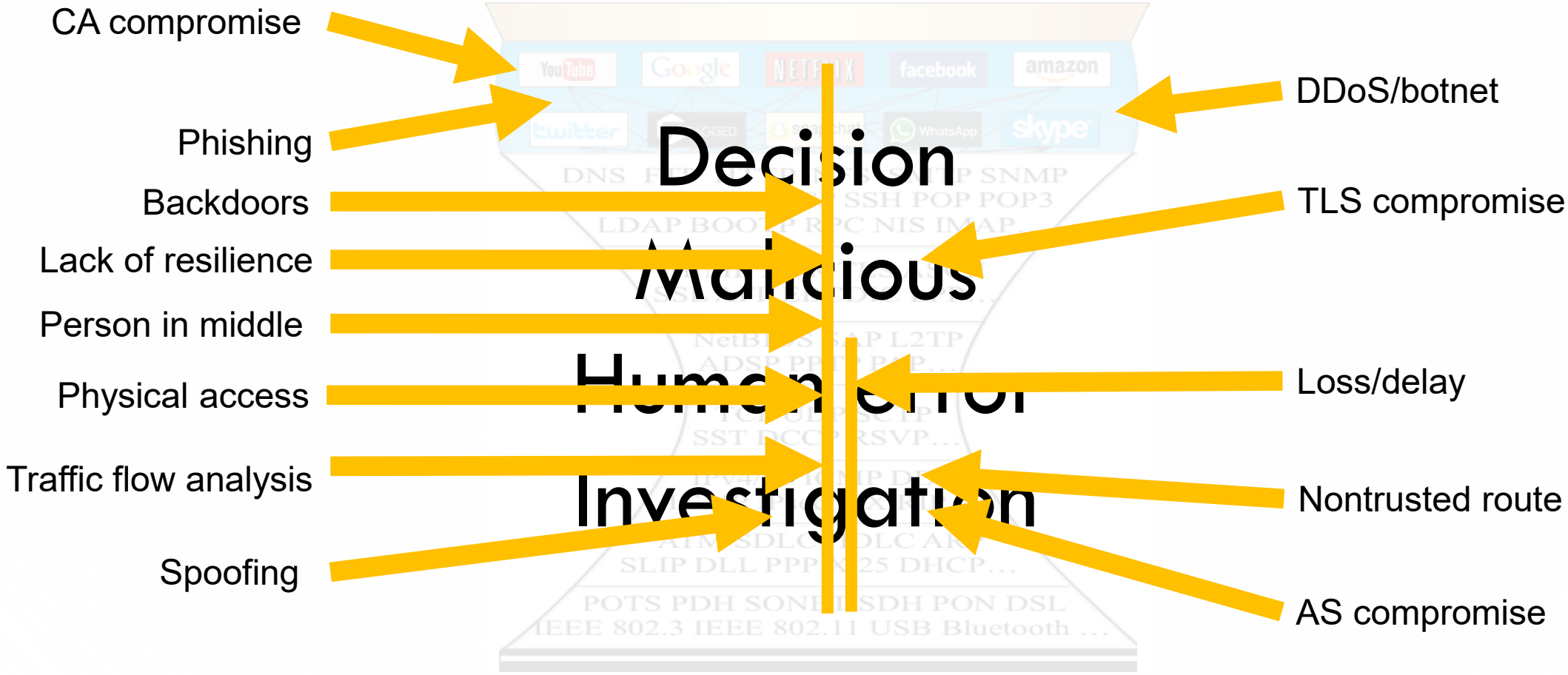
Security
German banks are moving away from SMS one-time passcodes

Security
Recent Windows zero-day used by Buhtrap gang for cyber-espionage

NEWSLETTERS

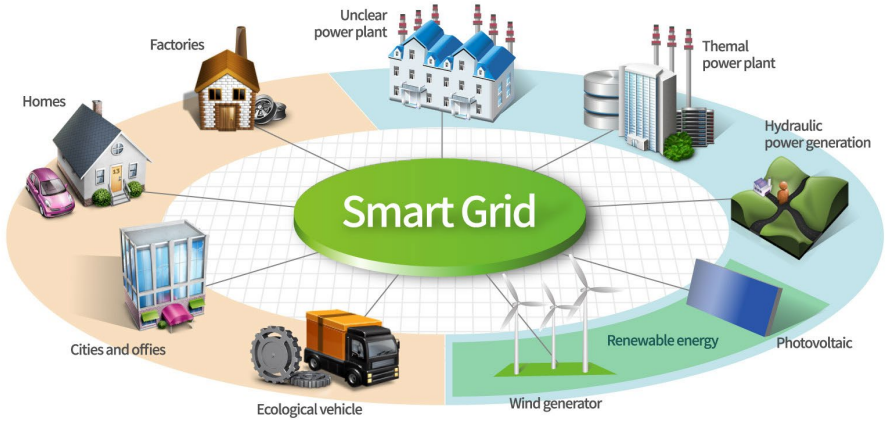
Transparency

Threats


CA compromise
Phishing
Backdoors
Lack of resilience
Person in middle
Physical access
Traffic flow analysis
Spoofing
DDoS/botnet
TLS compromise
Loss/delay
Nontrusted route
AS compromise
Decision
Malicious
Human error
Investigation

Lessons learnt over 50 years

- The Internet has come a long way: from small computer network to worldwide social environments
- QoS, scope, security, content delivery and mobility were though not part of initial Internet design



Several approaches to progress this

- Add functionality to Internet
  - Compatibility is easy
  - Unknow effects of add-ons on security and transparency
- Investigate more fundamental approaches
  - Include lessons learnt over 50 years
  - Transition is difficult, but easier for niche applications
- 2STiC programme will look at both in a practical approach…

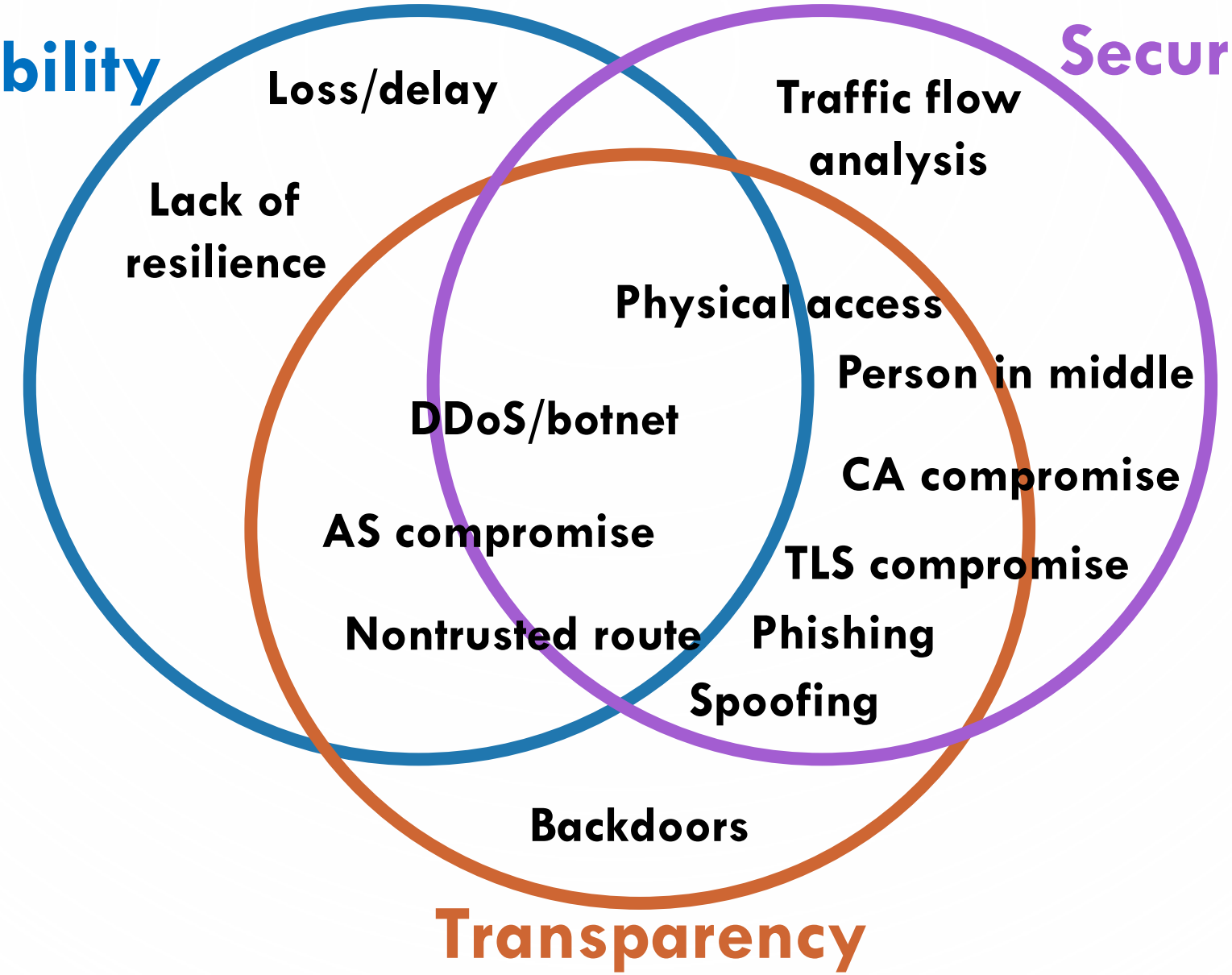
2STiC programme

Put Dutch and European internet communities in leading position of secure, stable and transparent inter-network communication

UNIVERSITY OF AMSTERDAM

UNIVERSITY OF TWENTE.

Security, stability and transparency are key



Motivations for 2STiC programme

- New applications need new security, resilience and transparency requirements
  - More interaction with physical space (e.g., transport, smart grids, drones, remote surgery)
  - More insight in and control over who processes their (user) data
- Meet requirements through (multiple) shared internets
  - Applications will increasingly require ubiquitous computing and networking
  - Operating dedicated infrastructure might have less value for money
- Open programmable network equipment become commercially available
  - Data plane and control plane programmability

Basic approach of 2STiC programme

- Act as an expertise centre
- Coordinate grant proposals
- Include multi-domain, governance, trust and deployment aspects from the start
- Evaluate future internet architectures that have active communities with testbeds and use open source code
- Focus on realistic/practical use cases and demonstrators

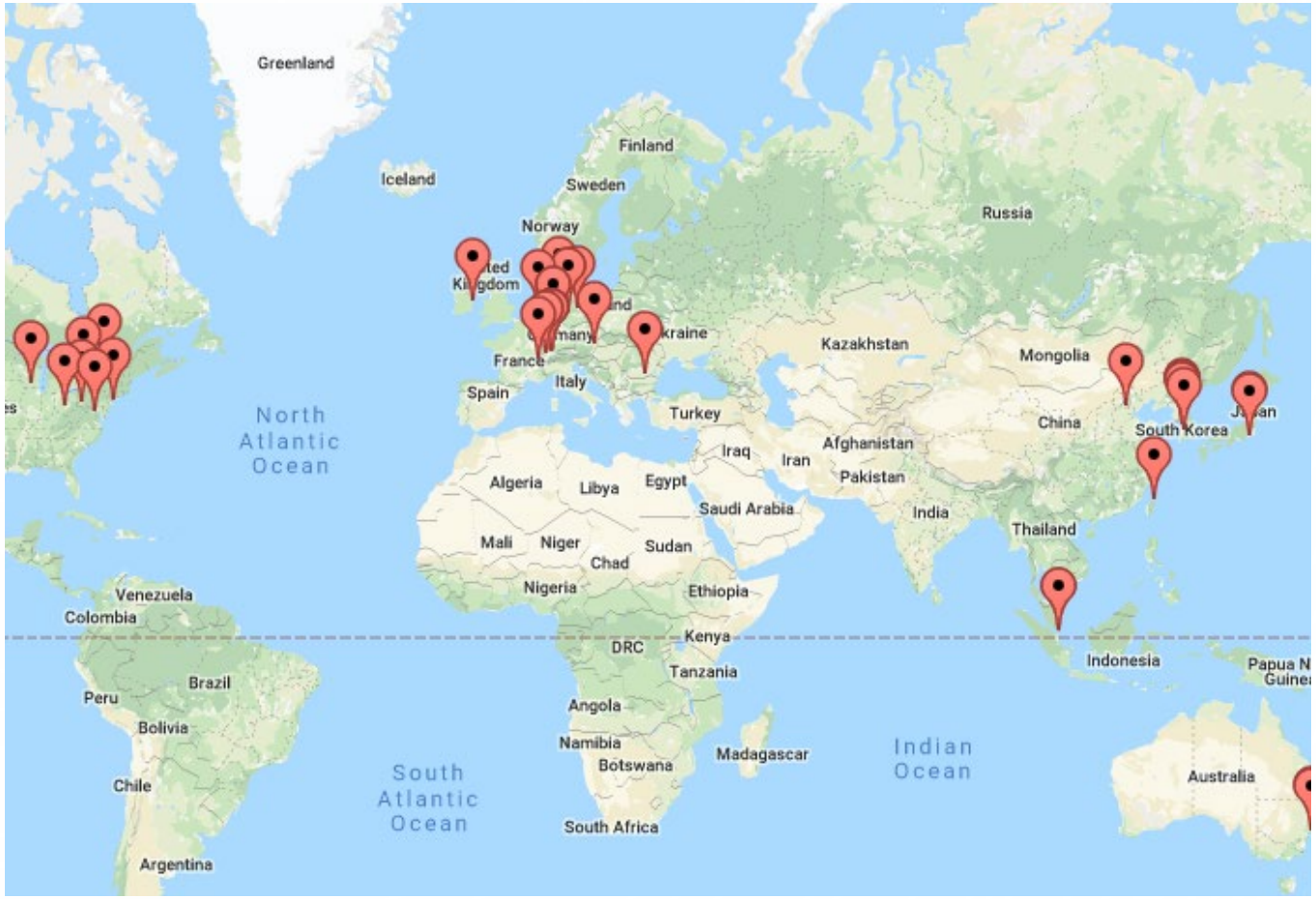
2STiC activities

Future internet architectures

- Current and past initiatives:
  - EC funded: Future Internet Research and Experimentation (FIRE), Next Generation Internet (NGI)
  - USA funded: NSF Future Internet Architecture
- Selection criteria:
  - Security, stability, transparency
  - Active
  - Open
- SCION, RINA, NDN

SCION

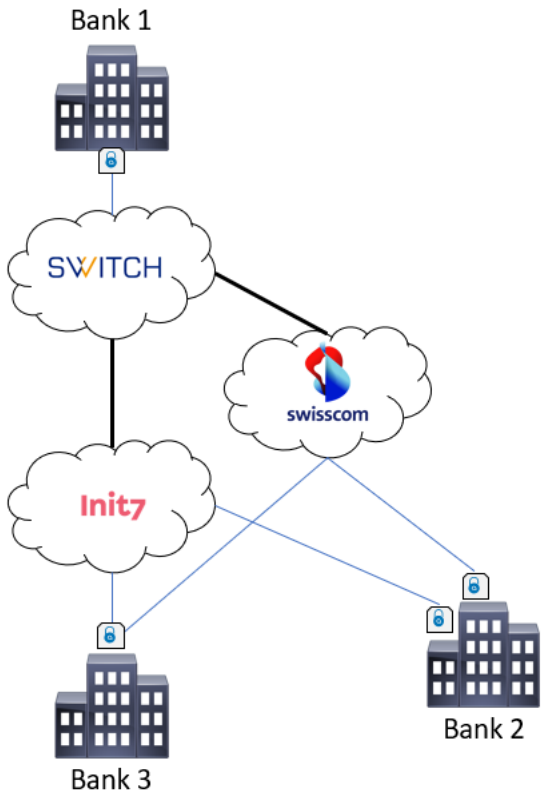
- SCION: Scalability, Control, and Isolation on Next-Generation Networks
- Network security group at ETH Zurich
- Goal: increase security of inter-domain routing
  - Path control
  - Resilience (e.g. redundant paths, no route hijacks)
  - Active research, e.g. into congestion control and QoS
  - Incremental deployment (e.g. SCION-IP gateway)
- Hands-on experience



Click to add text

Using existing applications with SCION

- Incremental deployment
  - Run IP applications on SCION; currently testing/experimenting with DNS
  - No need to change user applications
- Benefits: no route hijacks, resilience through multiple paths, path control at network level



anapaya systems

RINA

- RINA: Recursive InterNetwork Architecture
- Goal: address fundamental problems with a new architecture
  - A framework, not a protocol
  - Provides mechanisms and policies (a toolbox) to network designers
  - Organize repeated functionality across layers
  - Idea is to standardize security, management, congestion
- Starting to look into RINA

NDN

- NDN: Named Data Networking
- Fundamental change: information-centric rather than host-centric
- Distribution of information
- Little bit like Content Delivery Network (CDNs), but built into the network
- We'll look into NDN later

Open programmable networks

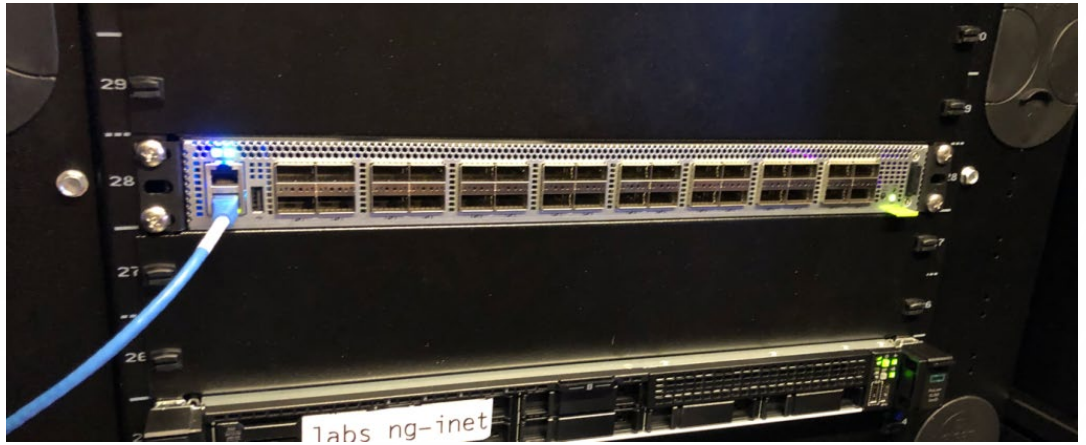
- Networking hardware such as routers and switches
- Related to Software Defined Networking (SDN)
  - Control plane vs. data plane
- Allows us to implement and deploy new protocols

2STiC testbed

- Goal: evaluate future internet architectures, see how they perform "in real life"
- Open programmable networking hardware
- Experiment with P4-capable hardware (switches and network interfaces)
- Status: some partners connected, working on connecting the others

Testbed activities

- Implement future internet architecture (SCION) in P4
- Network management: Inband Network Telemetry (INT)
- Path tracking and data collection
- Improving routing security



Applying our findings

- We are developing use cases to experiment with those technologies
  - What are interesting use cases?
  - How do they perform in practice?
  - Do they solve our problems?
- Talking to various organizations from several sectors: transport systems, health, energy suppliers, banks, government, industrial control systems
- Can we help you?

Q&A and discussion

References

- 2STiC consortium: www.2STiC.nl
- Voorbereiden op digitale ontwrichting: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting
- Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands: https://ris.utwente.nl/ws/portalfiles/portal/124347608/wodc_report_scada_final.pdf