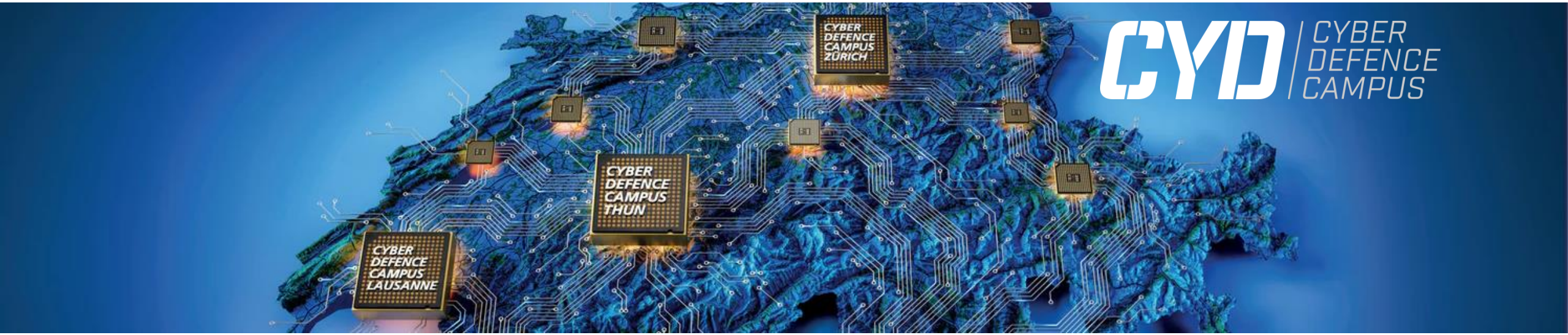
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Rüstung - armasuisse ar

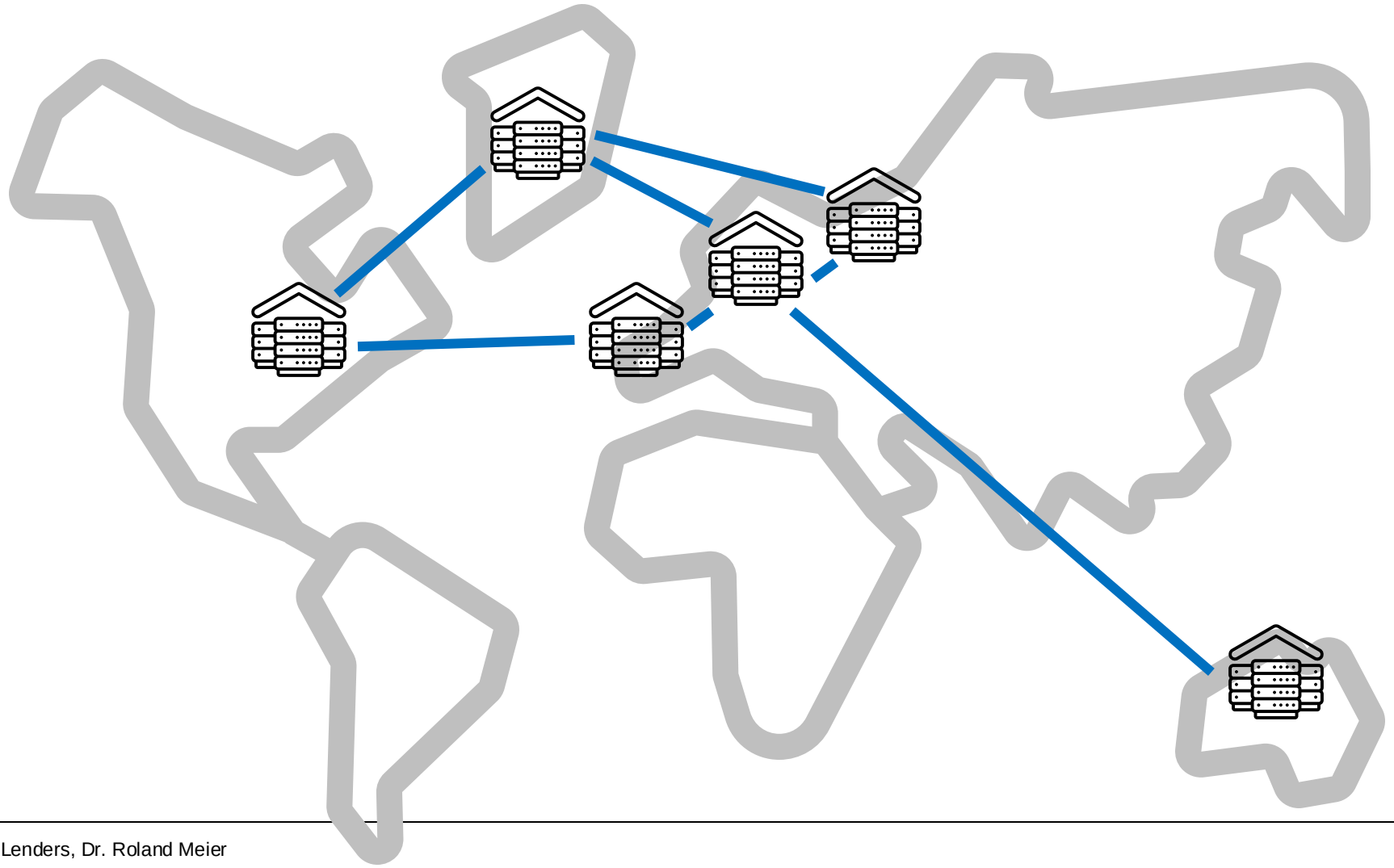


SCION @ CYD Campus

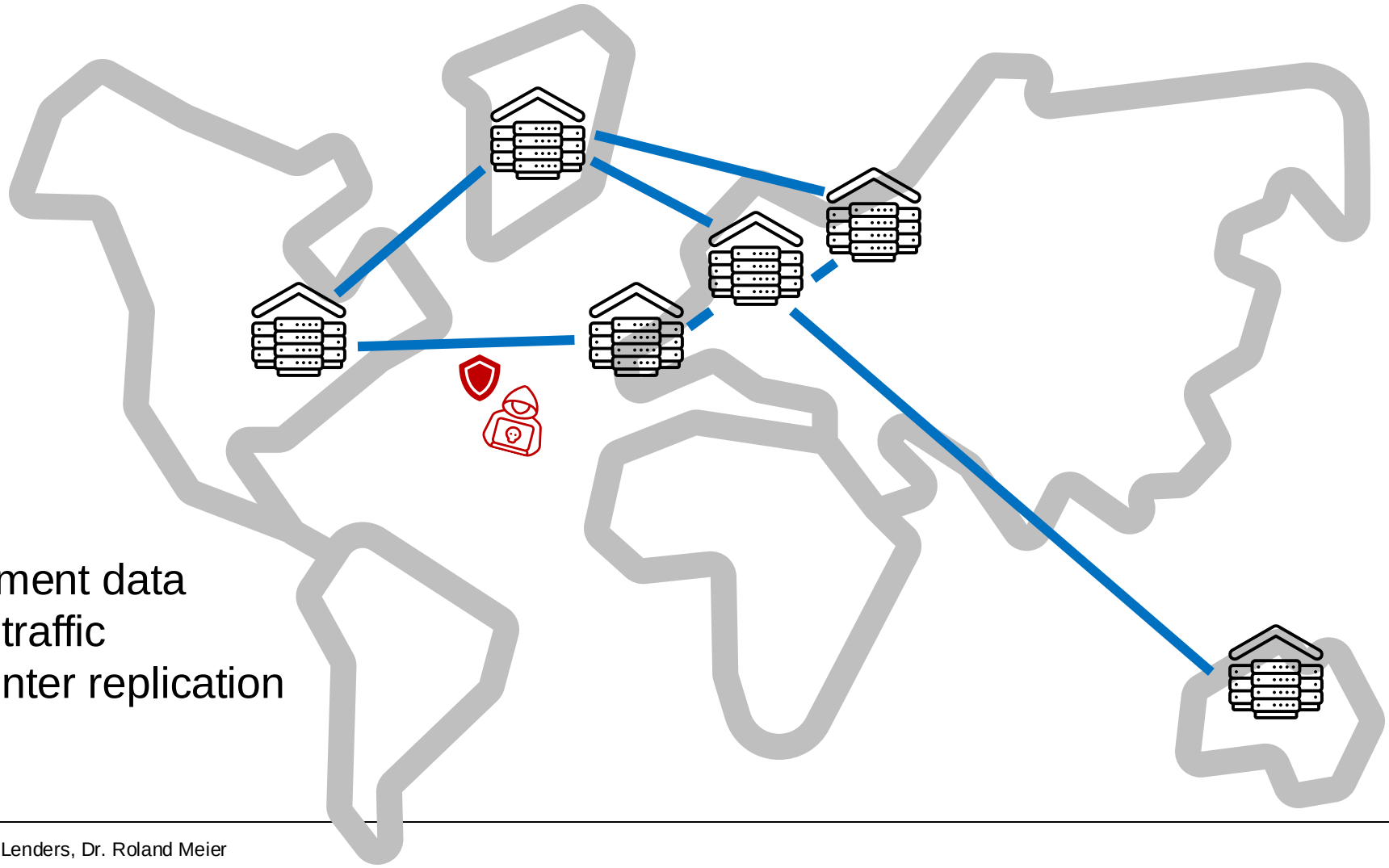
Building Military-grade Wide Area Networks with SCION

Dr. Vincent Lenders and Dr. Roland Meier

Wide area networks connect geographically distributed sites



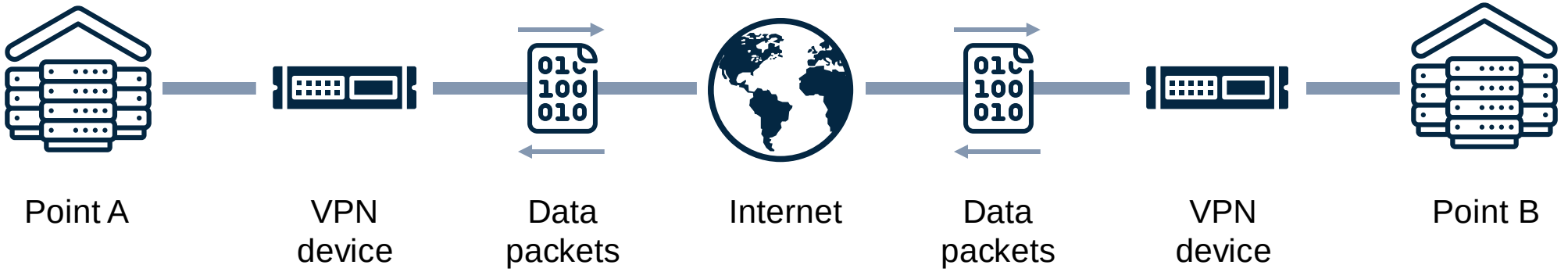
Wide area networks are often used to transmit sensitive information



Government data
Military traffic
Data center replication

A poor man’s approach for building WANs

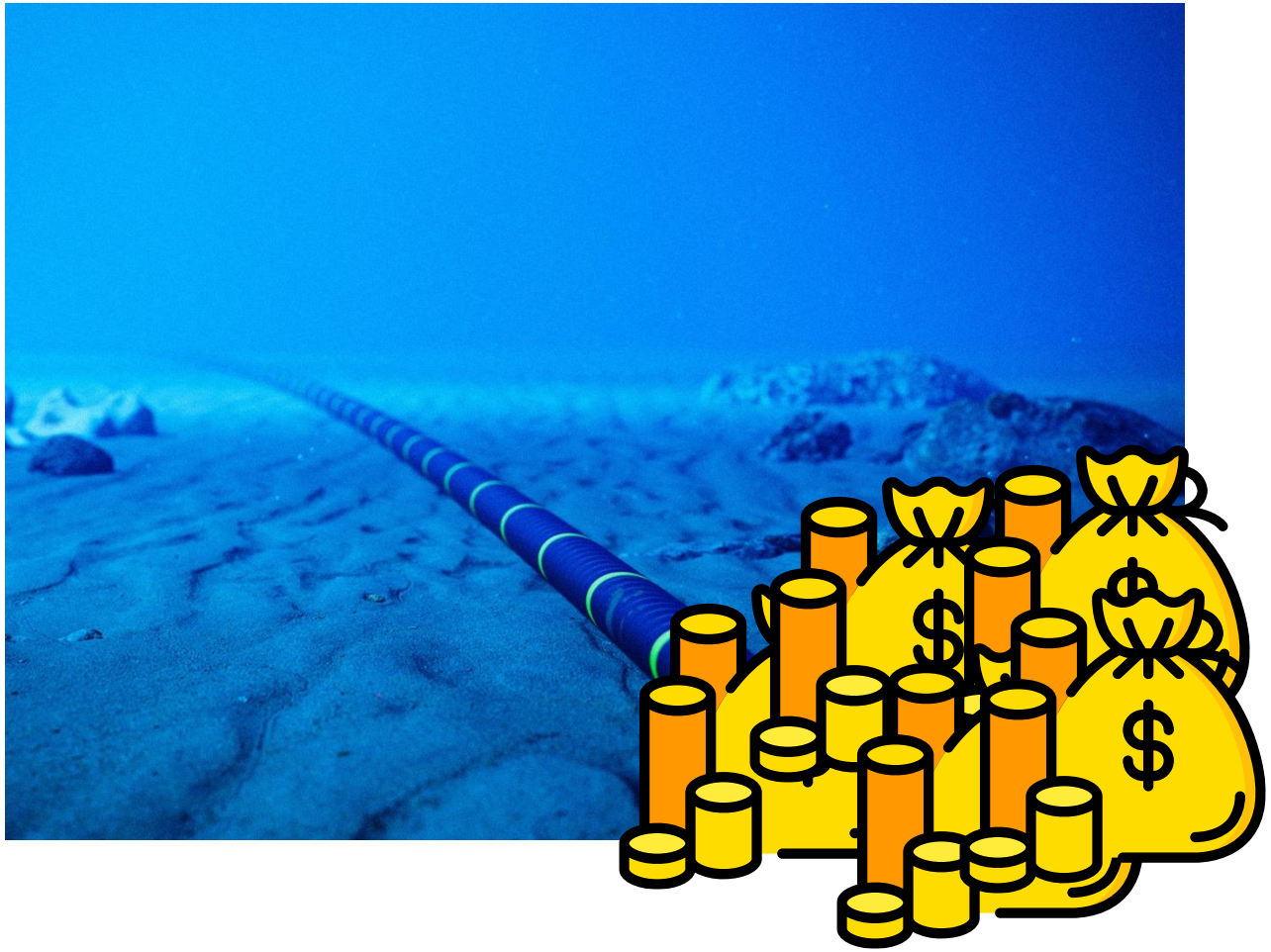
VPN tunneling over the Internet



Drawbacks:

- Performance
- Resilience
- Security and privacy

To increase their security, WANs are often built on dedicated infrastructure



Requirements for “Military-Grade” Networks

Security

confidentiality, integrity, availability

Resilience

function in degraded or contested environments

Scalability

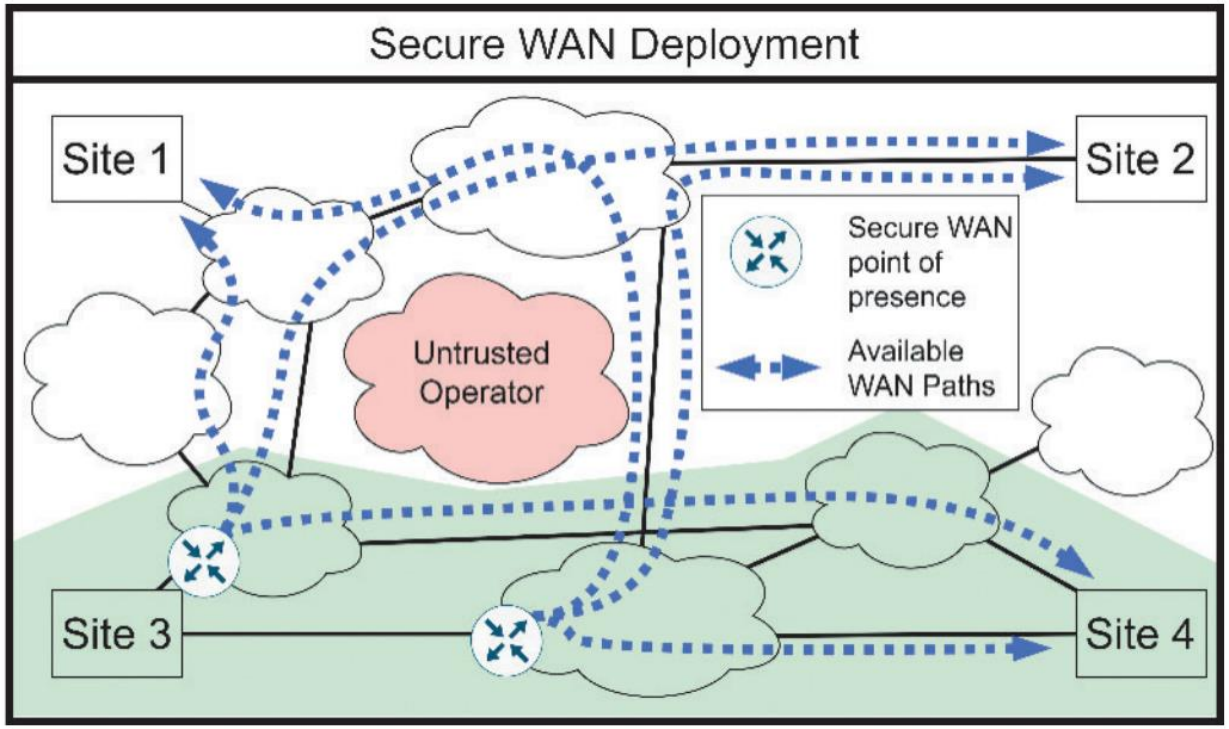
rapid deployment, interoperability, modular design

Performance

low latency, high bandwidth, QoS

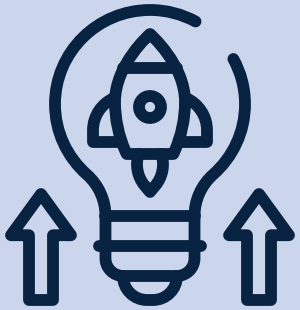
Our vision

Building military-grade wide area networks over shared infrastructures



Selection of CYD Campus activities related to SCION

SCION

Research	Innovation	Evaluation
		
Secure WAN architecture based on SCION – DDoS mitigation systems – Fine-grained path selection based on router properties	Secure communication with Threema over SCION – 5G core network over SCION	Independent security analysis of SCION implementations and appliances – Performance testing of SCION in combination with other protections

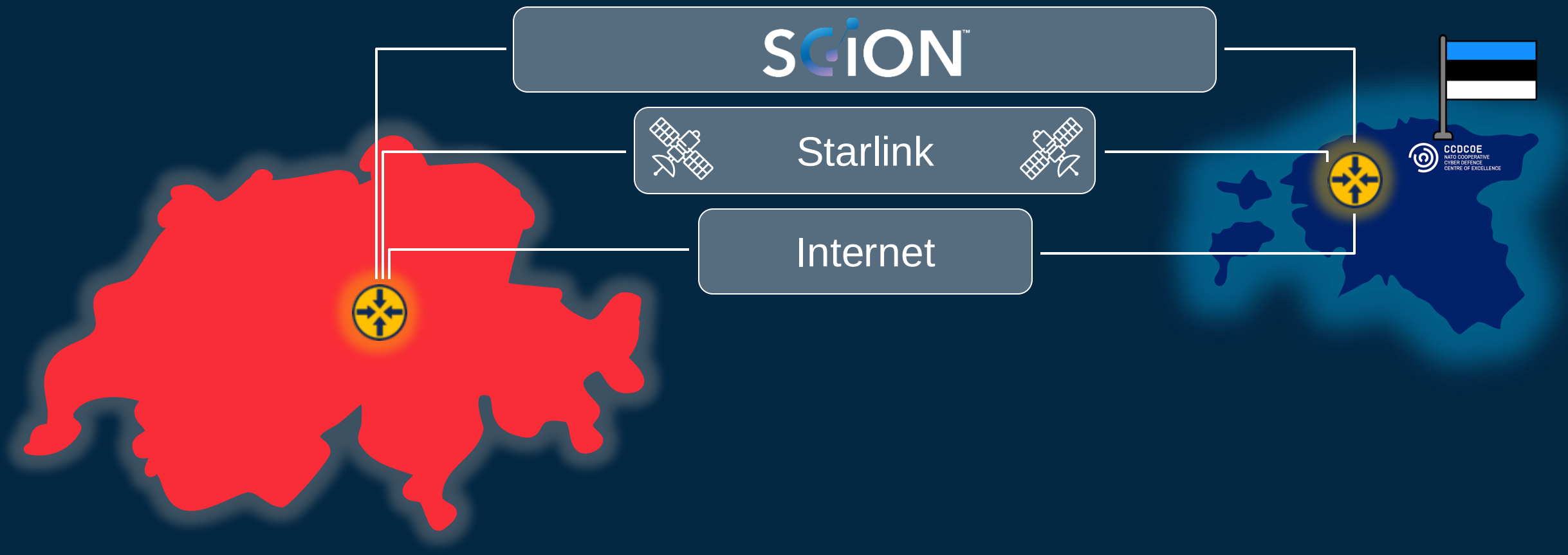
In 2020, the CYD Campus decided to build its own “SCION Lab” based on commercial offerings

Inauguration of the SCION Lab in 2022

In 2023, the CYD Campus extended the SCION Lab by an additional connection in Estonia

Use Case: Locked Shields, the largest live-fire global cyber defense exercise

The Swiss Armed Forces used three independent networks to access the Locked Shields network



Selection of CYD Campus activities related to SCION

Research

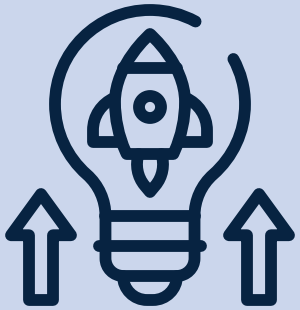
Secure WAN architecture based on SCION

–

DDoS mitigation systems

–

Fine-grained path selection based on router properties



Innovation

Secure communication with Threema over SCION

–

5G core network over SCION

Evaluation

Independent security analysis of SCION implementations and appliances

–

Performance testing of SCION in combination with other protections

This is joint work with researchers from ETH Zürich

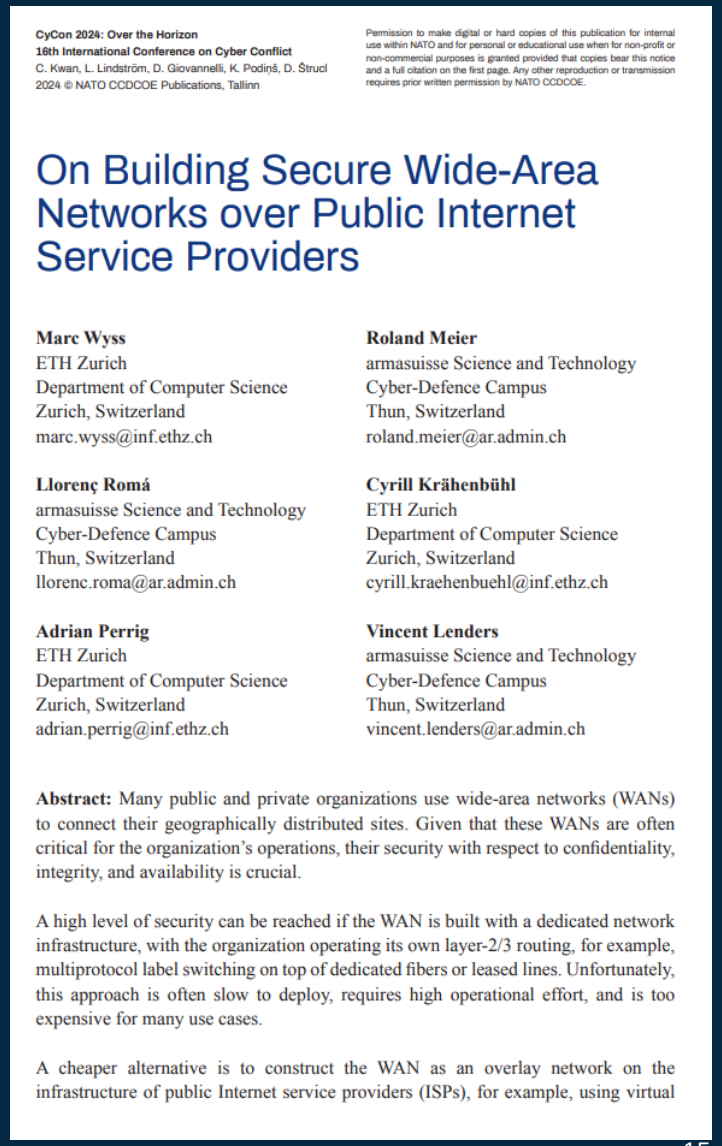
Marc Wyss[(1)], Roland Meier[(2)],

Llorenç Romá[(2)], Cyrill Krähenbühl[(1)],

Adrian Perrig[(1)], Vincent Lenders[(2)]

(1) ETH zürich

(2) Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
armasuisse



CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl
2024 © NATO CCDCOE Publications, Tallinn

On Building Secure Wide-Area Networks over Public Internet Service Providers

Marc Wyss
ETH Zurich
Department of Computer Science
Zurich, Switzerland
marc.wyss@inf.ethz.ch

Roland Meier
armasuisse Science and Technology
Cyber-Defence Campus
Thun, Switzerland
roland.meier@ar.admin.ch

Llorenç Romá
armasuisse Science and Technology
Cyber-Defence Campus
Thun, Switzerland
llorenc.roma@ar.admin.ch

Cyrill Krähenbühl
ETH Zurich
Department of Computer Science
Zurich, Switzerland
cyrill.kraehenbuehl@inf.ethz.ch

Adrian Perrig
ETH Zurich
Department of Computer Science
Zurich, Switzerland
adrian.perrig@inf.ethz.ch

Vincent Lenders
armasuisse Science and Technology
Cyber-Defence Campus
Thun, Switzerland
vincent.lenders@ar.admin.ch

Abstract: Many public and private organizations use wide-area networks (WANs) to connect their geographically distributed sites. Given that these WANs are often critical for the organization's operations, their security with respect to confidentiality, integrity, and availability is crucial.

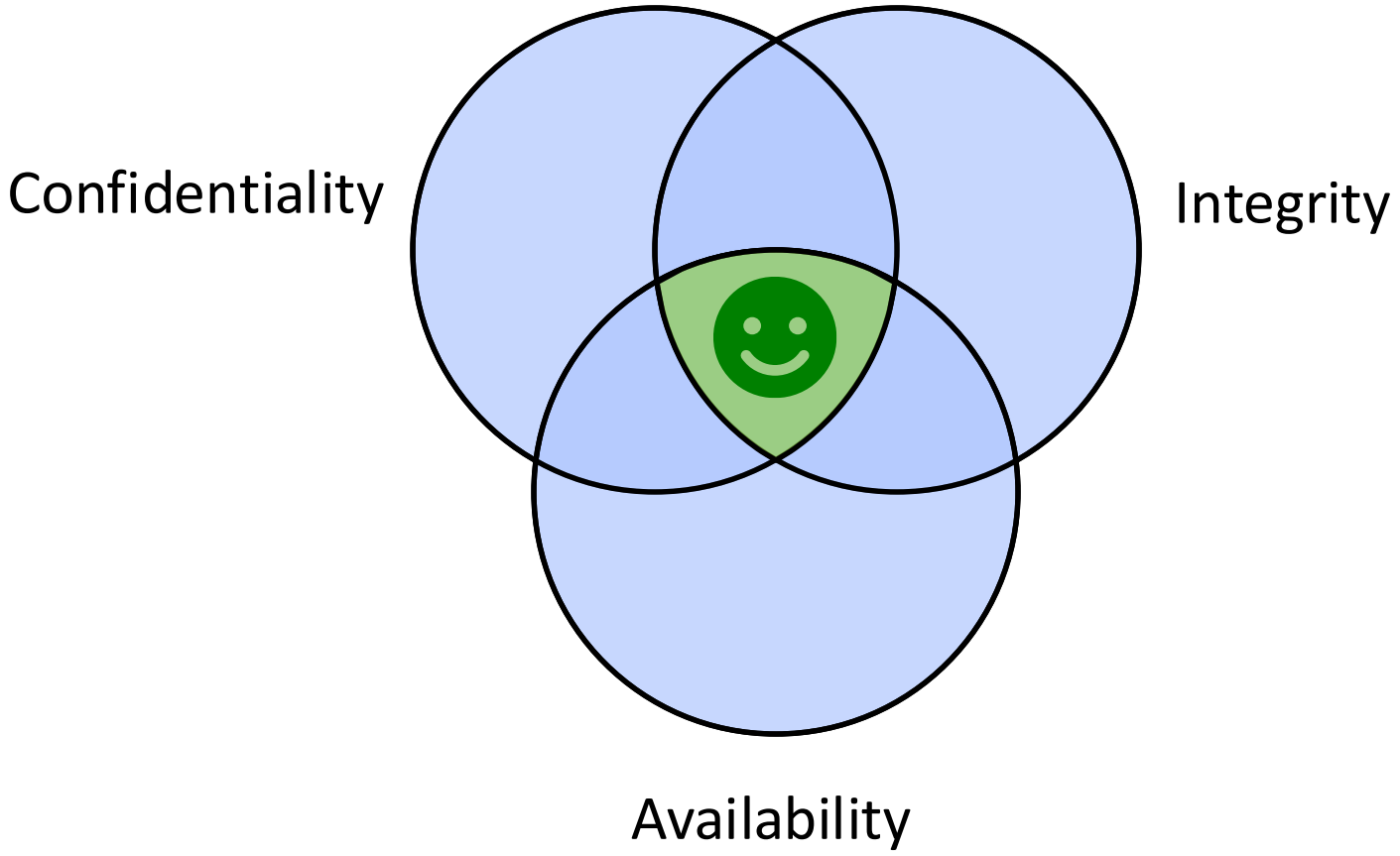
A high level of security can be reached if the WAN is built with a dedicated network infrastructure, with the organization operating its own layer-2/3 routing, for example, multiprotocol label switching on top of dedicated fibers or leased lines. Unfortunately, this approach is often slow to deploy, requires high operational effort, and is too expensive for many use cases.

A cheaper alternative is to construct the WAN as an overlay network on the infrastructure of public Internet service providers (ISPs), for example, using virtual

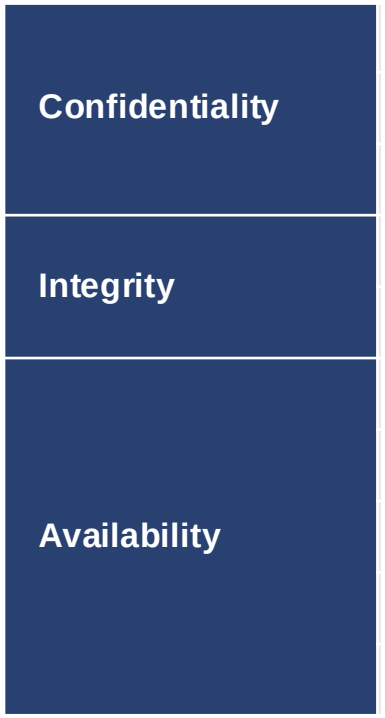
How can we build secure WANs on shared infrastructure?

How can we build secure WANs on shared infrastructure?

The CIA triad describes the most important security goals



We identified the most relevant threats and possible mitigations



We identified the most relevant threats and possible mitigations

Confidentiality	Eavesdropping (payloads)
	Eavesdropping (metadata)
	Traffic hijacking
Integrity	
Availability	

We identified the most relevant threats and possible mitigations

Confidentiality	Eavesdropping (payloads)
	Eavesdropping (metadata)
	Traffic hijacking
Integrity	Traffic injection
	Traffic modification
Availability	

We identified the most relevant threats and possible mitigations

Confidentiality	Eavesdropping (payloads)
	Eavesdropping (metadata)
	Traffic hijacking
Integrity	Traffic injection
	Traffic modification
Availability	Traffic dropping
	Traffic hijacking
	Congestion
	Volumetric DDoS
	Topology changes

How can we build secure WANs on shared infrastructure?

Components | Roadmap

How can we build secure WANs on shared infrastructure?

Components | Roadmap

We identified the most relevant threats and possible mitigations

Mitigations →

	Threats ↓
Confidentiality	Eavesdropping (payloads)
	Eavesdropping (metadata)
	Traffic hijacking
Integrity	Traffic injection
	Traffic modification
Availability	Traffic dropping
	Traffic hijacking
	Congestion
	Volumetric DDoS
	Topology changes

We identified the most relevant threats and possible mitigations

	Threats ↓	Mitigations → Traffic encryption
Confidentiality	Eavesdropping (payloads)	
	Eavesdropping (metadata)	
	Traffic hijacking	
Integrity	Traffic injection	
	Traffic modification	
Availability	Traffic dropping	
	Traffic hijacking	
	Congestion	
	Volumetric DDoS	
	Topology changes	

We identified the most relevant threats and possible mitigations

	Mitigations → / Threats ↓	Traffic encryption
Confidentiality	Eavesdropping (payloads)	✓
	Eavesdropping (metadata)	✓
	Traffic hijacking	
Integrity	Traffic injection	
	Traffic modification	
Availability	Traffic dropping	
	Traffic hijacking	
	Congestion	
	Volumetric DDoS	
	Topology changes	

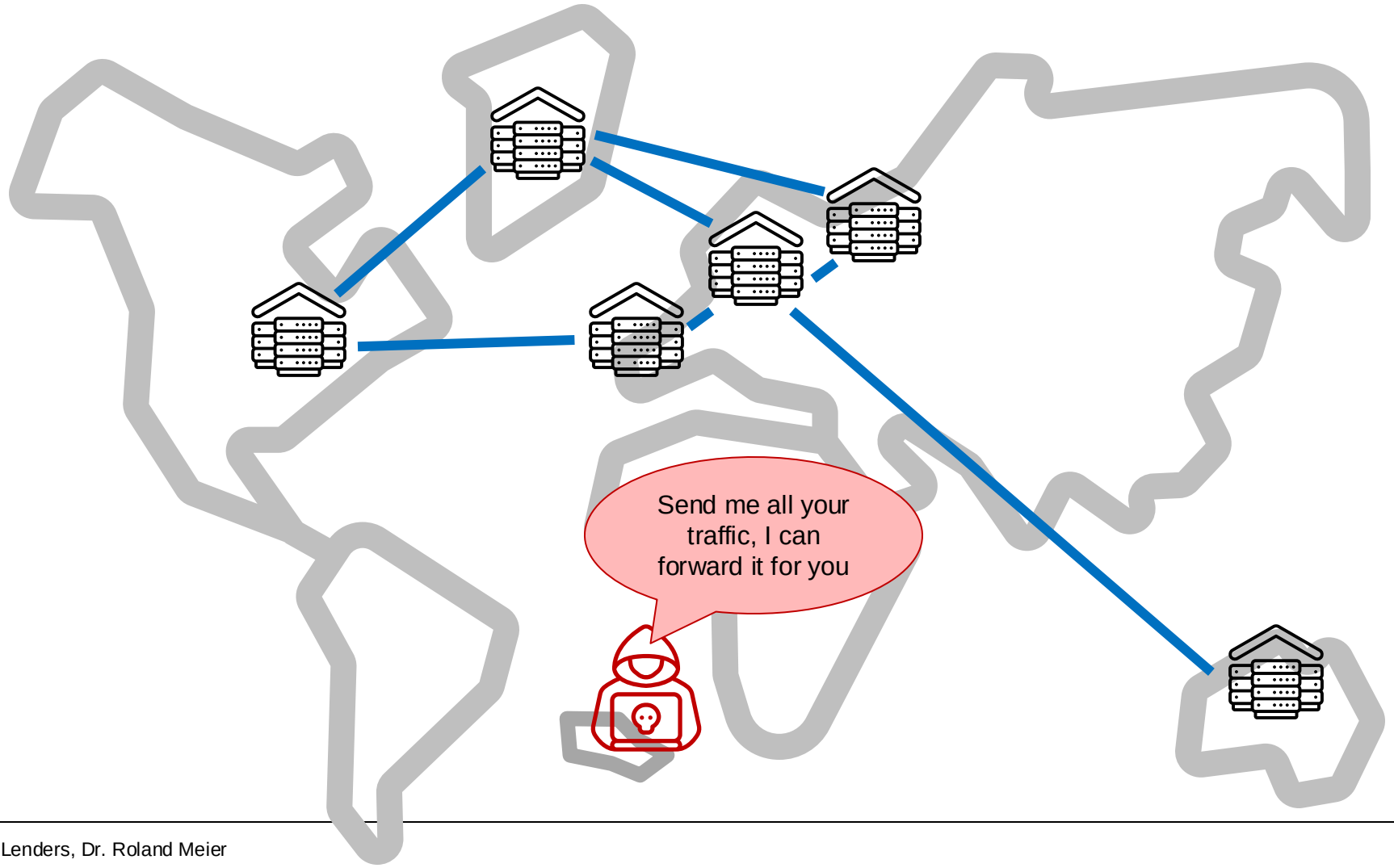
Encryption hides the contents of packets, but can still leak information

Padding and traffic shaping obfuscate the “shape” of packets

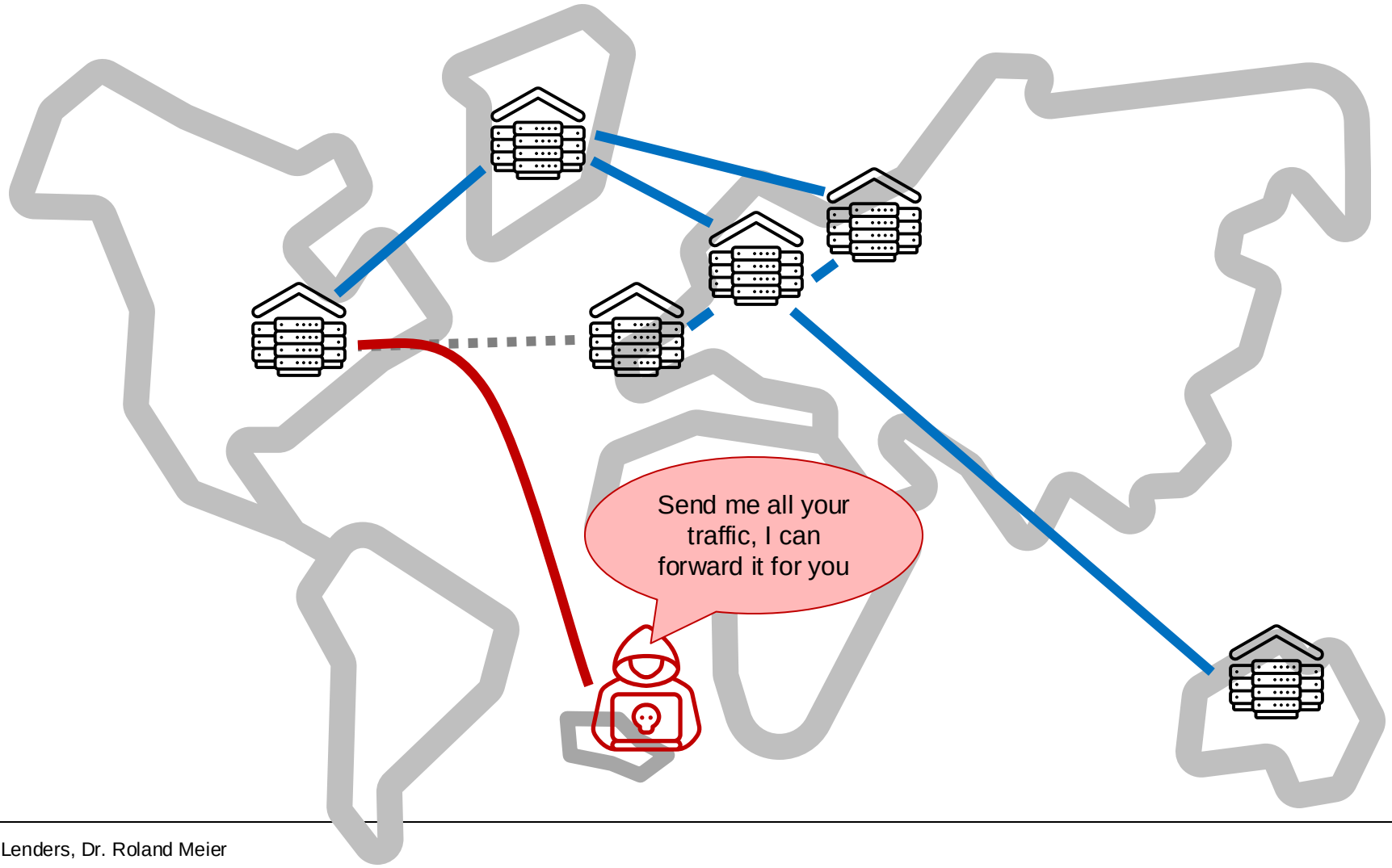
We identified the most relevant threats and possible mitigations

	Threats ↓ / Mitigations →	Traffic encryption	Traffic shaping and padding
Confidentiality	Eavesdropping (payloads)	✓	
	Eavesdropping (metadata)	✓	✓
	Traffic hijacking		
Integrity	Traffic injection		
	Traffic modification		
Availability	Traffic dropping		
	Traffic hijacking		
	Congestion		X
	Volumetric DDoS		
	Topology changes		

An adversary can “hijack” Internet traffic



An adversary can “hijack” Internet traffic



An adversary can “hijack” Internet traffic

ars TECHNICA SUBSCRIBE SIGN IN

BGP —

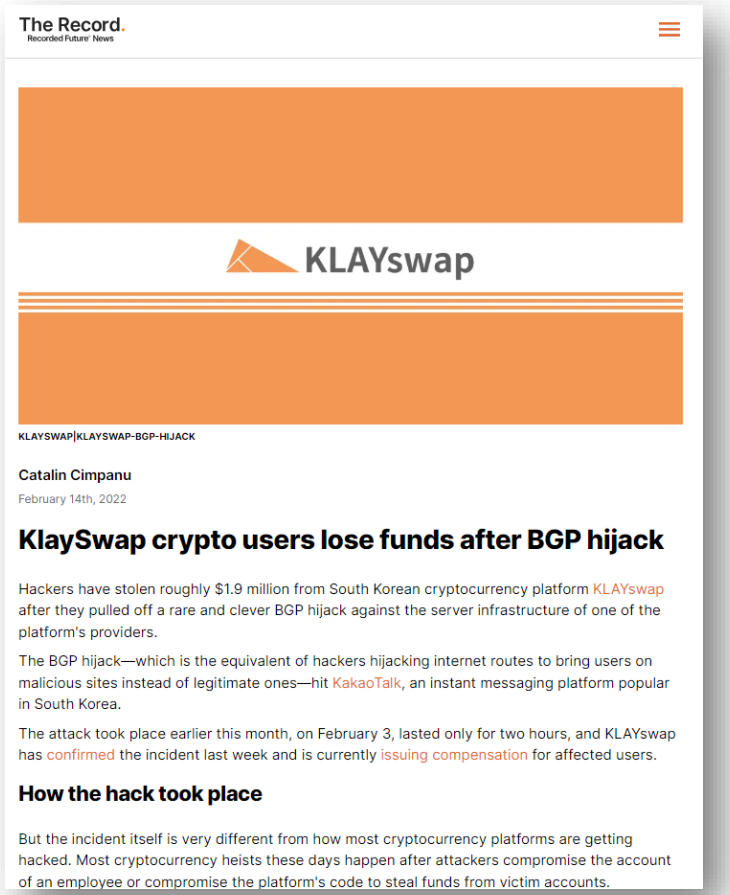
Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP mishap

Despite the timing, the 45-minute hijacking was most likely an error, not an attack.

DAN GOODIN - 3/29/2022, 4:00 AM

Enlarge

Some Internet traffic in and out of Twitter on Monday was briefly funneled through Russia after a major ISP in that country misconfigured the Internet's routing table, network monitoring services



The Record. Recorded Future News

KLAYswap

KLAYSWAP|KLAYSWAP-BGP-HIJACK

Catalin Cimpanu

February 14th, 2022

KlaySwap crypto users lose funds after BGP hijack

Hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.

The BGP hijack—which is the equivalent of hackers hijacking internet routes to bring users on malicious sites instead of legitimate ones—hit KakaoTalk, an instant messaging platform popular in South Korea.

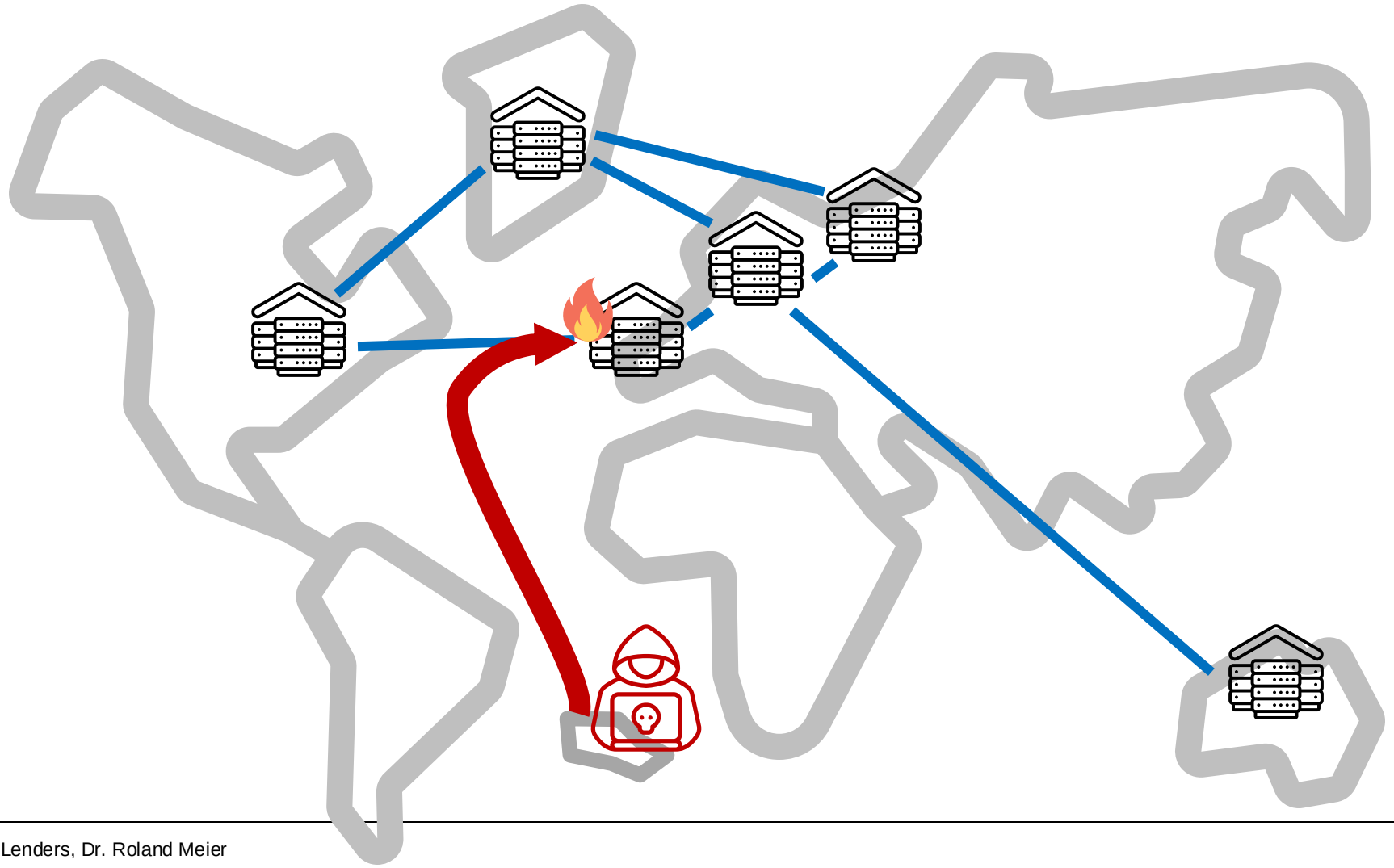
The attack took place earlier this month, on February 3, lasted only for two hours, and KLAYswap has confirmed the incident last week and is currently issuing compensation for affected users.

How the hack took place

But the incident itself is very different from how most cryptocurrency platforms are getting hacked. Most cryptocurrency heists these days happen after attackers compromise the account of an employee or compromise the platform's code to steal funds from victim accounts.

We identified the most relevant threats and possible mitigations

	Threats ↓ / Mitigations →	Traffic encryption	Traffic shaping and padding	Path control
Confidentiality	Eavesdropping (payloads)	✓		✓/✗
	Eavesdropping (metadata)	✓	✓	✓/✗
	Traffic hijacking			✓
Integrity	Traffic injection			
	Traffic modification			
Availability	Traffic dropping			✓
	Traffic hijacking			✓
	Congestion		✗	✓/✗
	Volumetric DDoS			✓
	Topology changes			✓



We identified the most relevant threats and possible mitigations

	Threats ↓ / Mitigations →	Traffic encryption	Traffic shaping and padding	Path control	Traffic filtering	Traffic authentication	Path authentication	Traffic prioritization
Confidentiality	Eavesdropping (payloads)	✓		✓/✗				
	Eavesdropping (metadata)	✓	✓	✓/✗				
	Traffic hijacking			✓			✓	
Integrity	Traffic injection					✓		
	Traffic modification					✓		
Availability	Traffic dropping			✓	✗			
	Traffic hijacking			✓			✓	
	Congestion		✗	✓/✗				✓
	Volumetric DDoS			✓	✓	✓		✓
	Topology changes			✓				

We identified the most relevant threats and possible mitigations

	Mitigations → / Threats ↓	Traffic encryption	Traffic shaping and padding	Path control	Traffic filtering	Traffic authentication	Path authentication	Traffic prioritization
Confidentiality	Eavesdropping (payloads)	✓		✓/✗				
	Eavesdropping (metadata)	✓	✓	✓/✗				
	Traffic hijacking			✓			✓	
Integrity	Traffic injection					✓		
	Traffic modification					✓		
Availability	Traffic dropping			✓	✗			
	Traffic hijacking			✓			✓	
	Congestion		✗	✓/✗				✓
	Volumetric DDoS			✓	✓	✓		✓
	Topology changes			✓				

Mitigations can be implemented using a combination of existing (research) works

Mitigations can be implemented using a combination of existing (research) works

Technology ↓ \ Mitigations →	Traffic encryption	Traffic shaping and padding	Path control	Traffic filtering	Traffic authentication	Path authentication	Traffic prioritization
IPsec	✓				✓		

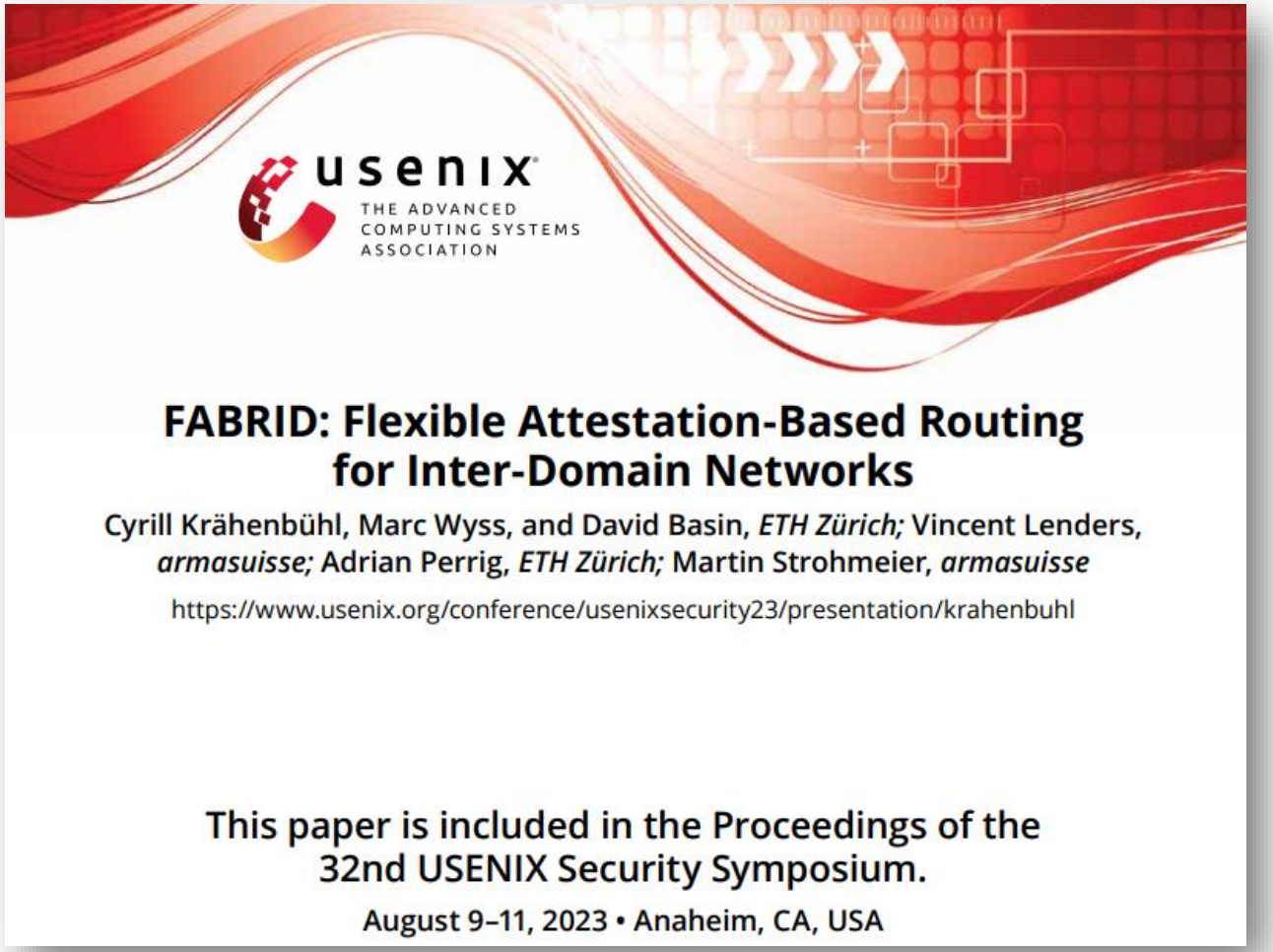
Mitigations can be implemented using a combination of existing (research) works

Technology ↓ \ Mitigations →	Traffic encryption	Traffic shaping and padding	Path control	Traffic filtering	Traffic authentication	Path authentication	Traffic prioritization
IPsec	✓				✓		
SCION			✓			✓	

Mitigations can be implemented using a combination of existing (research) works

Technology ↓ \ Mitigations →	Traffic encryption	Traffic shaping and padding	Path control	Traffic filtering	Traffic authentication	Path authentication	Traffic prioritization
IPsec	✓				✓		
SCION			✓			✓	
Lightning Filter				✓	✓		✓
FABRID			✓		✓		
Helia					✓		✓

FABRID for flexible routing

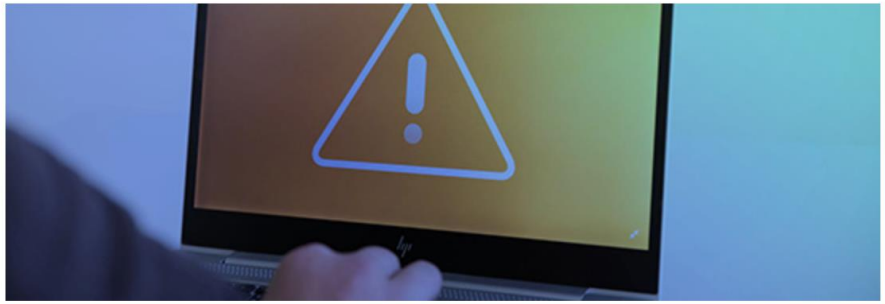


One of the use-cases: Avoid network devices with outdated software

National Cyber Security Centre NCSC

Critical vulnerability in Palo Alto firewalls

18.04.2024 - The NCSC warns of the security vulnerability in Palo Alto's Next-Generation Firewall (NGFW). These firewalls are mainly used by companies and public authorities. They have a critical vulnerability that is already being exploited by cyber criminals. The attackers exploit the vulnerability to execute commands. The NCSC has already received corresponding reports from organisations in Switzerland. The NCSC recommends installing the security updates as quickly as possible or even reinstalling the NGFW if possible.



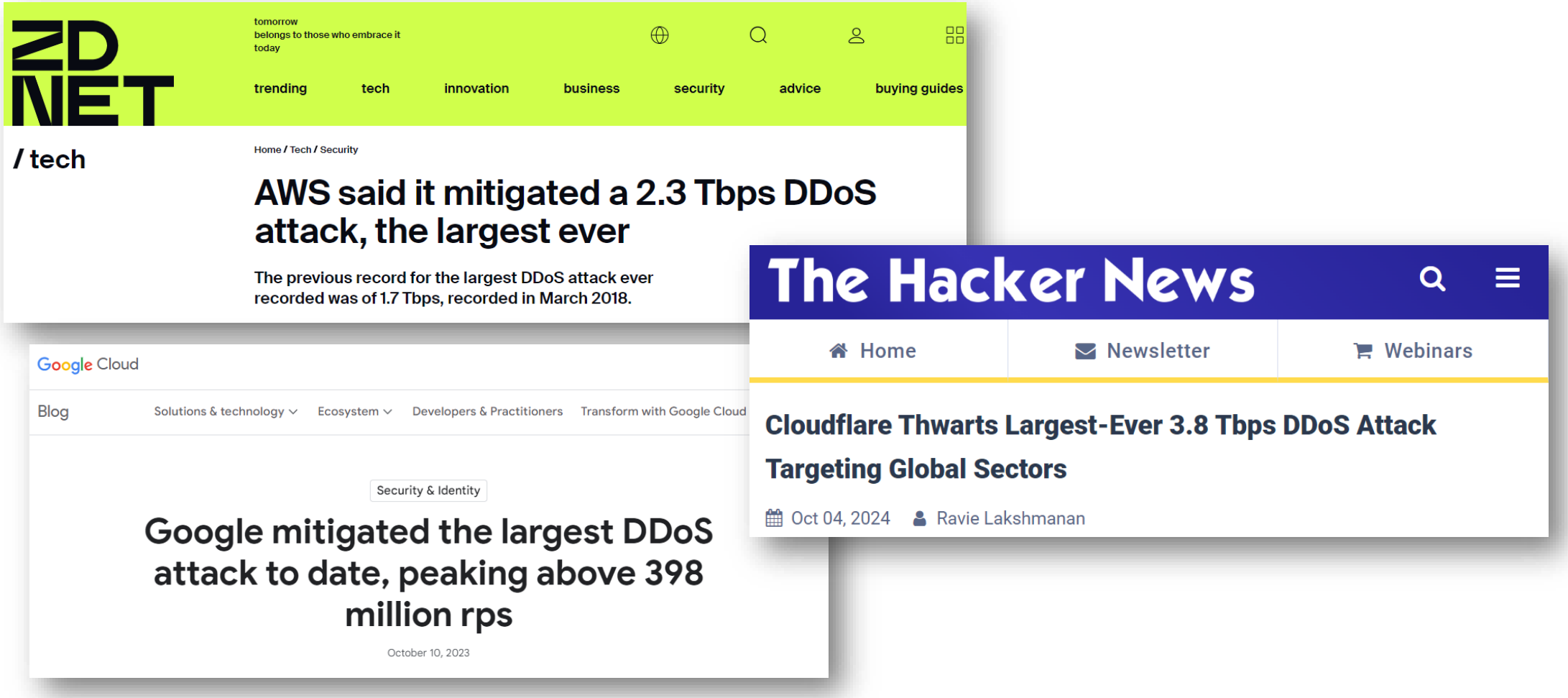
On April 12 2024, the US manufacturer of firewall solutions Palo Alto publicly disclosed a critical vulnerability in PAN-OS. Palo Alto's products are mainly used in companies. The critical vulnerability allows an attacker to remotely execute arbitrary code on vulnerable devices and thereby compromise them (CVE-2024-3400).

On April 18 2024, the NCSC received several reports from organizations in Switzerland showing widespread attacks on the aforementioned vulnerability. The NCSC therefore strongly advises organizations to apply the security patch released by Palo Alto as soon as possible. Devices that have already been demonstrably

Paths can be selected with many different objectives

- Manufacturer
- Hardware
- Software (+ patch level)
- Geolocation
- Jurisdiction
- CO_2 emissions

Some WANs run at high bandwidths, which requires high-performance protection mechanisms



Mitigations can be implemented using a combination of existing (research) works

Technology ↓ / Mitigations →	Traffic encryption	Traffic shaping and padding	Path control	Traffic filtering	Traffic authentication	Path authentication	Traffic prioritization
IPsec	✓				✓		
SCION			✓			✓	
Lightning Filter				✓	✓		✓
FABRID			✓		✓		
Helia					✓		✓
ACC-Turbo							✓
DITTO		✓					

Mitigations can be implemented using a combination of existing (research) works

Technology ↓ \ Mitigations →	Traffic encryption	Traffic shaping and padding	Path control	Traffic filtering	Traffic authentication	Path authentication	Traffic prioritization
IPsec	✓				✓		
SCION			✓			✓	
Lightning Filter				✓	✓		✓
FABRID			✓		✓		
Helia					✓		✓
ACC-Turbo							✓
DITTO		✓					

How can we build secure WANs on shared infrastructure?

Components | Roadmap

SCION is commercially available, but many other components only exist as research prototypes

Technology	Offered by ISPs	Technology Readiness Level
IPsec		
SCION connectivity		
FABRID		
Helia		
Lightning Filter		
ACC-Turbo		
DITTO		

SCION is commercially available, but many other components only exist as research prototypes

Technology	Offered by ISPs	Technology Readiness Level
IPsec	Not needed	9 (Actual system proven in operational environment)
SCION connectivity	Yes	7 (System prototype demonstration in operational environment)
FABRID		
Helia		
Lightning Filter		
ACC-Turbo		
DITTO		

SCION is commercially available, but many other components only exist as research prototypes

Technology	Offered by ISPs	Technology Readiness Level
IPsec	Not needed	9 (Actual system proven in operational environment)
SCION connectivity	Yes	7 (System prototype demonstration in operational environment)
FABRID	Not yet	3 (Experimental proof of concept)
Helia	Not yet	
Lightning Filter	Not yet	
ACC-Turbo	Not yet	
DITTO	Not needed	

Requirements for “Military-Grade” Networks

Security

confidentiality, integrity, availability

Resilience

function in degraded or contested environments

Scalability

rapid deployment, interoperability, modular design

Performance

low latency, high bandwidth, QoS

Selection of CYD Campus activities related to SCION

Research

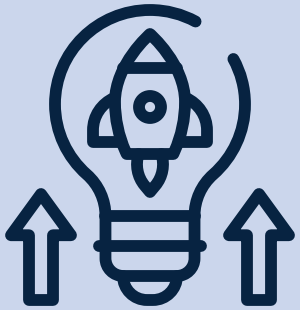
Secure WAN architecture based on SCION

–

DDoS mitigation systems

–

Fine-grained path selection based on router properties



Innovation

Secure communication with Threema over SCION

–

5G core network over SCION

Testing

Independent security analysis of SCION implementations and appliances

–

Performance testing of SCION in combination with other protections

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

CYD | CYBER DEFENCE CAMPUS

Thank you for your attention!

Vincent Lenders
vincent.lenders@ar.admin.ch

Roland Meier
roland.meier@ar.admin.ch

cydcampus.admin.ch
cyber-defence-campus
@cydcampus