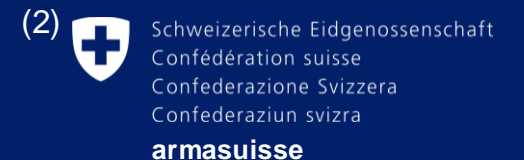
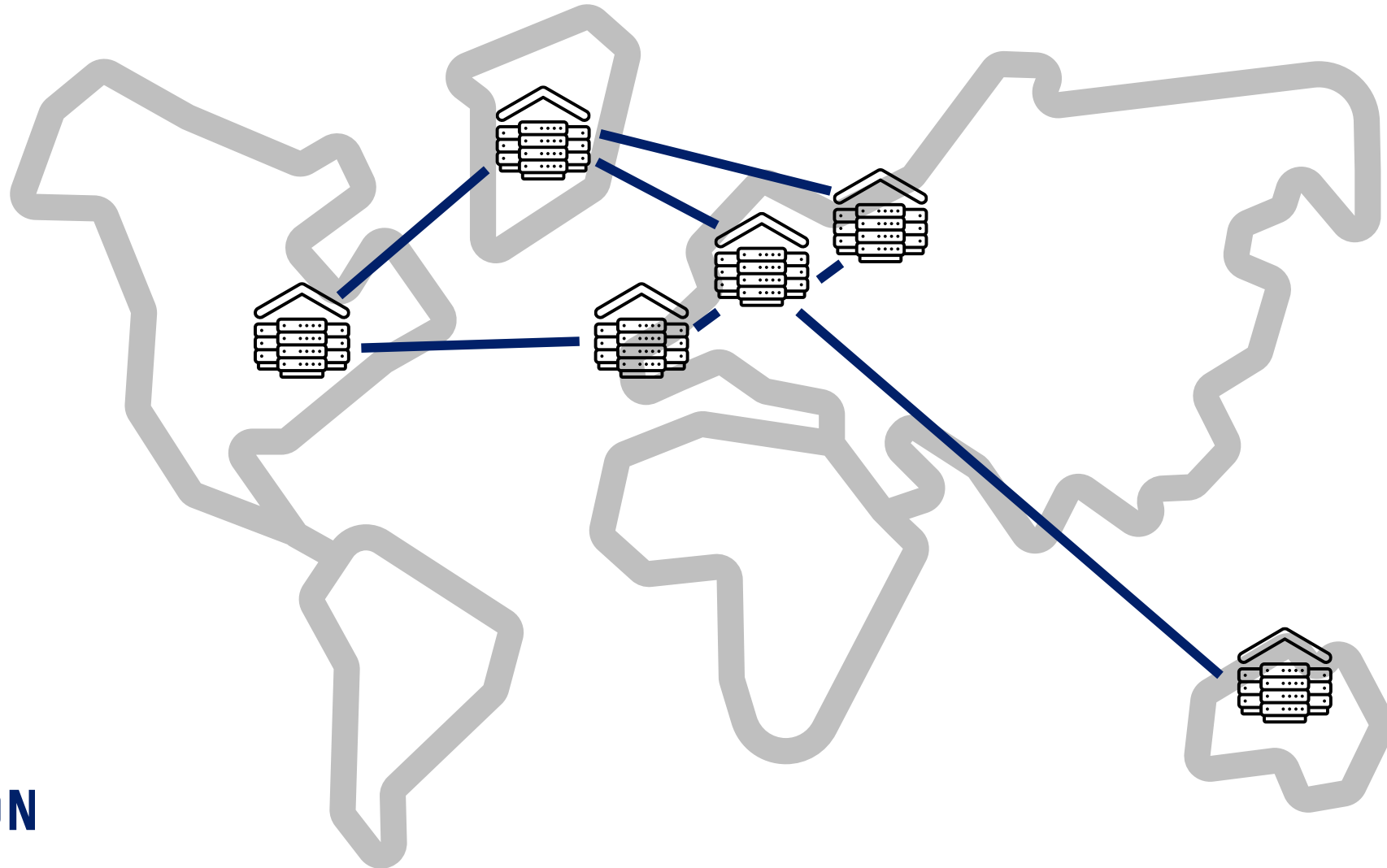


On Building Secure Wide Area Networks over Public Internet Service Providers

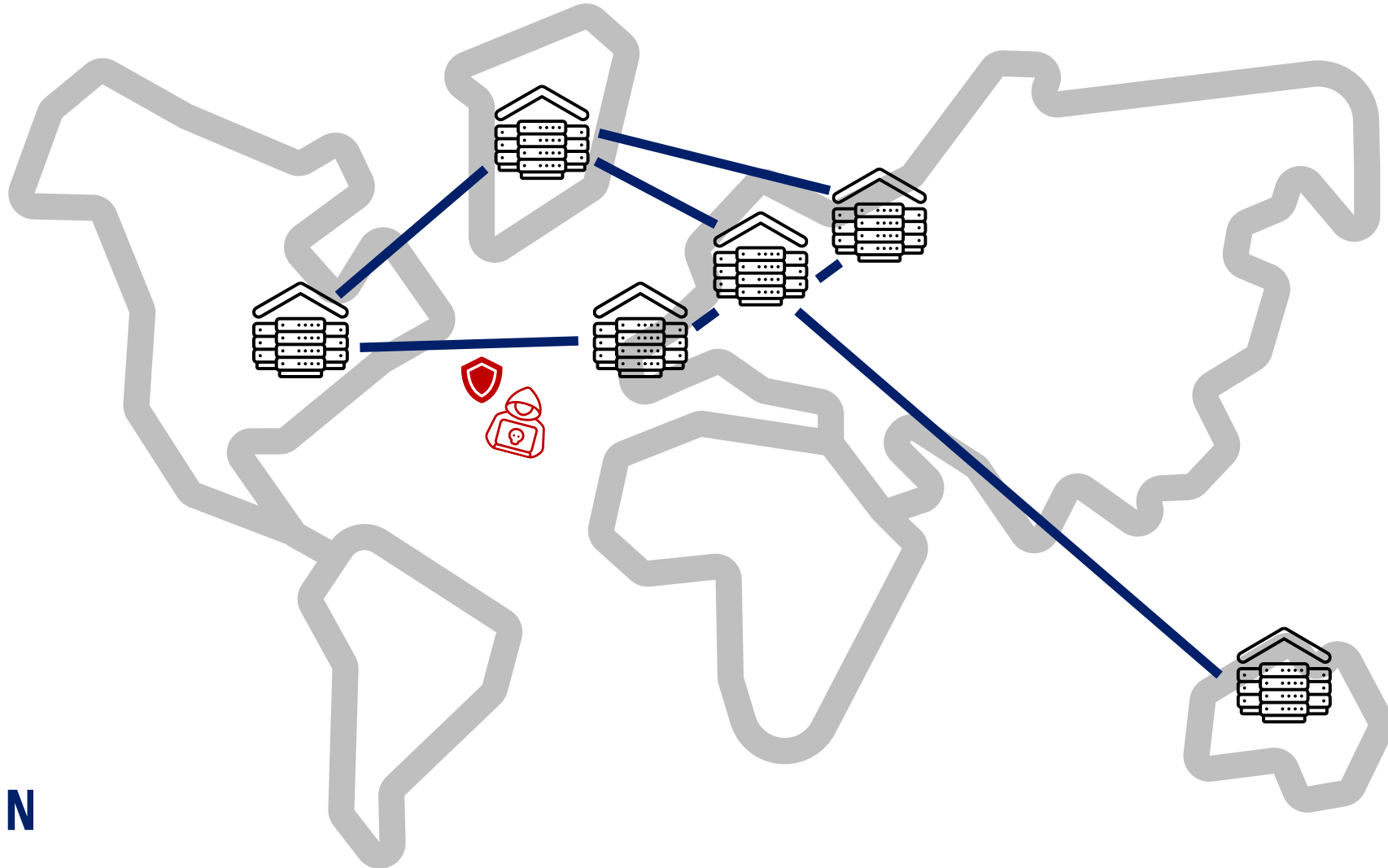
Marc Wyss⁽¹⁾, Roland Meier⁽²⁾, Llorenç Romá⁽²⁾,
Cyrill Krähenbühl⁽¹⁾, Adrian Perrig⁽¹⁾, Vincent Lenders⁽²⁾



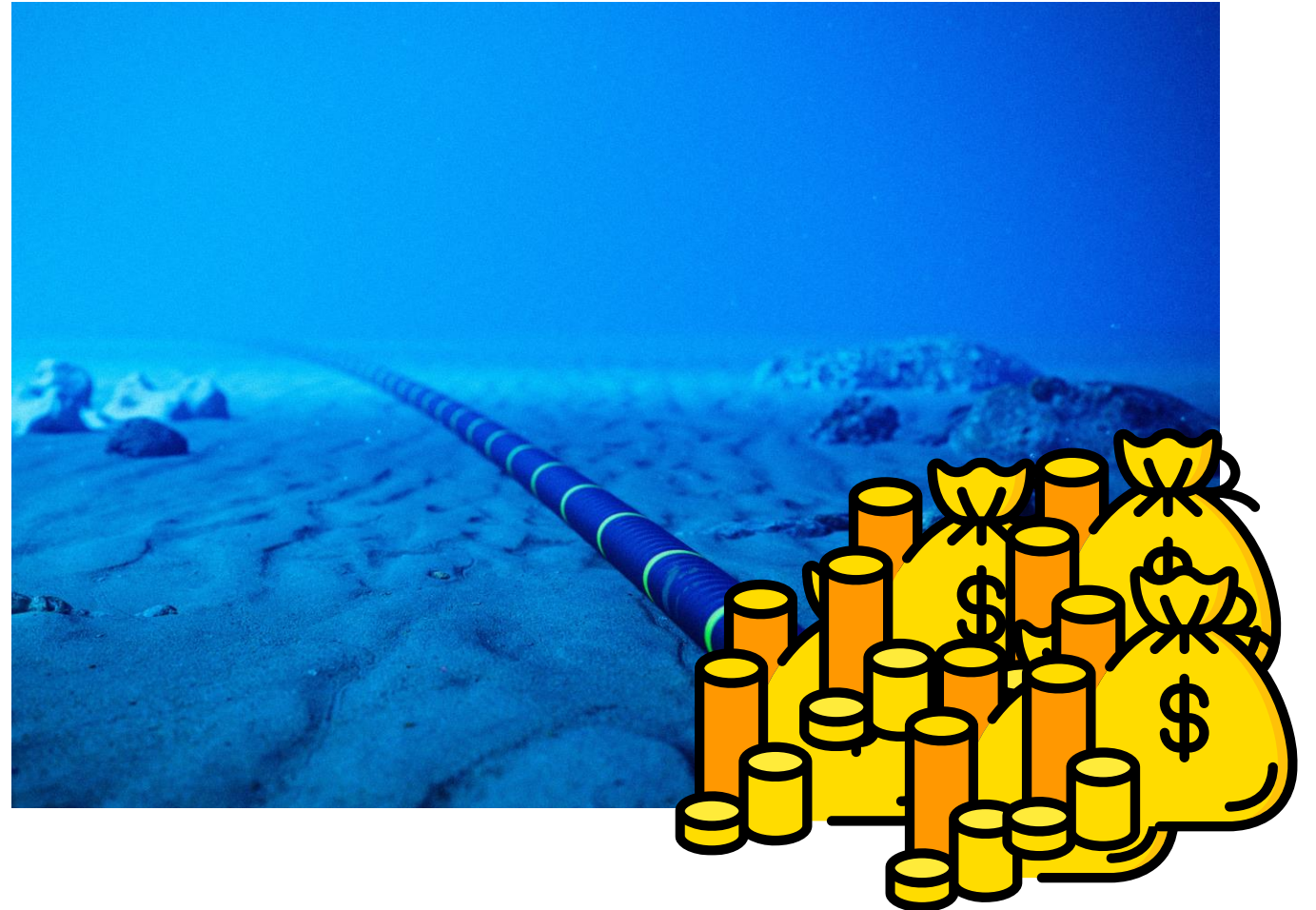
Wide area networks connect geographically distributed sites



Wide area networks are often used to transmit sensitive information



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

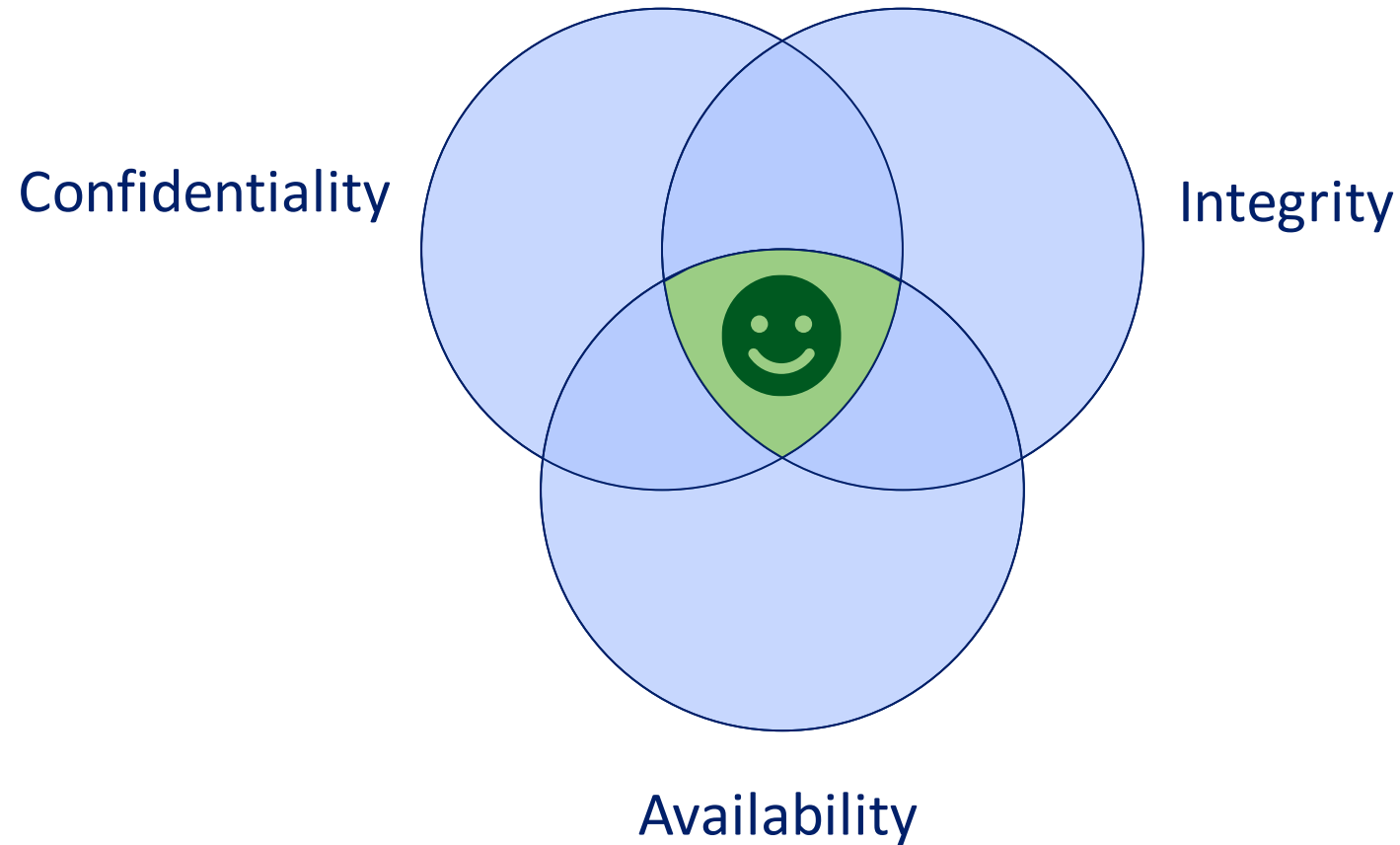


How can we build secure WANs
on shared infrastructure?

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

Confidentiality

Integrity

Availability

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** | **Use-cases**



How can we build secure WANs
on shared infrastructure?

Components | Roadmap | Use-cases



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

Traffic encryption

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



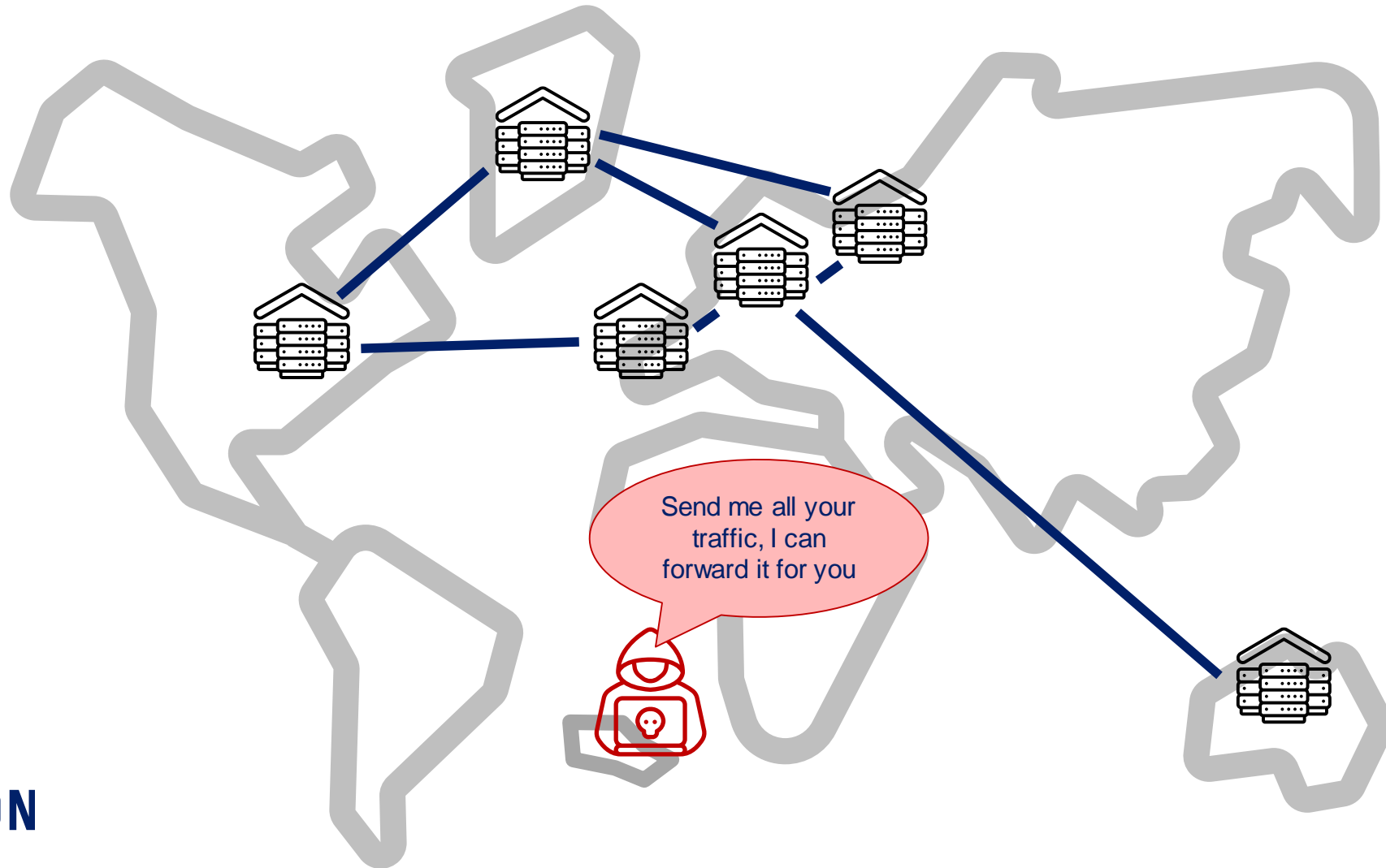
Padding and traffic shaping obfuscate the “shape” of packets



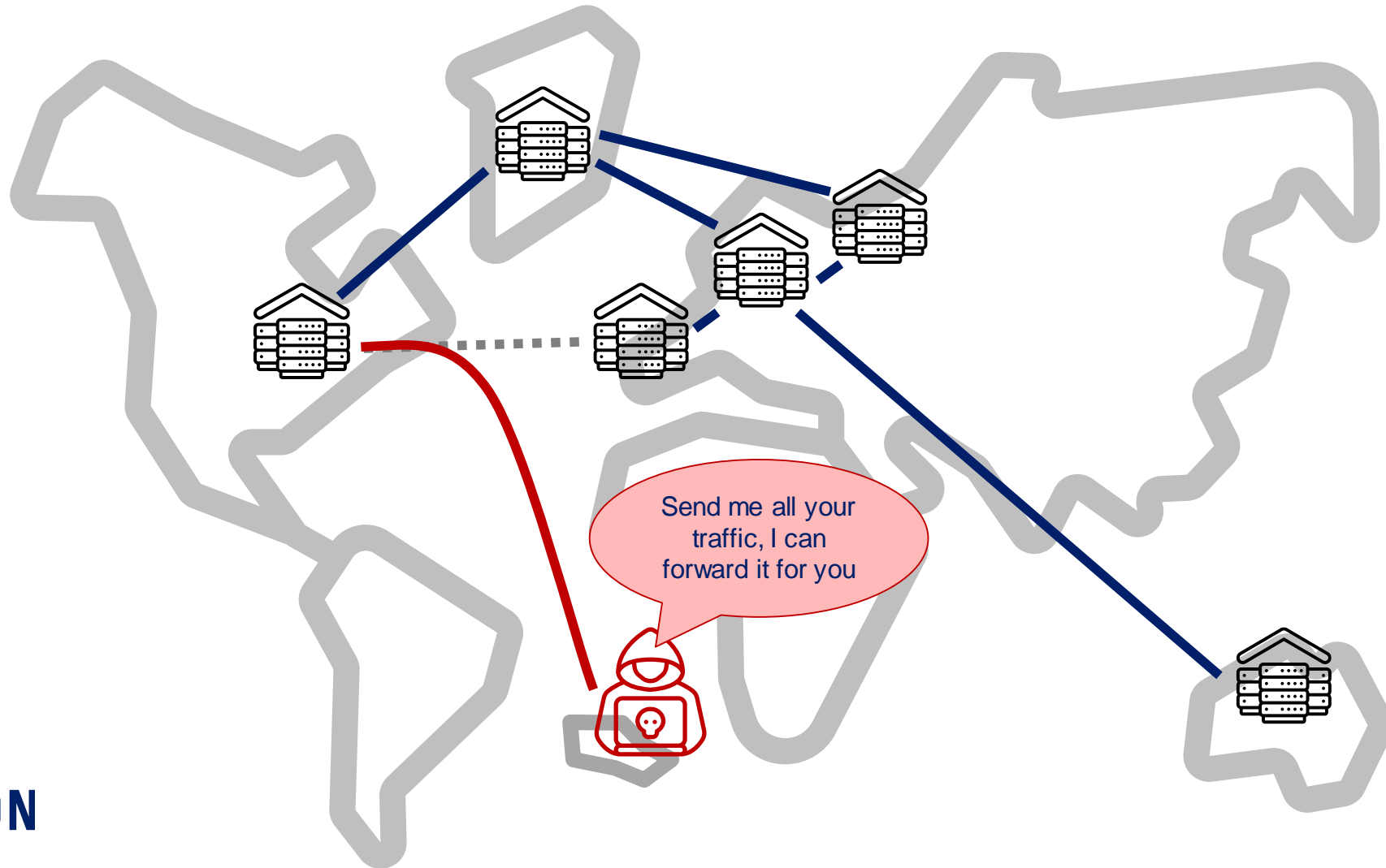
We identified the most relevant threats and possible mitigations

		Mitigations →	
		Traffic encryption	Traffic shaping and padding
Threats ↓			
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 said.

The Record.
Recorded Future News



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.

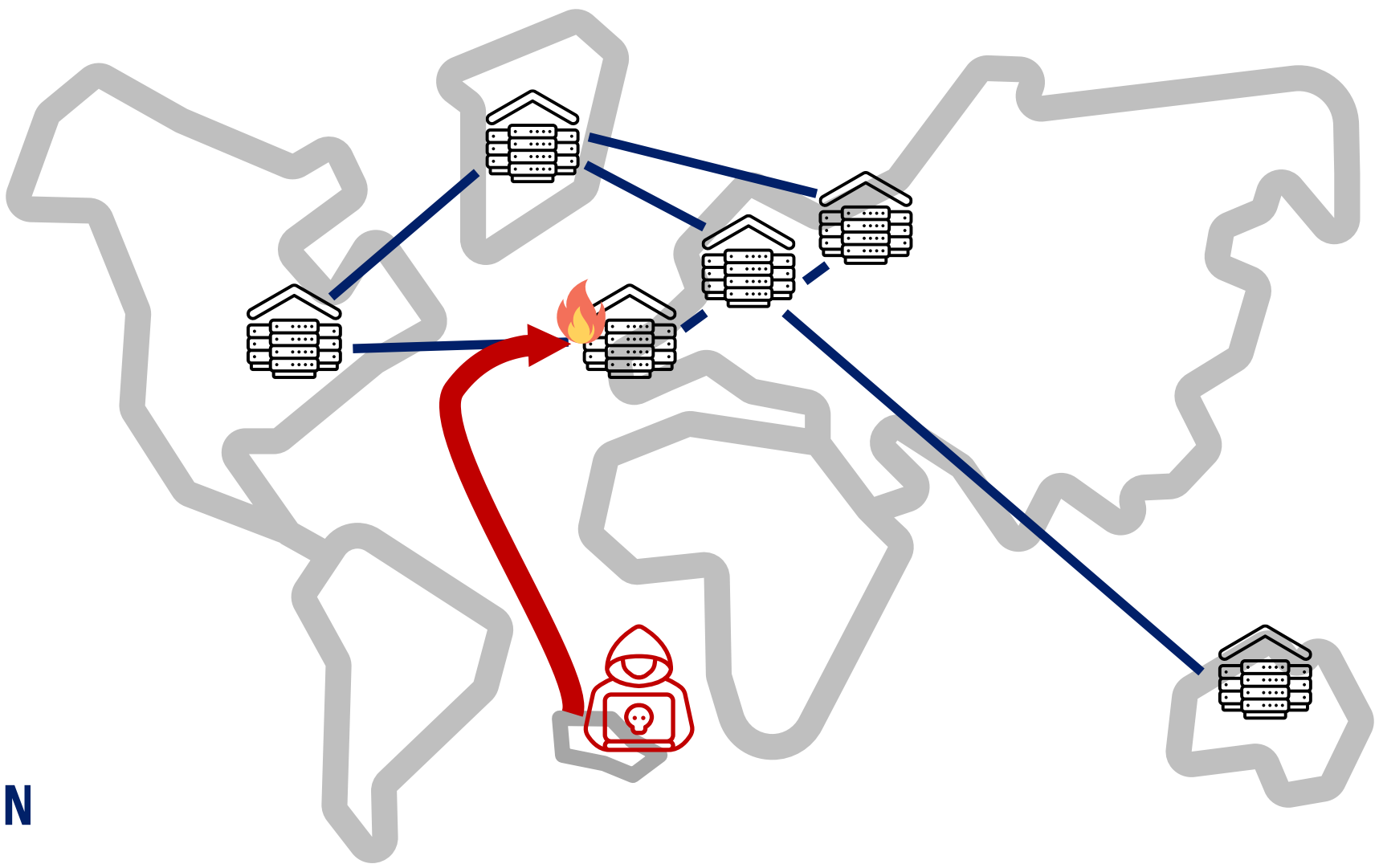
The attack took place earlier this month, on February 3, lasted only for two hours, and KLAYswap has confirmed the incident last week and is currently issuing compensation for affected users.

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

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

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

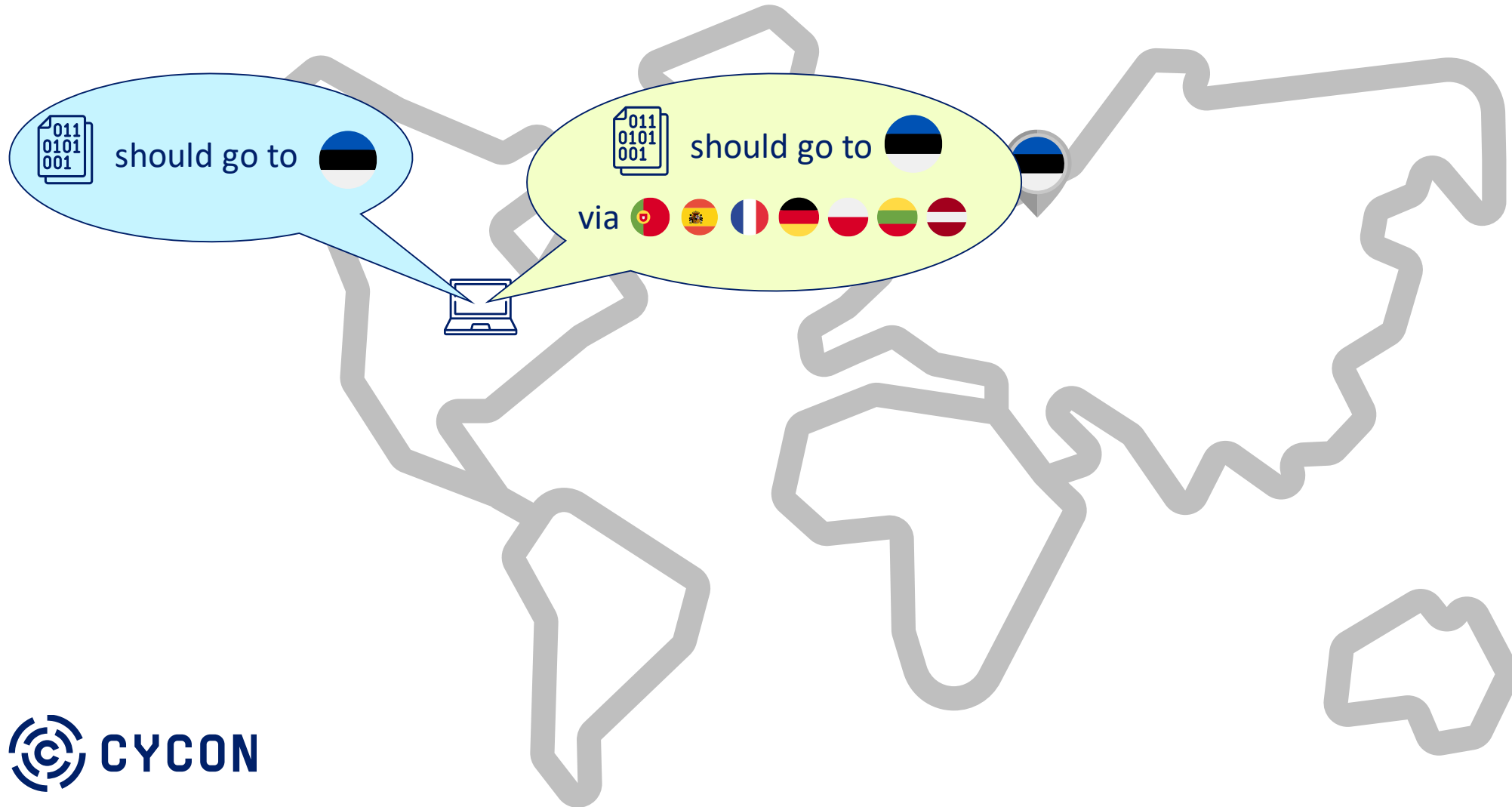
Mitigations can be implemented using a combination of existing (research) works

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

SCION is a new Internet routing architecture

Scalability,
Control, and
Isolation
On
Next-generation networks

The biggest difference between SCION and today's Internet is who selects the path



SCION started as a research project with the first publication in 2011

Abstract—We present the first Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. SCION separates ASes into groups of independent routing sub-planes, called *trust domains*, which then interconnect to form complete routes. Trust domains provide natural isolation of routing failures and human misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness. As a result, our architecture provides strong resilience and security properties as an intrinsic consequence of good design principles, avoiding piecemeal add-on protocols as security patches. Meanwhile, SCION only assumes that a few top-tier ISPs in the trust domain are trusted for providing reliable end-to-end communications, thus achieving a small Trusted Computing Base. Both our security analysis and evaluation results show that SCION naturally prevents numerous attacks and provides a high level of resilience, scalability, control, and isolation.



SCION: Scalability, Control, and Isolation On Next-Generation Networks

Xin Zhang, Hsu-Chun Hsiao, Geoffrey Haker, Haowen Chan, Adrian Perrig and David G. Andersen
CyLab / Carnegie Mellon University

Abstract—We present the first Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. SCION separates ASes into groups of independent routing sub-planes, called *trust domains*, which then interconnect to form complete routes. Trust domains provide natural isolation of routing failures and human misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness. As a result, our architecture provides strong resilience and security properties as an intrinsic consequence of good design principles, avoiding piecemeal add-on protocols as security patches. Meanwhile, SCION only assumes that a few top-tier ISPs in the trust domain are trusted for providing reliable end-to-end communications, thus achieving a small Trusted Computing Base. Both our security analysis and evaluation results show that SCION naturally prevents numerous attacks and provides a high level of resilience, scalability, control, and isolation.

I. INTRODUCTION

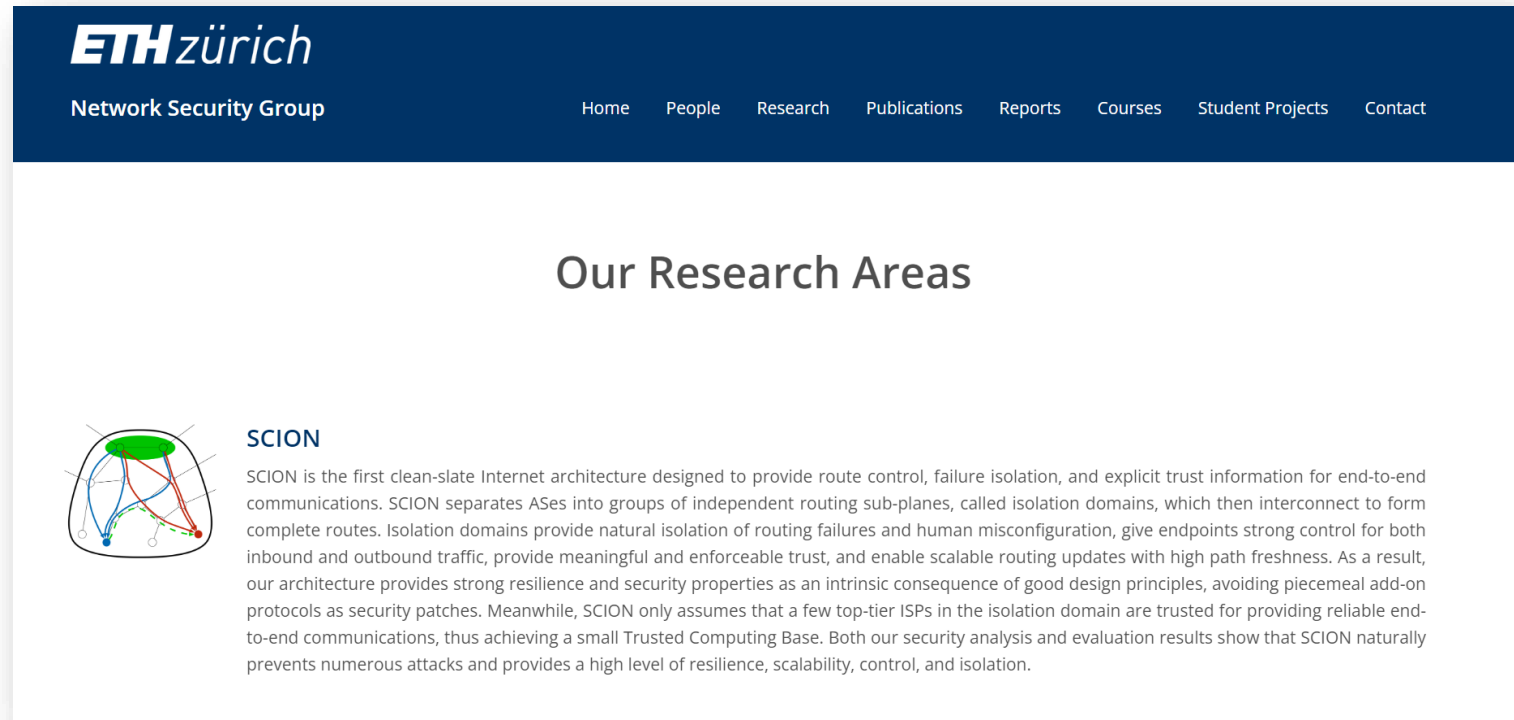
The Internet is the most geographically, administratively, and socially diverse distributed system ever invented. While today's Internet architecture admits some administrative diversity, such as by separating routing inside a domain (intra-AS routing) from global inter-domain routing, it falls short in handling the key challenges of security and isolation that arise in this intensely heterogeneous setting. As a result, we see surprisingly frequent incidents in which communication is interrupted by actions or actors far from the communicating entities. In addition to classical examples such as YouTube being globally disrupted by routing announcements from Pakistan [1], other issues surrounding the lack of resource control and isolation are not solved by existing proposals such as S-BGP [2]: the introduction of excessive routing churn [3]; traffic flooding; and even issues of global conflicts over naming and

to the endpoints diverse communication path sets that can support a wide spectrum of routing policies and path preferences (*path expressiveness*).

We introduce the notion of a hierarchy of *trust domains* whose members all share a common contractual, legal, cultural, geographical, or other basis for extending limited trust among each other. Examples may be a domain of U.S. commercial and educational institutions, ISPs that participate in the same peering point who share a common, binding legal contract on their behavior, or ISPs in the same state or country who are subject to the same laws and regulations. Using this abstraction, we provide the machinery to guarantee control-plane isolation: *Entities outside a trust domain cannot affect control-plane computation and communication within that trust domain*. For communication that must span trust domains, we provide the property that *the entities who can affect the communication are limited to a necessary and explicitly identified set of other trust domains*. We leave data-plane security as future work and thus do not consider denial of service attacks. In addition, the introduction of trust domains enables sources, transit ISPs, and destinations in SCION to agree *jointly* on which path to use. The architecture naturally controls routing information flow, and provides for explicit trust in path selection.

Through isolation and control, SCION enables expressive trust, i.e., *all the communicating endpoints can decide and control explicitly and precisely whom they need to trust for providing reliable communications*. Exposing such explicit trust information for end-to-end communication can eventually benefit network availability, because the endpoints can select more "trusted" communication paths with presumably more reliable data-link layers, even if SCION holds the routing

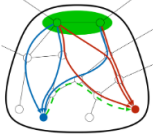
Researchers from ETH Zürich are leading the academic development of SCION



ETH zürich
Network Security Group

Home People Research Publications Reports Courses Student Projects Contact

Our Research Areas



SCION

SCION is the first clean-slate Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. SCION separates ASes into groups of independent routing sub-planes, called isolation domains, which then interconnect to form complete routes. Isolation domains provide natural isolation of routing failures and human misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness. As a result, our architecture provides strong resilience and security properties as an intrinsic consequence of good design principles, avoiding piecemeal add-on protocols as security patches. Meanwhile, SCION only assumes that a few top-tier ISPs in the isolation domain are trusted for providing reliable end-to-end communications, thus achieving a small Trusted Computing Base. Both our security analysis and evaluation results show that SCION naturally prevents numerous attacks and provides a high level of resilience, scalability, control, and isolation.

Many more publications followed...

Google Scholar

SCION: Scalability, Control, and Isolation On Next-Generation Networks

Articles About 313 results (0.07 sec)

Any time
Since 2024
Since 2023
Since 2020
Custom range...

SCION: Scalability, control, and isolation on next-generation networks [PDF] dtic.mil

X Zhang, HC Hsiao, G Hasker, H Chan... - ... IEEE Symposium on ..., 2011 - [ieeexplore.ieee.org](#)

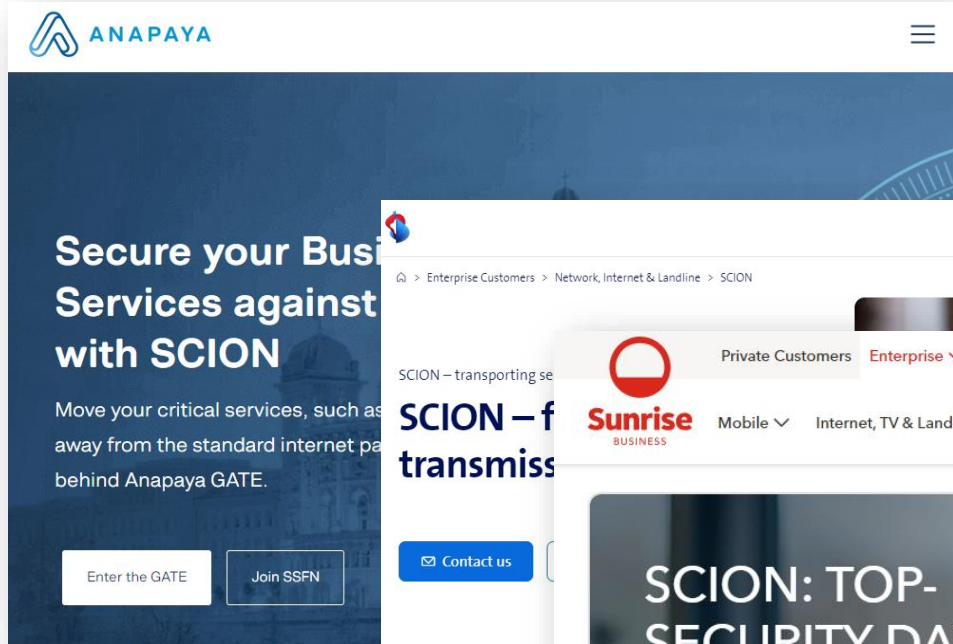
... architecture, **SCION**, that provides strong guarantees for failure **isolation** and route **control** in ... We show that strong **control** and **isolation** naturally leads to security and reliability without ...

☆ Save Cite **Cited by 246** Related articles All 21 versions

... and also commercial offerings

— Anapaya (ETH Spin-Off) in 2017

ISP offerings
around 2020

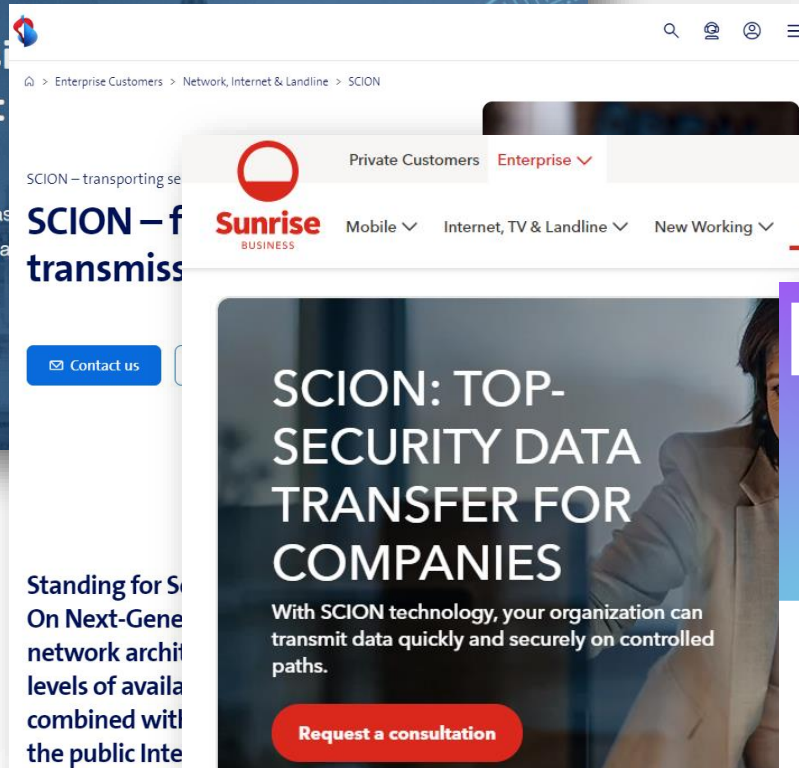


ANAPAYA

Secure your Business Services against attacks with SCION

Move your critical services, such as cloud services, away from the standard internet path and behind Anapaya GATE.

Enter the GATE | Join SSFN



Enterprise Customers > Network, Internet & Landline > SCION

SCION – transporting services securely

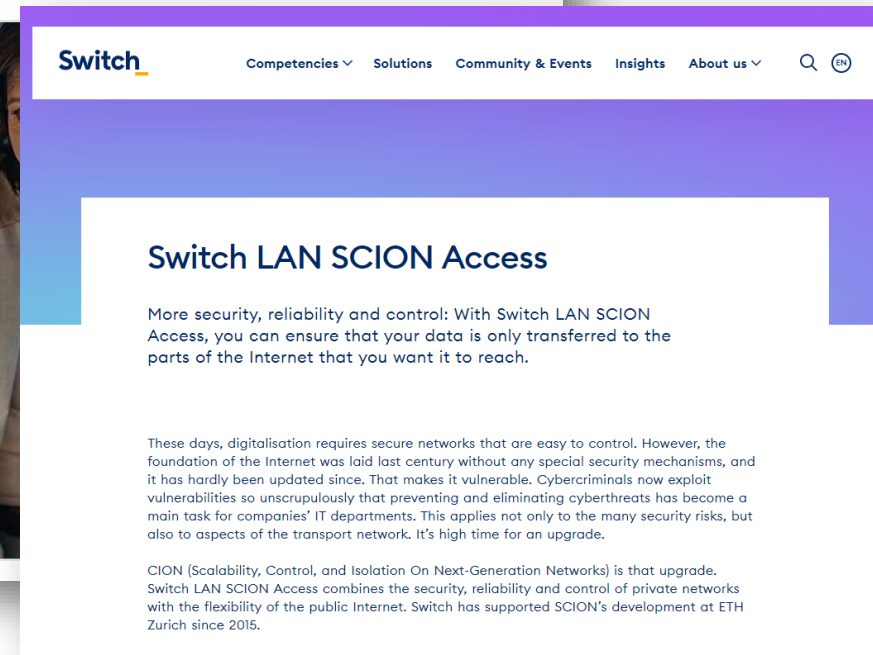
SCION – fast and secure data transmission

Contact us

SCION: TOP-SECURITY DATA TRANSFER FOR COMPANIES

With SCION technology, your organization can transmit data quickly and securely on controlled paths.

Request a consultation



Switch

Competencies | Solutions | Community & Events | Insights | About us

Switch LAN SCION Access

More security, reliability and control: With Switch LAN SCION Access, you can ensure that your data is only transferred to the parts of the Internet that you want it to reach.

These days, digitalisation requires secure networks that are easy to control. However, the foundation of the Internet was laid last century without any special security mechanisms, and it has hardly been updated since. That makes it vulnerable. Cybercriminals now exploit vulnerabilities so unscrupulously that preventing and eliminating cyberthreats has become a main task for companies' IT departments. This applies not only to the many security risks, but also to aspects of the transport network. It's high time for an upgrade.

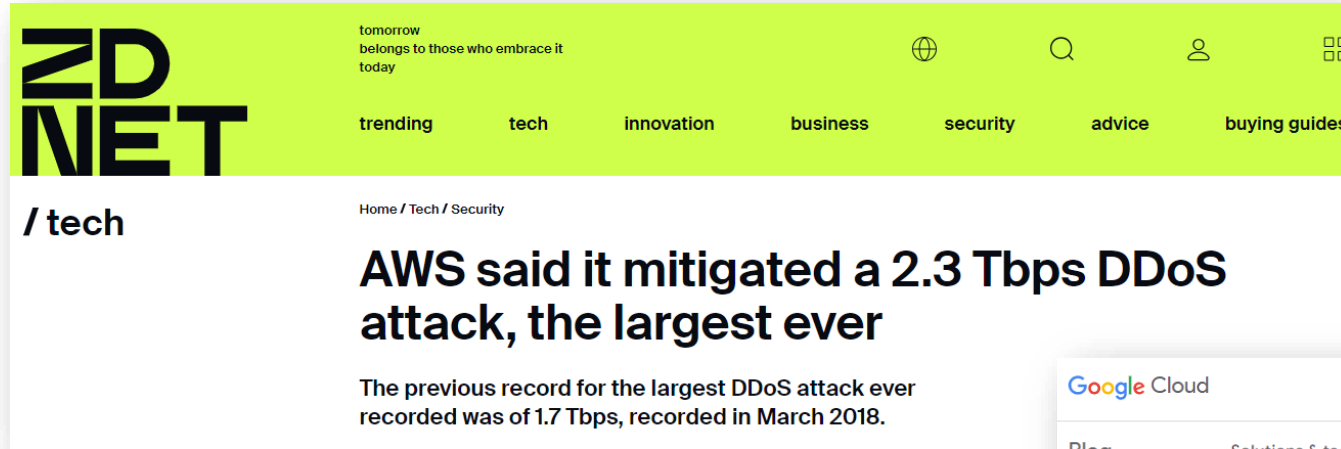
SCION (Scalability, Control, and Isolation On Next-Generation Networks) is that upgrade. Switch LAN SCION Access combines the security, reliability and control of private networks with the flexibility of the public Internet. Switch has supported SCION's development at ETH Zurich since 2015.



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					✓		✓

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



tomorrow belongs to those who embrace it today

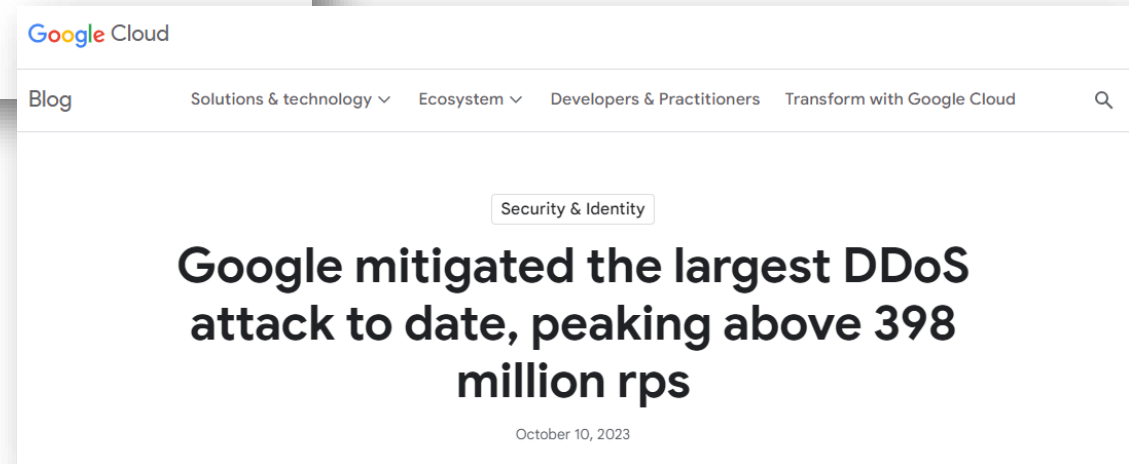
trending tech innovation business security advice buying guides

/ tech

Home / Tech / Security

AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever

The previous record for the largest DDoS attack ever recorded was of 1.7 Tbps, recorded in March 2018.



Google Cloud

Blog Solutions & technology Ecosystem Developers & Practitioners Transform with Google Cloud

Security & Identity

Google mitigated the largest DDoS attack to date, peaking above 398 million rps

October 10, 2023

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** | Use-cases

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	

We built a testbed using commercially available SCION connectivity



How can we build secure WANs on shared infrastructure?

Components | Roadmap | **Use-cases**

Locked Shields is the largest live-fire global cyber defense exercise

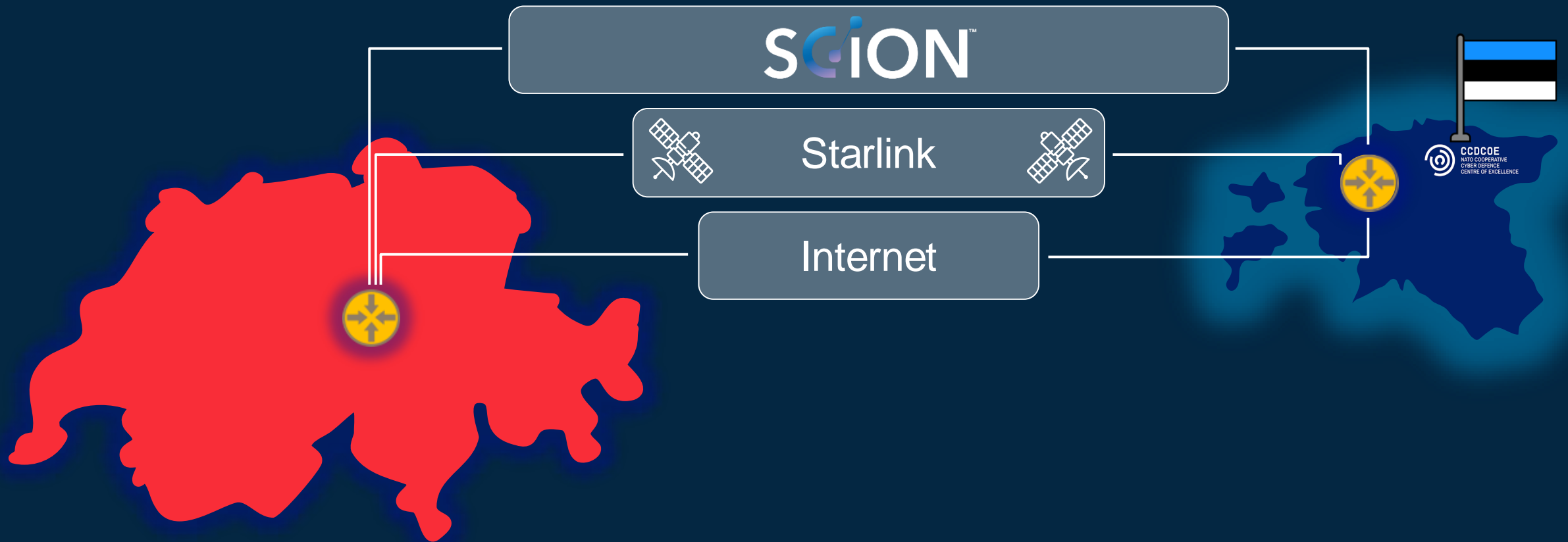


- Red team (attackers) vs. Blue teams (defenders)
 - 1 Red team
 - ~20 Blue teams from different countries
- Game infrastructure is in Estonia
- Blue teams connect remotely via VPN

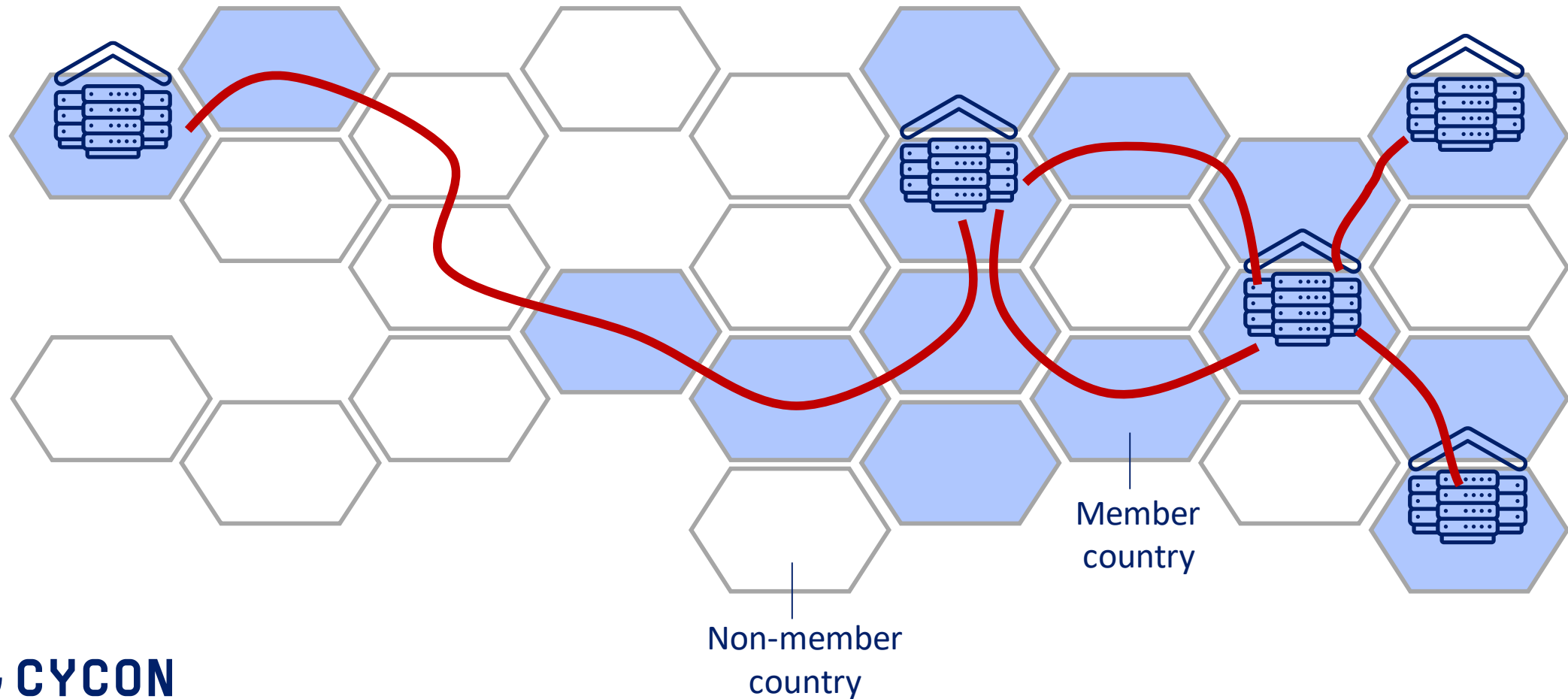
The CYD Campus helped the Swiss Blue Team at Locked Shields to use SCION



The Swiss Blue Team used three independent networks to access the Locked Shields network



Our architecture allows cost-effective WANs spanning over many countries



How can we build secure WANs on shared infrastructure?

Components | Roadmap | Use-cases

Thanks for your attention

How can we build secure WANs on shared infrastructure?

Components | Roadmap | Use-cases



Roland Meier
roland.meier@ar.admin.ch

