ETH zürich

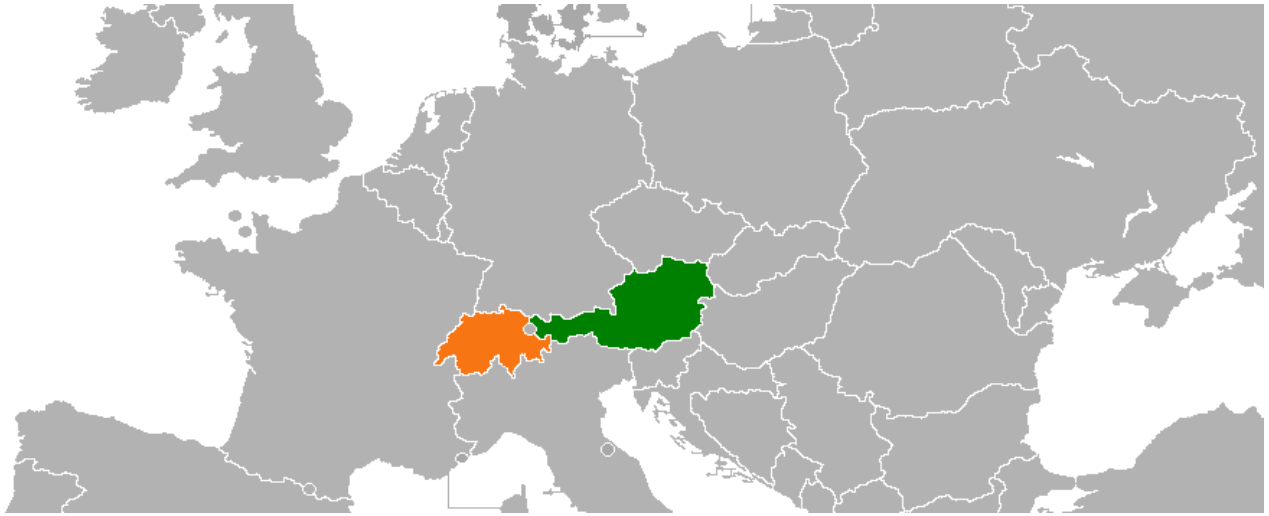
SCION

SCION: eine sichere Internetarchitektur

Dr. Markus Legner
Network Security Group, ETH Zürich
ATNOG 2020/1, 2020-11-24

$ whoami

- aufgewachsen in Axams bei Innsbruck
- Physik-Studium und -Doktorat an der ETH Zürich
- seit 2017 beteiligt am SCION-Projekt
- seit 2018 Postdoktorand und Dozent in der *Network Security Group* (geleitet von Prof. Adrian Perrig)



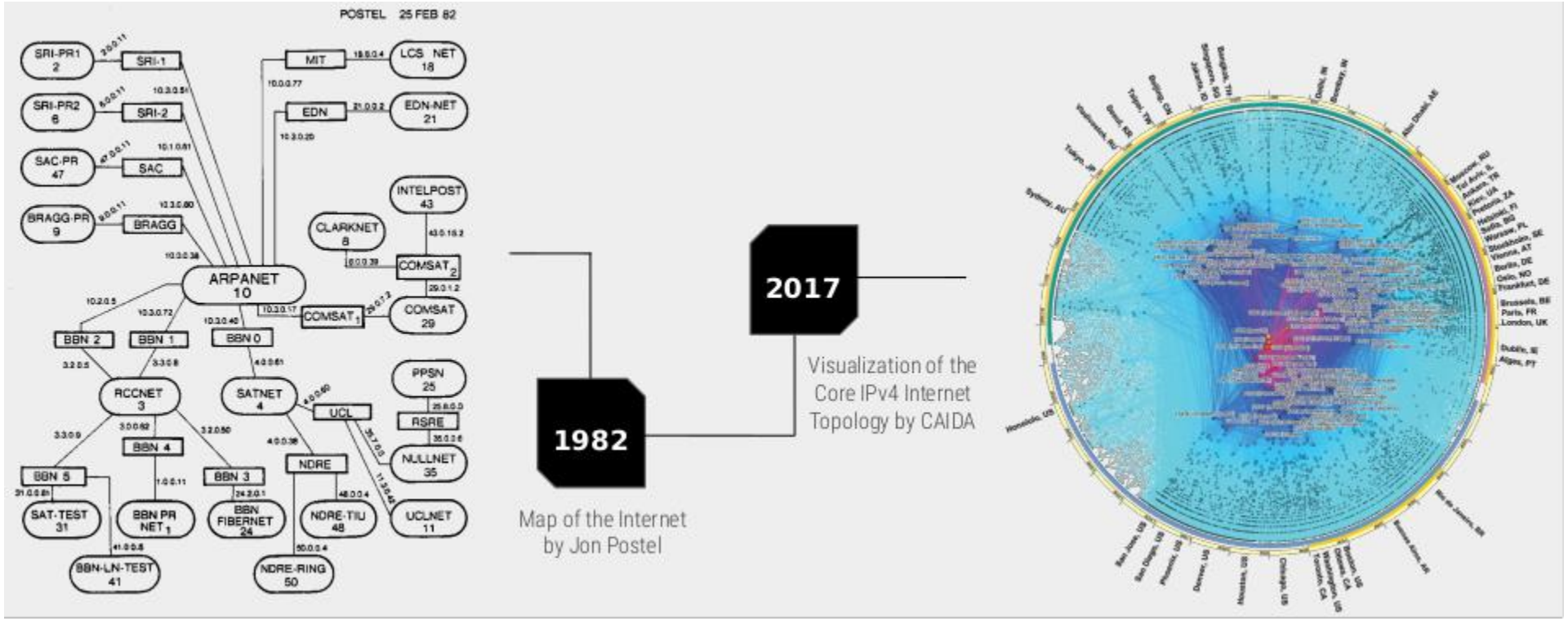
1. Image: https://commons.wikimedia.org/wiki/File:Austria_Switzerland_Locator.png

Worum geht es in meiner Präsentation?

1. Warum entwickeln wir eine neue Internetarchitektur?
2. Was ist SCION und wie unterscheidet es sich vom heutigen Internet?
3. Welche Vorteile bietet SCION und welche Anwendungen werden durch SCION ermöglicht?
4. Was ist der heutige Status der SCION-Architektur?

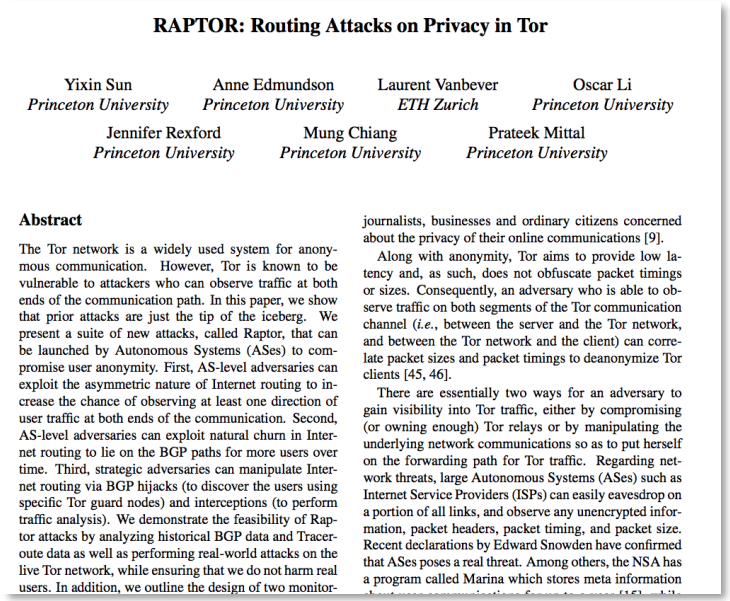
Warum entwickeln wir eine neue Internetarchitektur?

Das Internet ist ein bemerkenswertes System, das aber nicht für die heutigen Grössenordnungen, Anwendungen und Bedrohungen designt wurde.



1. Image credit: https://blog.apnic.net/2020/11/03/tcp-path-brokenness-and-transport-layer-evolution/

Zahlreiche Systeme verlassen sich darauf, dass Pakete am richtigen Ort ankommen...



RAPTOR: Routing Attacks on Privacy in Tor

Yixin Sun, *Princeton University*; Anne Edmundson, *Princeton University*; Laurent Vanbever, *ETH Zurich*; Oscar Li, *Princeton University*; Jennifer Rexford, *Princeton University*; Mung Chiang, *Princeton University*; Prateek Mittal, *Princeton University*

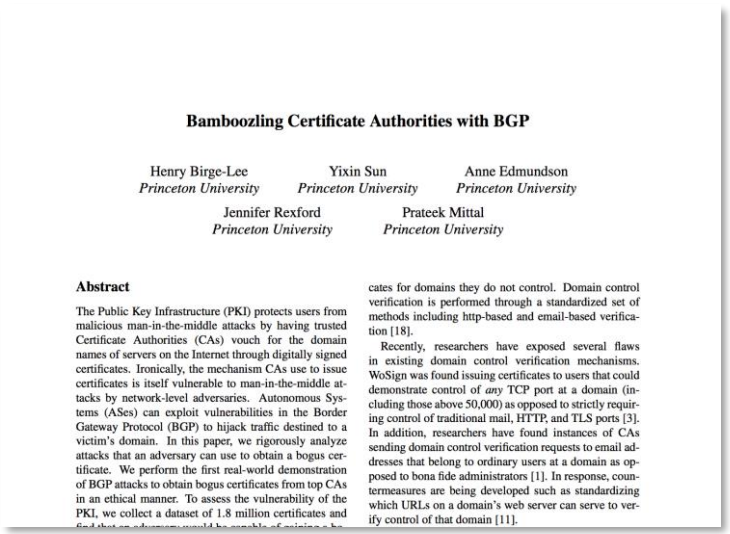
Abstract

The Tor network is a widely used system for anonymous communication. However, Tor is known to be vulnerable to attackers who can observe traffic at both ends of the communication path. In this paper, we show that prior attacks are just the tip of the iceberg. We present a suite of new attacks, called Raptor, that can be launched by Autonomous Systems (ASes) to compromise user anonymity. First, AS-level adversaries can exploit the asymmetric nature of Internet routing to increase the chance of observing at least one direction of user traffic at both ends of the communication. Second, AS-level adversaries can exploit natural churn in Internet routing to lie on the BGP paths for more users over time. Third, strategic adversaries can manipulate Internet routing via BGP hijacks (to discover the users using specific Tor guard nodes) and interceptions (to perform traffic analysis). We demonstrate the feasibility of Raptor attacks by analyzing historical BGP data and Traceroute data as well as performing real-world attacks on the live Tor network, while ensuring that we do not harm real users. In addition, we outline the design of two monitor-

journalists, businesses and ordinary citizens concerned about the privacy of their online communications [9].

Along with anonymity, Tor aims to provide low latency and, as such, does not obfuscate packet timings or sizes. Consequently, an adversary who is able to observe traffic on both segments of the Tor communication channel (*i.e.*, between the server and the Tor network, and between the Tor network and the client) can correlate packet sizes and packet timings to deanonymize Tor clients [45, 46].

There are essentially two ways for an adversary to gain visibility into Tor traffic, either by compromising (or owning enough) Tor relays or by manipulating the underlying network communications so as to put herself on the forwarding path for Tor traffic. Regarding network threats, large Autonomous Systems (ASes) such as Internet Service Providers (ISPs) can easily eavesdrop on a portion of all links, and observe any unencrypted information, packet headers, packet timing, and packet size. Recent declarations by Edward Snowden have confirmed that ASes poses a real threat. Among others, the NSA has a program called Marina which stores meta information



Bamboozling Certificate Authorities with BGP

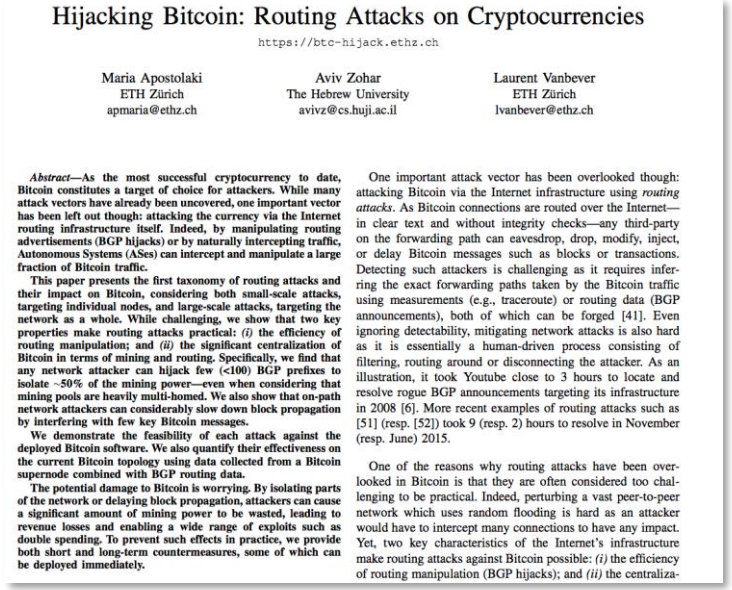
Henry Birge-Lee, *Princeton University*; Yixin Sun, *Princeton University*; Anne Edmundson, *Princeton University*; Jennifer Rexford, *Princeton University*; Prateek Mittal, *Princeton University*

Abstract

The Public Key Infrastructure (PKI) protects users from malicious man-in-the-middle attacks by having trusted Certificate Authorities (CAs) vouch for the domain names of servers on the Internet through digitally signed certificates. Ironically, the mechanism CAs use to issue certificates is itself vulnerable to man-in-the-middle attacks by network-level adversaries. Autonomous Systems (ASes) can exploit vulnerabilities in the Border Gateway Protocol (BGP) to hijack traffic destined to a victim's domain. In this paper, we rigorously analyze attacks that an adversary can use to obtain a bogus certificate. We perform the first real-world demonstration of BGP attacks to obtain bogus certificates from top CAs in an ethical manner. To assess the vulnerability of the PKI, we collect a dataset of 1.8 million certificates and

cates for domains they do not control. Domain control verification is performed through a standardized set of methods including http-based and email-based verification [18].

Recently, researchers have exposed several flaws in existing domain control verification mechanisms. WoSign was found issuing certificates to users that could demonstrate control of *any* TCP port at a domain (including those above 50,000) as opposed to strictly requiring control of traditional mail, HTTP, and TLS ports [3]. In addition, researchers have found instances of CAs sending domain control verification requests to email addresses that belong to ordinary users at a domain as opposed to bona fide administrators [1]. In response, countermeasures are being developed such as standardizing which URLs on a domain's web server can serve to verify control of that domain [11].



Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

https://btc-hijack.ethz.ch

Maria Apostolaki, ETH Zürich, apmaria@ethz.ch; Aviv Zohar, The Hebrew University, avivz@cs.huji.ac.il; Laurent Vanbever, ETH Zürich, lvanbever@ethz.ch

***Abstract*—As the most successful cryptocurrency to date, Bitcoin constitutes a target of choice for attackers. While many attack vectors have already been uncovered, one important vector has been left out though: attacking the currency via the Internet routing infrastructure itself. Indeed, by manipulating routing advertisements (BGP hijacks) or by naturally intercepting traffic, Autonomous Systems (ASes) can intercept and manipulate a large fraction of Bitcoin traffic.**

This paper presents the first taxonomy of routing attacks and their impact on Bitcoin, considering both small-scale attacks, targeting individual nodes, and large-scale attacks, targeting the network as a whole. While challenging, we show that two key properties make routing attacks practical: *(i)* the efficiency of routing manipulation; and *(ii)* the significant centralization of Bitcoin in terms of mining and routing. Specifically, we find that any network attacker can hijack few (<100) BGP prefixes to isolate ~50% of the mining power—even when considering that mining pools are heavily multi-homed. We also show that on-path network attackers can considerably slow down block propagation by interfering with few key Bitcoin messages.

We demonstrate the feasibility of each attack against the deployed Bitcoin software. We also quantify their effectiveness on the current Bitcoin topology using data collected from a Bitcoin supernode combined with BGP routing data.

The potential damage to Bitcoin is worrying. By isolating parts of the network or delaying block propagation, attackers can cause a significant amount of mining power to be wasted, leading to revenue losses and enabling a wide range of exploits such as double spending. To prevent such effects in practice, we provide both short and long-term countermeasures, some of which can be deployed immediately.

One important attack vector has been overlooked though: attacking Bitcoin via the Internet infrastructure using *routing attacks*. As Bitcoin connections are routed over the Internet—in clear text and without integrity checks—any third-party on the forwarding path can eavesdrop, drop, modify, inject, or delay Bitcoin messages such as blocks or transactions. Detecting such attackers is challenging as it requires inferring the exact forwarding paths taken by the Bitcoin traffic using measurements (e.g., traceroute) or routing data (BGP announcements), both of which can be forged [41]. Even ignoring detectability, mitigating network attacks is also hard as it is essentially a human-driven process consisting of filtering, routing around or disconnecting the attacker. As an illustration, it took Youtube close to 3 hours to locate and resolve rogue BGP announcements targeting its infrastructure in 2008 [6]. More recent examples of routing attacks such as [51] (resp. [52]) took 9 (resp. 2) hours to resolve in November (resp. June) 2015.

One of the reasons why routing attacks have been overlooked in Bitcoin is that they are often considered too challenging to be practical. Indeed, perturbing a vast peer-to-peer network which uses random flooding is hard as an attacker would have to intercept many connections to have any impact. Yet, two key characteristics of the Internet's infrastructure make routing attacks against Bitcoin possible: *(i)* the efficiency of routing manipulation (BGP hijacks); and *(ii)* the centraliza-

… was leider nicht immer der Fall ist.

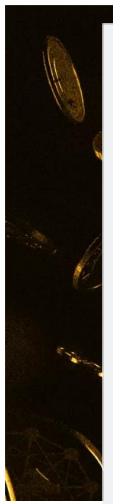
THE VERGE TECH

TECH CYBERSECURITY ENTERPRISE

Hackers emp
basic infrastr

By Russell Brandom | @russellbrandom |

SHARE



BORDER GATEWAY PROTOCOL —

How 3ve's BGP hijackers eluded the Internet—and made $29M

3ve used addresses of unsuspecting owners—like the US Air Force.

DAN GOODIN - 12/21/2018, 6:30 PM

THE ACCIDENTAL LEAK —

Google goes down after major BGP mishap routes traffic through China

Google says it doesn't believe leak was malicious despite suspicious appearances.

DAN GOODIN - 11/13/2018, 8:25 AM

SCIONs Vision:
ein sicheres, globales, öffentliches Internet.

- Hohe Sicherheit und Verfügbarkeit
- Netzwerk mit Pfadkontrolle und Multipath-Routing
- Globale Garantien für Kommunikation

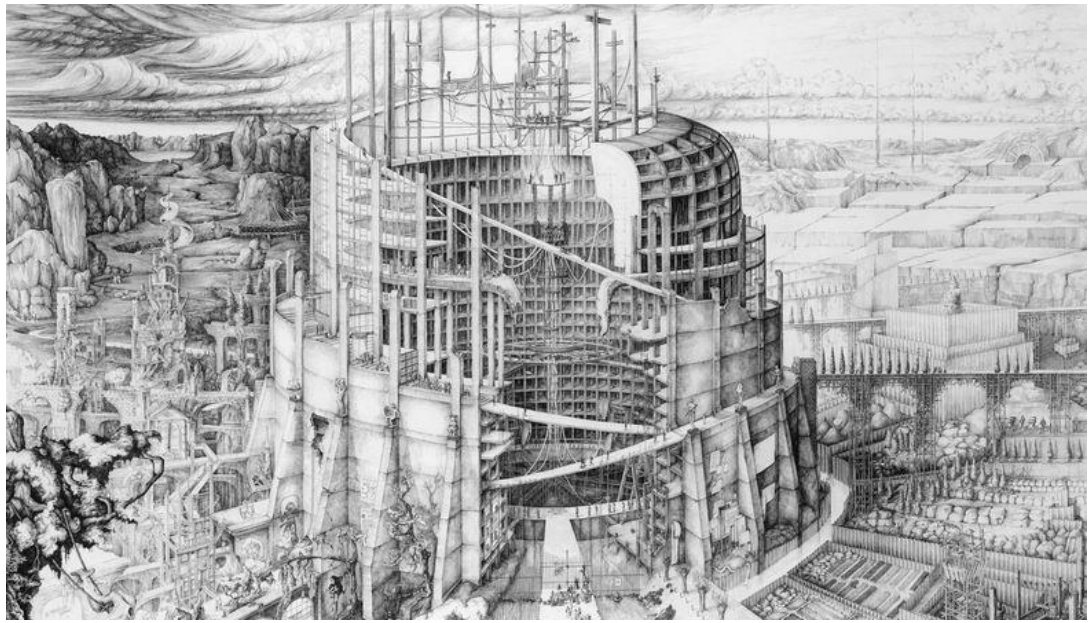
Was ist SCION und wie unterscheidet es sich vom heutigen Internet?

SCION ersetzt BGP und IP im *inter-domain*-Kontext.

- Routing-Architektur zwischen autonomen Systemem (ASes), ersetzt BGP
- Infrastruktur und Netzwerkprotokolle *innerhalb* eines AS werden nicht verändert
- Offen: Spezifikation und Referenzimplementierung sind frei verfügbar
- Höchst effizient, sogar schneller als das aktuelle Internet
- Hochsicher: Angriffe werden entweder vollständig verhindert oder zumindest abgeschwächt
- Netzwerk-Souveränität: lokale Vertrauensanker ermöglichen flexible Vertrauensbeziehungen und verhindern Angriffe von aussen
- Verifizierbar: Sicherheitsbeweise durch formale Methoden

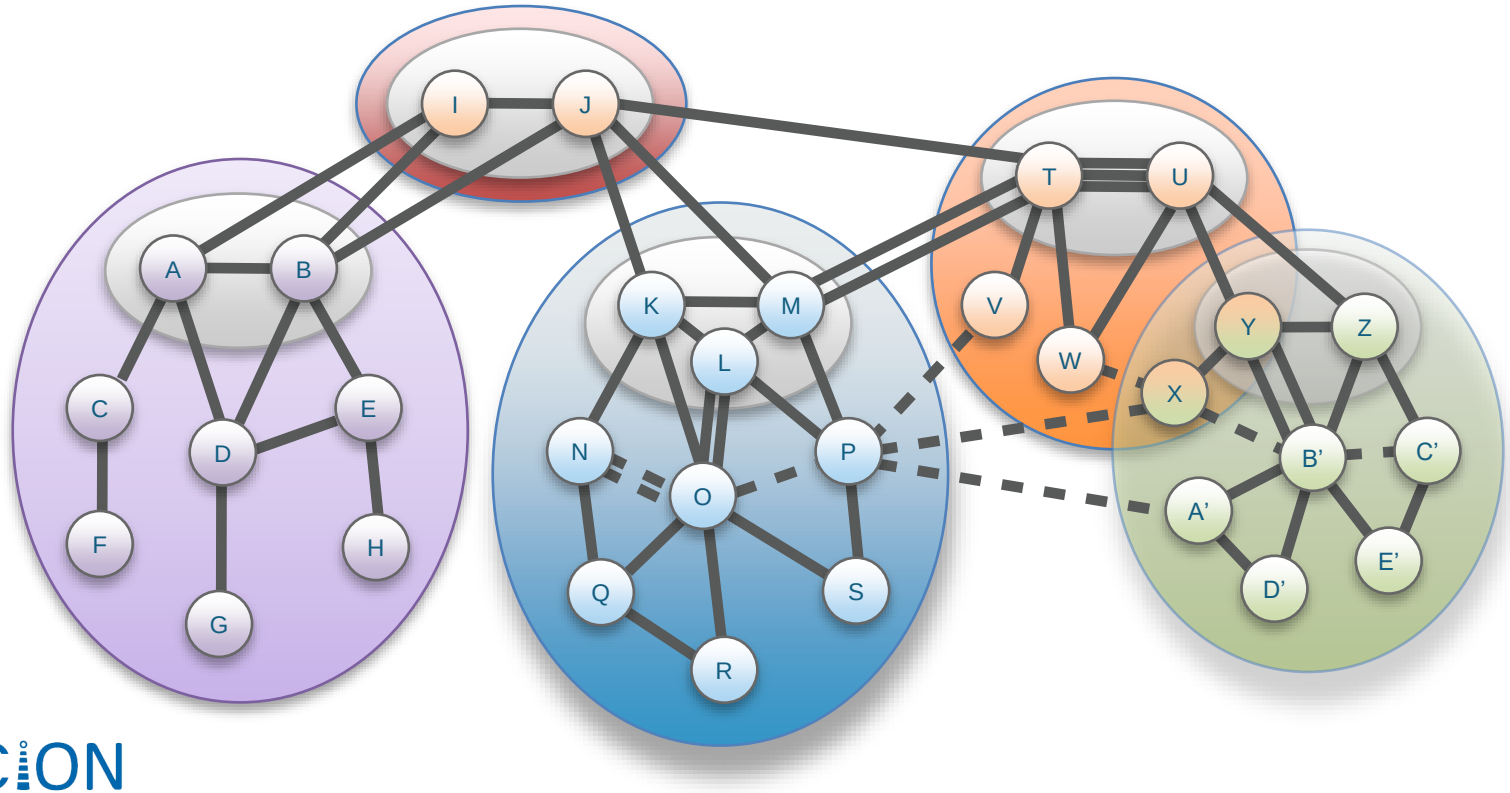
Design-Prinzipien der SCION-Architektur.

1. Paketweiterleitung ohne Routing-Tabellen («stateless forwarding»)
2. Konvergenz-freies Routing
3. Pfadkontrolle für Hosts
4. Multipath-Kommunikation
5. Hohe Sicherheit durch Design und formale Verifikation
6. Souveränität und Transparenz für Vertrauensanker



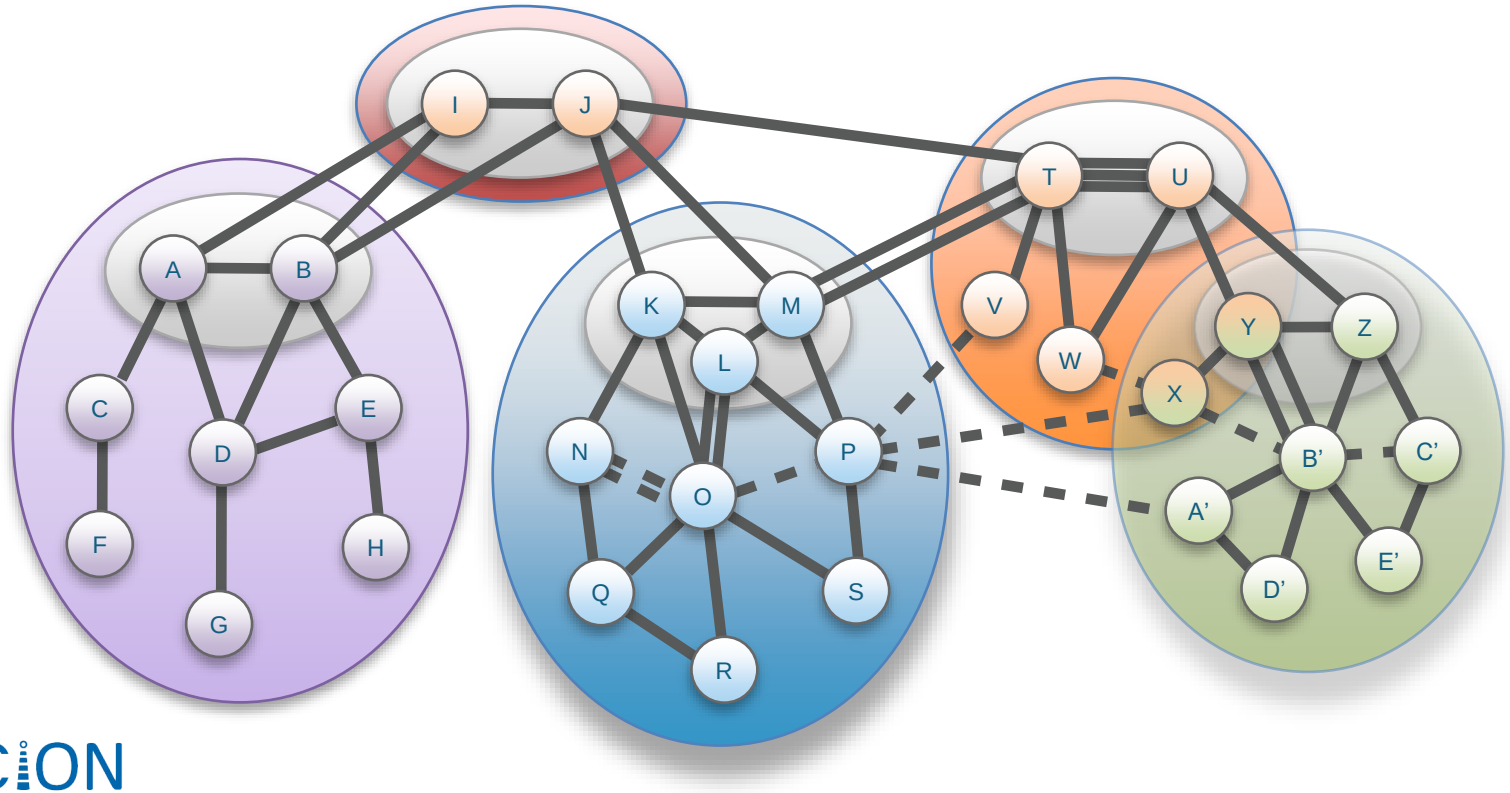
«Isolation Domains (ISDs)»: SCIONs Ansatz für Skalierbarkeit und Souveränität.

- Isolation Domain (ISD): Gruppierung von ASes (z.B. innerhalb gemeinsamer Jurisdiktionen)
- ISD core: ASes, die die ISD managen und globale Konnektivität sicherstellen



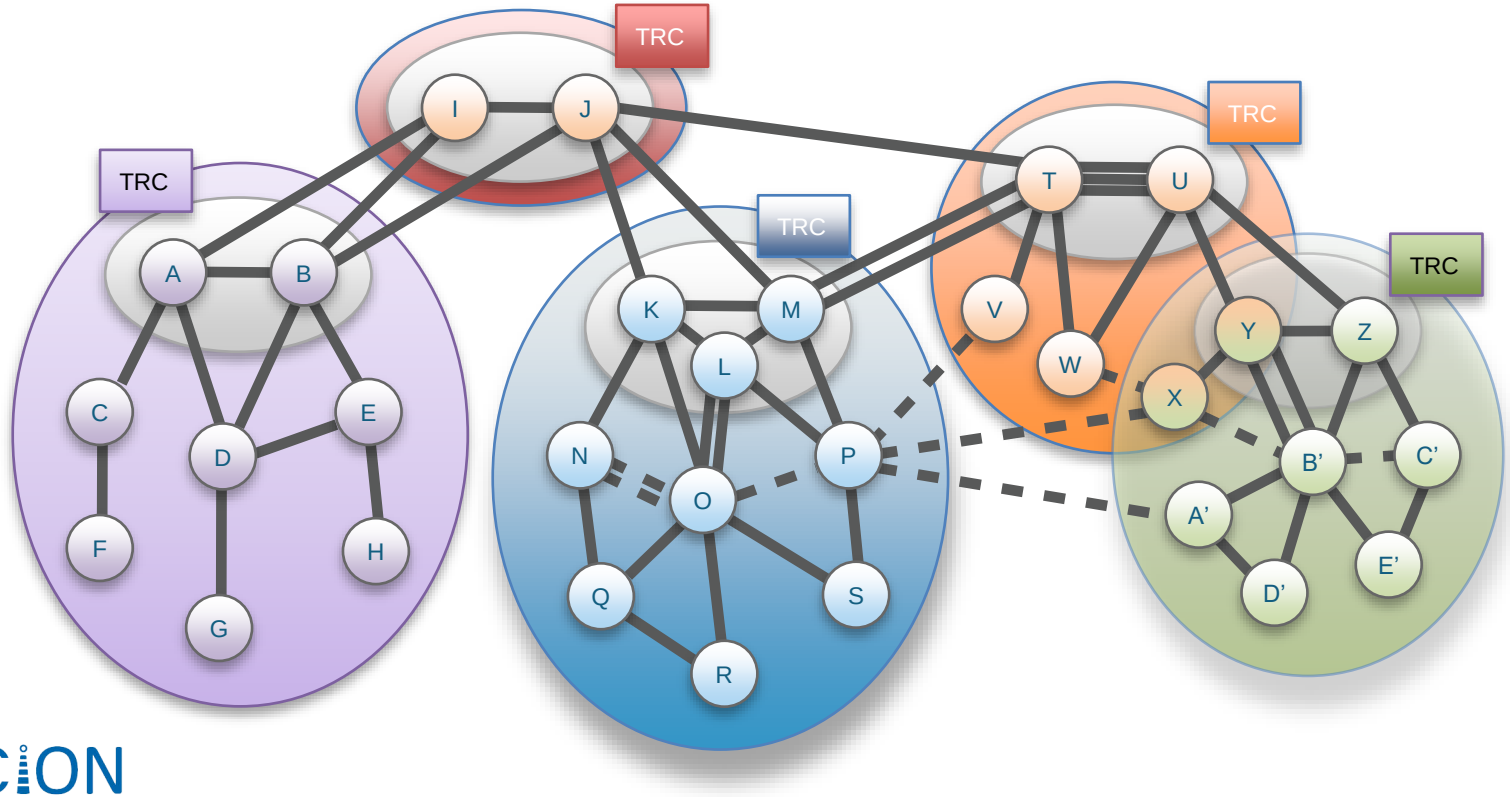
ISDs verbessern die Skalierbarkeit des Routing-Protokolls.

- Routing kann in einen intra-ISD und einen inter-ISD-Prozess aufgeteilt werden
- Ähnlich wie «Areas» in OSPF oder IS-IS



ISDs ermöglichen heterogene Vertrauensbeziehungen und Souveränität.

- Jede ISD kann ihre eigenen Vertrauensanker in einer «trust root configuration» (TRC) definieren
  - Löst Probleme von «Oligopoly»-Modellen (Web PKI) and «Monopoly»-Modellen (DNSSEC, RPKI)
- Externe Angreifer können den Routing-Prozess innerhalb einer ISD nicht beeinflussen



SCION auf einer Folie.

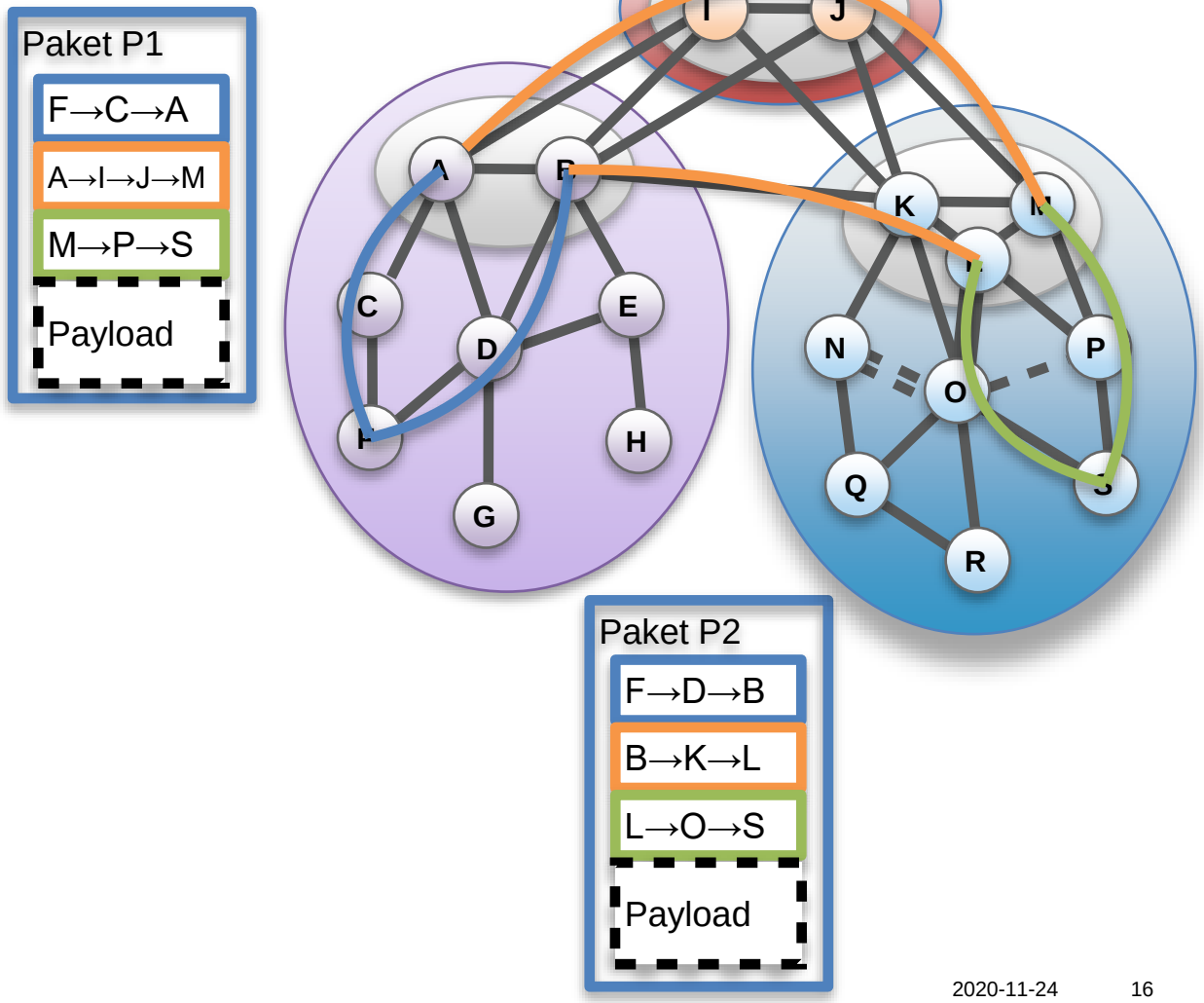
Pfad-basierte («path-aware») Netzwerk-Architektur

Kontrollebene: Routing

- Konstruiert und verteilt Pfad-Segmente

Datenebene: Paket-Weiterleitung

- Hosts verbinden Pfad-Segmente zu einem Pfad
- Datenpakete enthalten Pfad
- Router authentifizieren Informationen und leiten Paket weiter
  - → «Einfache» Router, keine Routing-Tabellen notwendig



Welche Vorteile bietet SCION und welche Anwendungen werden durch SCION ermöglicht?

Mit SCION sind Routing-Hijacks nicht mehr möglich.

- Alle Routing-Nachrichten sind signiert
- Hosts wählen Pfad aus und fügen ihn im Paket-Header ein → Angreifer, die nicht auf dem Pfad sind, können den Pfad nicht verändern
  - Hosts können Pfade auswählen, die nur vertrauenswürdige ASes traversieren
  - Ermöglicht «Geo-Fencing»
- Zusätzliche Extensions ermöglichen noch stärkere Sicherheitseigenschaften
  - Source authentication
  - Path validation

Welche Eigenschaften hat SCION im Vergleich zu BGP(sec)?

BGP	BGPsec	SCION
Keine Sicherheit	PKI mit «Kill Switch»	Flexible PKI
Einzelner Pfad	Einzelner Pfad	Multipath
Mässige Skalierbarkeit	Schlechtere Skalierbarkeit	Bessere Skalierbarkeit (ISDs)
Benötigt Konvergenz	Benötigt Konvergenz	Keine Konvergenz nötig

Ein Beispiel, warum Pfadkontrolle und Multipath-Kommunikation relevant sind.

- Generell gibt es zwei Netzwerkpfade zwischen Europa und Südostasien:
  - Hohe Latenz, hohe Bandbreite: westliche Route durch die USA, ~450ms RTT
  - Niedrige Latenz, kleine Bandbreite: östliche Route durch das Rote Meer, ~250ms RTT
- Mit BGP wird meist die günstigste Route ausgewählt, typischerweise diejenige mit der höchsten Bandbreite
- Je nach Applikation kann der eine oder andere Pfad sinnvoller sein
- Mit SCION können beide Pfade gleichzeitig verwendet werden

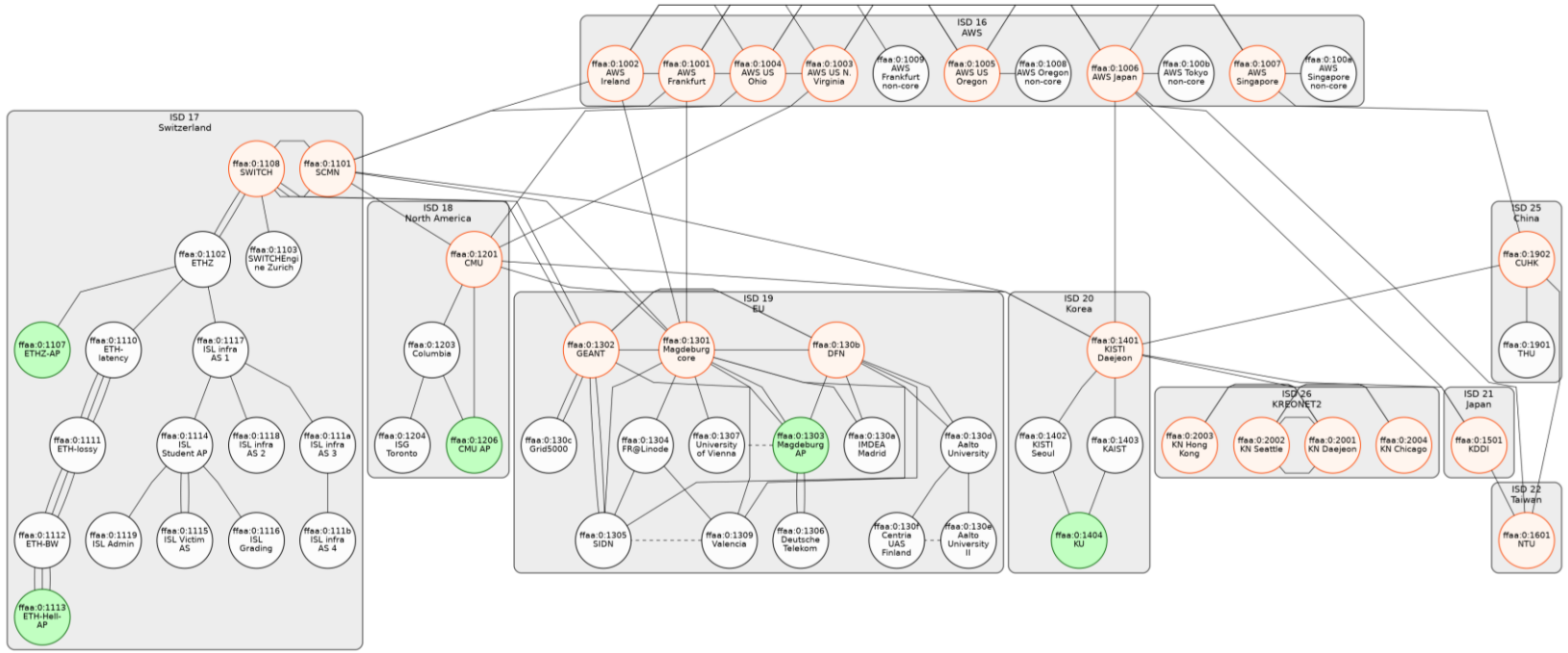
Was ist der heutige Status der SCION-Architektur?

SCION ist bereits heute Realität.

- Mehr als 11 Jahre Forschung, 150+ Personenjahre investiert
- Production-grade Implementierung entwickelt von ETH-Spin-off Anapaya
- Natives (BGP-freies) SCION-Netzwerk über 7 ISPs in der Schweiz und in Asien
- Konnektivität in 60+ Rechenzentren
- Im Einsatz bei der Schweizer Nationalbank, weiteren Banken, und der Schweizer Bundesverwaltung

SCIONLab: ein SCION-basiertes globales Netzwerk-Testbed. https://www.scionlab.org/

- Offen für alle Interessierten: erzeuge ein AS und verbinde dich mit dem Netzwerk innerhalb weniger Minuten
- ISPs in Europa: Swisscom, SWITCH, KDDI, GEANT, DFN
- Korea: GLORIAD, KISTI (KREONET), KU, KAIST, ETRI
- 35+ permanente Ases weltweit, 600+ Forschungs-ASes

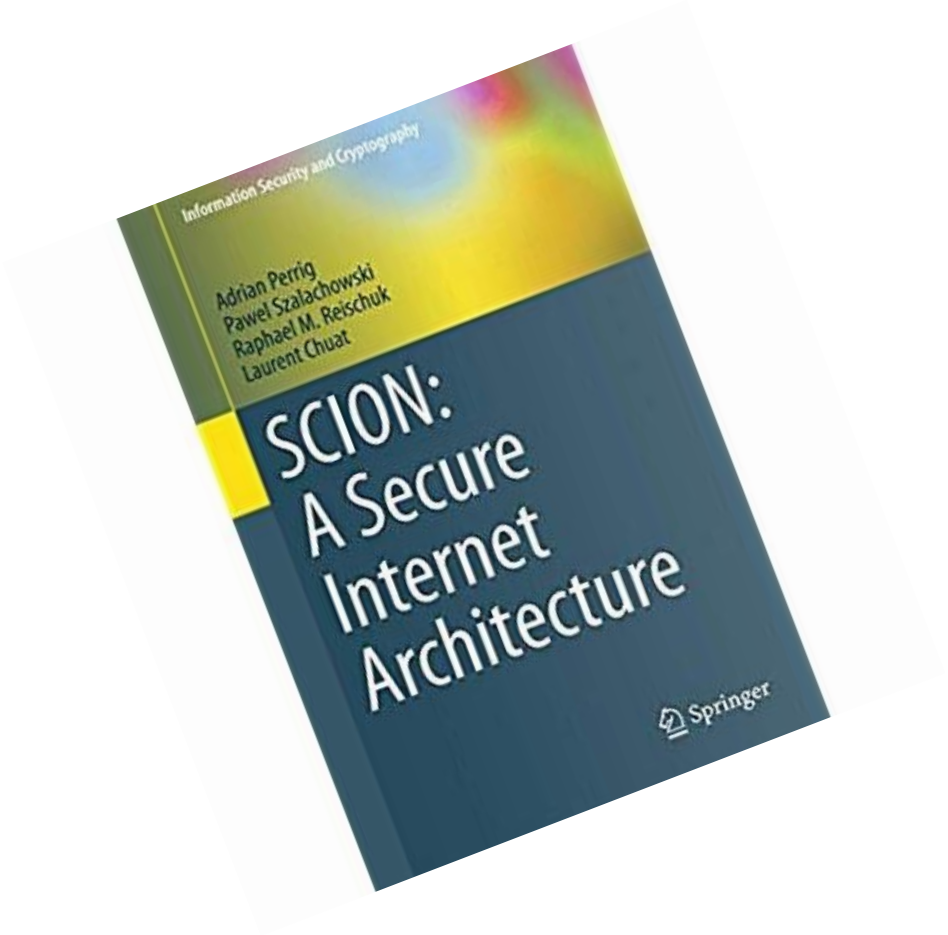


Zusammenfassung

SCION ist eine sichere Internetarchitektur die bereits heute eingesetzt werden kann.

- Es ist möglich (aber schwierig) den Internet-Layer zu verändern
  - Durch die Verwendung der existierenden intra-AS Infrastruktur und Protokolle ist ein Deployment von SCION verhältnismässig einfach
  - SCION kann sukzessive wachsen und benötigt keine globale Koordination
  - Bereits heute gibt es ein interkontinentales SCION-Netzwerke für den komerziellen Einsatz und für Forschungszwecke
- Eine sichere Kontrollebene verhindert Routing-Hijacks
- Pfadkontrolle und Transparenz für Hosts, Multipath-Kommunikation
- Open-source Implementierung

Ressourcen zu SCION.



- https://www.scion-architecture.net
  - Buch, Veröffentlichungen, Videos, Tutorials
- https://www.scionlab.org
  - SCIONLab testbed
- https://www.anapaya.net
  - ETH-Spin-off mit SCION-basierten Produkten
- https://github.com/scionproto/scion
  - Open-source code

ETH zürich

Dr. Markus Legner
Postdoktorand und Dozent
markus.legner@inf.ethz.ch

ETH Zürich
Institut für Informationssicherheit
CAB F 85.2
Universitätsstrasse 6
8092 Zürich

https://netsec.ethz.ch