Experiencing a Next-Generation Internet Architecture

Adrian Perrig, Network Security Group, ETH Zurich
Incredible Story

- BGP was designed in 1989 by Kirk Lougheed and Yakov Rekhter on three paper napkins over lunch, and today the Internet relies on it!
Journey Towards a Next-Generation Internet

- During our journey, we have encountered many interesting discoveries
- Several discoveries suggest new approaches for inter-domain networking

*The real voyage of discovery consists not in seeking new landscapes, but in having new eyes. Marcel Proust*
New Internet Architecture: Goals and Desires

- Internet to support applications?
  - Cloud computing
  - Mobility
  - Video streaming
  - IoT

- Internet to provide properties?
  - Security
  - Low latency
  - Privacy, anonymity
  - High performance
  - High availability, rapid failover
Approach: Massive Multipath

- Provide inter-domain multipath routing system that establishes a large number of distinct paths
  - Paths can be selected based on application requirements: security, latency, privacy, performance, etc.
- Provide flexible routing fabric that enables creation and dissemination of additional paths
- Observation: massive multipath satisfies most goals
- Caution: scalability, security, and compatibility with business models need to be built-in from the beginning
Strawman Approach 1

- Approach: Full Internet topology dissemination and source routing

- Problems
  - Scalability of global topology dissemination
  - Not compatible with ISP business models
  - Privacy of AS topologies
  - AS routing policies need to be honored
Strawman Approach 2

- **Approach:** All traffic is sent to a hyperscaler cloud provider, which provides global connectivity

- **Problems**
  - Current Internet cannot provide good connectivity even to ubiquitous cloud provider
  - Misalignment of incentives: hyperscaler has no incentive to provide high-quality connectivity to competitors
  - Lack of innovation and competition: Internet needs healthy ecosystem of large and small connectivity providers to fuel innovation in a competitive environment
Inspirations for a New Beginning

- Many exciting next-generation Internet projects over the past 25 years
- General Future Internet Architectures (FIA)
  - **XIA**: enhance flexibility to accommodate future needs
  - MobilityFirst: empower rapid mobility
  - Nebula *(ICING, SERVAL)*: support cloud computing
  - NIMROD: improved scale and flexibility
  - NewArch *(FARA, NIRA, XCP)*
  - RINA: clean API abstractions simplify architecture
- Content-centric FIAs: NDN, CCNx, PSIRP, SAIL / NETINF
- Routing security: BGPSEC, **S-BGP**, soBGP, psBGP, SPV, PGBGP, H-NPBR
- Path control: MIRO, Deflection, Path splicing, Pathlet, I3
- Inter-domain routing proposals: ChoiceNet, HLP, HAIR, RBF, AIP, POMO, ANA, ...
- Intra-domain / datacenter protocols: SDN, HALO, ...
Suggested New Architecture

- Control plane
  - Scalable creation of path segments
  - Scalable on-demand dissemination of path segments
  - Flexible architecture enables creation of additional paths with unforeseen properties

- Data plane
  - Policy-compliant path segment combination
  - Packet-carried path information, cryptographically protected to ensure policy compliance
  - Per-flow stateless in router fast path to avoid signaling overhead

ETH Zürich
Scion
Architecture Design Details

- Scalability: two-level hierarchical routing, creating 2 kinds of path segments: global (think “highways”) and local (think “local roads”)

- Massively multipath: path segments can be combined in policy-compliant ways to offer very large number of path choices

- Data plane makes use of packet-carried forwarding state, without needing any inter-domain forwarding tables
Two-level hierarchy through Isolation Domain (ISD)

- **Isolation Domain (ISD):** grouping of Autonomous Systems (AS)
- **ISD core:** ASes that manage the ISD and provide global connectivity
- **Core AS:** AS that is part of ISD core
- **Two-level hierarchical routing:** inter-ISD and intra-ISD
SCION Routing and Forwarding Overview

Path-based Network Architecture

Control Plane - Routing
- Constructs and Disseminates Path Segments

Data Plane - Packet forwarding
- Combine Path Segments to Path
- Packets contain Path
- Routers forward packets based on Path
  - Simple routers, stateless operation

Packet P1
- F→C→A
- A→I→J→M
- M→P→S
- Payload

Packet P2
- F→D→B
- B→K→L
- L→O→S
- Payload
Scalability of SCION Intra-ISD Beaconing

![Graph showing relative cost of AS instances sorted by SCION cost](image-url)
Scalability of SCION Core Beaconing

**Graphs**

1. **SCION Core**
   - Relative cost (Normalized to BGP)
   - AS Instance (sorted by SCION cost)
   - Average

2. **SCION Core, BGPSec and BGP**
   - Relative cost (Normalized to BGP)
   - AS Instance (sorted by SCION cost)
   - Average

**Note:**
- SCION Core
- BGPSec
- BGP

**Institution:** ETH Zürich
Scalability Study Results

- On a per-path basis, SCION spends about 200 times less effort than BGP, and about 1000 times less effort than BGPsec
- Time-to-connectivity in SCION is over 3 orders of magnitude faster than BGP
  - The iterative convergence approach in BGP takes minutes to converge with fully updated forwarding tables (in case of small changes), but hours for larger outages
Importance of Path Awareness & Multipath

- Generally, two paths exist between Europe and Southeast Asia
  - High latency, high bandwidth: Western route through US, ~450ms RTT
  - Low latency, low bandwidth: Eastern route through Suez canal, ~250ms RTT
- BGP is a “money routing protocol”, traffic follows cheapest path, typically highest bandwidth path
- Depending on application, either path is preferred
- With SCION, both paths can be offered!
SCION is Massively Multipath

- SCION not only finds many disjoint path segments, but enables a massive number of multipath choices through segment combinations.
- In this example, S has 5 path segments to core ASes, D has 6 path segments, and 7 core path segments are provided.
- These path segments enable 54 different end-to-end paths!
Flexibility to Support Different Optimization Criteria

- Thanks to massive number of path choices, SCION will likely offer best path for different optimality requirements
  - Low latency, jitter
  - High bandwidth
  - Privacy, anonymity
  - Low CO2 footprint
- Application can make use of multiple paths simultaneously
- System can dynamically optimize paths for optimal performance
- New world, offering exciting opportunities!
SCION Multipath Demo by Tony John (OvGU)

- https://www.youtube.com/watch?v=q8ugQtj0THk
SCION Multipath Teleconferencing

- Jonas Gessner is implementing teleconferencing app on iOS leveraging SCION multipath.
SCION Extensions

- SCION Extensions
- RAINS
- DRKey
- Hidden paths
- Mondrian
- COLIBRI
- EPIC
- HORNET
- TARANET
- SBAS
- Time Sync
- F-PKI
- LightningFilter
- GMA
- SCION

ETH Zürich
Online Resources

- https://www.scion-architecture.net
  - Book, papers, videos, tutorials
- https://www.scionlab.org
  - SCIONLab testbed infrastructure
- https://www.anapaya.net
  - SCION commercialization
- https://github.com/scionproto/scion
  - Source code
Governance

- Non-technical management
- Drive foundation in the start phase
- Networking with stakeholders
- Fundraising
- User community management

Standardisation & Documentation

- Collaboration with Internet standards organisations
- Standardisation committee

Open-Source Development

- Development of the SCION reference open source implementation
- Engagement with dev community

Community Building

- Manage stakeholders (users, developers, hardware vendors, ISPs, IXPs)
- Accelerate adoption
- Presence at conferences and industry events
- Education and training

Certification

- Software & Hardware SCION certification
- Deployment & ISP testing
- Green routing certificates
- Engineer certification
How to Deploy SCION: ISP

- CORE Routers are set up at the borders of an ISP
  - to peer with other SCION-enabled networks
  - to collect customer accesses
- No change to the internal network infrastructure of an ISP needed!
How to Deploy SCION: End Domain

- SCION IP Gateway (SIG) enables seamless integration of SCION capabilities in end-domain networks
- No upgrades of end hosts or applications needed
SCIONLab: Global Research Testbed

- Global SCION research testbed: https://www.scionlab.org
- Led by David Hausheer’s team at University of Magdeburg
- Open to everyone: create and connect your own AS within minutes
- ISPs: Swisscom, SWITCH, KDDI, GEANT, DFN
- Deployed 35+ permanent ASes worldwide, 600+ user ASes
  - Contact us to become an infrastructure AS, we can provide HW
- Kwon et al., “SCIONLab: A Next-Generation Internet Testbed”, ICNP 2020
Exciting SCIONLab Research Opportunities

- Next-generation Internet architecture research
- Users obtain real ASes with all cryptographic credentials to participate in the control plane
- ASes can use their own computing resources and attach at several points in the SCIONLab network
- Path-aware networking testbed
- Hidden paths for secure IoT operation
- Control-plane PKI in place, each AS has certificate
- Network availability and performance measurement (bandwidth and latency)
- Supported features (PKI, DDoS defense mechanisms, path selection support, end host / application support)
- Inter-domain routing scalability research
- Multipath research
- Multipath QUIC socket
- End-to-end PKI system that application developers can rely on to build highly secure TLS applications
- Colibri inter-domain resource allocation system
- DDoS defense research using in-network defense mechanisms
- Next-generation routing architecture policy definitions
SCION Production Network

- Led by Anapaya Systems
- **BGP-free global communication**
  - Fault independent from BGP protocol
- Deployment with international ISPs
  - Goal: First **global public secure** communication network
- Construction of SCION network backbone at select locations to bootstrap adoption
- Current deployment
  - ISPs: Swisscom, Sunrise, SWITCH, Axpo, Init7, Proximus, LG, …
  - IXPs: SwissIX offers SCION peering, + others joining soon
  - Bank deployment: Largest Swiss banks use SCION in production
Global Availability of Native SCION Connectivity

- Native SCION (BGP-free) connectivity: no reliance / dependency on BGP communication
- SCION deploying ISP’s networks are reaching global data centers and IXPs, offering native SCION connectivity
- Anapaya Connect: native SCION connectivity to 100+ data centers in 10+ countries
Endhost Deployment Opportunity

- Server can announce SCION capability through DNS txt record
- SCION parameters can be auto configured on endhost
  - SCION client bootstrapping package by François Wirz
- Extend Happy Eyeballs (RFC 8305) with SCION as third option besides IPv4 and IPv6
  - Asynchroneous DNS queries and connection attempts
- Incentive for server and client: SCION offers lower latency connection and possibly higher bandwidth through multipath
SCION and the Secure Swiss Financial Network (SSFN)

“The financial sector has faced many challenges in terms of distribution, flexibility and security when using the Internet for daily business activities. It is vulnerable to cyberattacks, including distributed DDoS or traffic-hijacking attacks.”

“This alternative would provide better control over the exchange of sensitive financial information among market participants while reducing implementation complexity and effort.”

“Extensive testing under extreme conditions has proven the reliability and resilience of the infrastructure—made possible by the path control and inherent multipathing properties of a SCION-based network architecture. This level of reliability and resilience is a vast improvement to ensure business continuity for current and future system-relevant use cases and applications not only in the financial sector but also for other critical infrastructures.”

Fritz Steinmann Director, Senior Network Security Architect
SCION and EDA

- 1st PoC in 2018 connecting Bern to the Berlin embassy with Deutsche Telekom and Swisscom

- 2nd PoC connecting Bern to Seoul, Korea (via HK) along with Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). In partnership with LG U+ / IoT Cube

- Test started for DDPS and FDFA in March 2021

Start of set-up: March 2021
DDPS Implementation: Target: June 2021
FDFA Implementation: Target: May 2021
SCION and ETH

- SCION for the ETH Domain (SCI-ED) is a research network connecting the institutes of the ETH Domain, e.g.:
  - ETH Zürich
  - EPF Lausanne
  - The Paul-Scherrer Institute
  - The National Centre for Super-Computing (CSCS)
- The first real-world setting that provided a rich environment for use-case evaluation and secure data transfers
- The SCI-ED project was instrumental in the advancement of the SCION infrastructure and paved the way for SSFN
Insight: Incremental Deployment Possible

- Incremental deployment of a new Internet architecture is possible, operating side-by-side with BGP.
- For ISPs, new architecture can be deployed with minimal effort.
- For end domains, SCION-IP Gateway (SIG) offers immediate benefits without updating any end hosts.
- Important: no reliance on BGP for inter-domain operation ("BGP-free").
  - Overlay / insecure underlay should be avoided not to inherit vulnerabilities.
- Re-use of intra-domain network architecture for local communication.
Insight: Secure Routing Insufficient

- Secure routing protocol cannot prevent outages caused by bottleneck link or continuing announcement of failed or congested routes, as announcement is often legitimate.
Insight: Multipath is a Necessity for High Availability and Performance

- Inter-domain multipath is not a luxury, but a necessity to achieve high availability
- Rapid failover without routing system convergence
  - Routing bottlenecks can be circumvented
- Enable higher network capacity
  - No more passive links for redundancy, all links can be active
  - Simultaneous use of several links
- Enables higher communication efficiency
  - Latency- vs. bandwidth optimal paths can be chosen
- Helps defend against DoS attacks, as adversary needs to congest all links
- QoS needs multipath, as several alternatives need to be available to attempt resource reservations
Insight: Cryptographic Processing at Line Rate Possible

- Symmetric-key cryptographic operations are possible within nanoseconds, thus enabling line-rate processing
- With hardware implementation, computing an AES block cipher can be accomplished within a few nanoseconds
- DRKey + EPIC systems enable per-packet source authentication in software ~ 100 ns
- This enables new approaches for network security
Insight: Formal Security Verification Necessary

- To achieve strong assurance for a large-scale distributed system, formal security verification is necessary.
- Performing formal verification from the beginning avoids “difficult-to-verify” components.
- Many design aspects of SCION facilitate formal verification.
- Collaboration with David Basin’s and Peter Müller’s teams in the VerifiedSCION project.
SCION Summary

- SCION: Next-generation Internet you can use today!
- High-performance
  - Path-aware network enables application-specific optimizations to provide enhanced efficiency
  - Multipath communication enables simultaneous use of multiple paths, increasing available bandwidth
- Secure, high assurance, high availability
  - Per-packet authentication verification possible on routers
  - Formal verification of protocols and code
  - Immune against routing attacks, e.g., BGP prefix hijacking
Expeditions Enable New Insights & Discoveries

- What started with the question “How secure can a global Internet be” has rewarded us with an exciting journey with many discoveries
- We hope to question engrained assumptions to counter Internet ossification
- Join the journey
  - https://www.scionlab.org
  - https://www.scion-architecture.net
SCION Team