Towards Deployment of
a Next-generation Secure
Internet Architecture

Wie können wir die Kommunikation
von Kritischen Infrastrukturen Sichern?

Adrian Perrig
Network Security Group

ETH Zürich

SATW Fachveranstaltung Cyber Security
21 April 2016

What's Wrong with the Internet?

(why do we need a next-gen Internet architecture?)

What's Wrong with the Internet?*

- **Scalability** - routing tables are getting too large
- **Availability** - misconfigurations, prefix hijacks, or slow routing protocol convergence leads to unreachability
- **Security** - data protection, mass surveillance, denial of service, no authentication of control plane
- **Authentication** - attacks on TLS PKI
- **Control** - cannot specify communication paths
- **Transparency** - cannot ensure which network path was used

*Not a comprehensive list, not even the tip of the iceberg

Band-aid Solutions

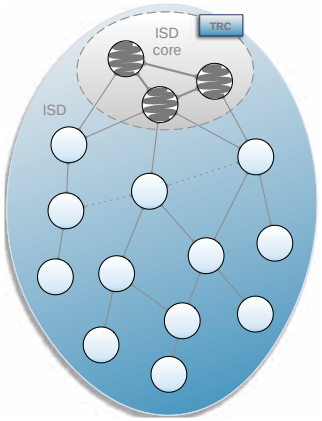
- **Scalability** - prefix aggregation + more memory
- **Availability** - multihoming + failover
- **Security** - encryption, traffic scrubbing
- **Authentication** - TLS, DNSSEC, BGPSEC
- **Control** - multihoming
- **Transparency** - ?

SCION Architectural Design Goals

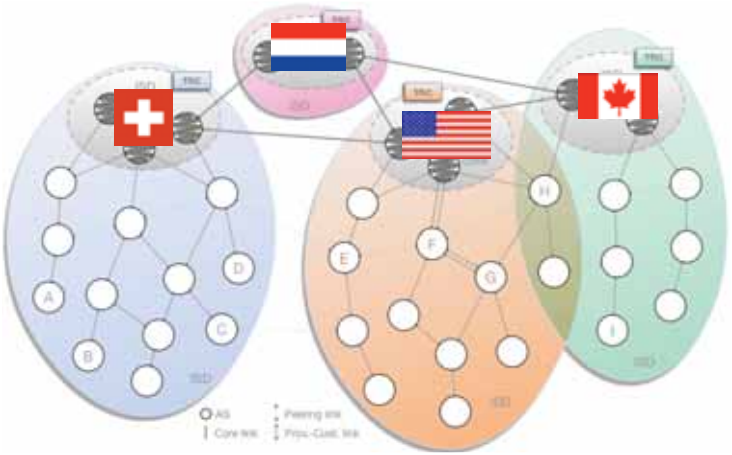
- **High availability**, even in the presence of adversaries
- **Secure entity authentication** that scales to global heterogeneous (dis)trusted environment
- **Flexible trust**: heterogeneous trust environment
- **Transparent operation**: Clear *what* is happening to packets and *whom* needs to be relied upon for operation
- **Balanced control** among ISPs, senders, and receiver
- **Scalability, efficiency, flexibility**

SCION Isolation Domains (ISD)

- Isolation domains are groups of Internet Service Providers (ISPs) that agree to operate under a uniform legal framework and policy
- ISD routing can only be modified by entities inside the ISD
- ISD core manages the domain
- Trust Root Certificate (TRC) specifies the policy

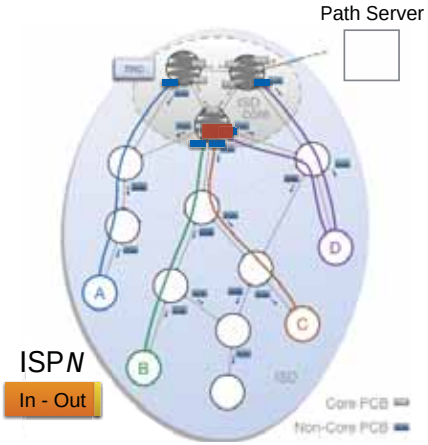


SCION Isolation Domains (ISD)



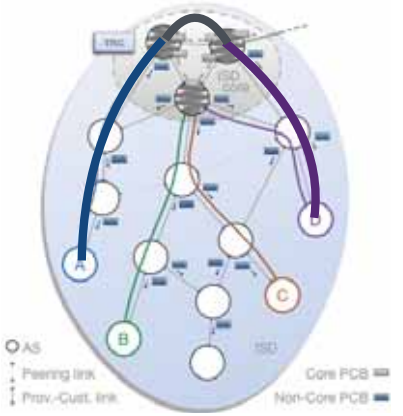
Route Discovery

- Path Construction Beacon (PCBs)
  - Periodic dissemination of path/topological information from the core to leaf ISPs
- Each ISP appends its hop routing information
- Paths to the core are registered at DNS-like “Path Servers”



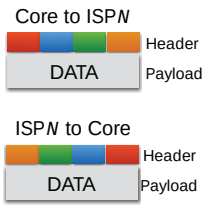
End to End Communication

- Source picks a path to the core (up path)
- Source asks for a path from the core to the destination (down path)
- Source joins those paths to construct an end to end path.

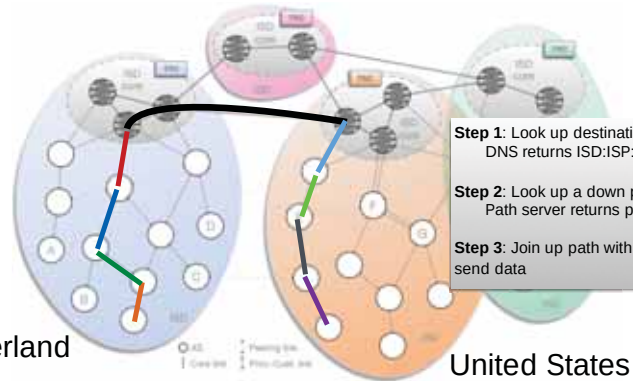


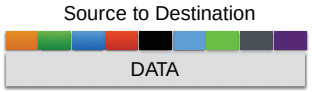
Data Transmission

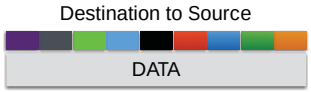
- Stateless: packets carry forwarding information in their headers (PCFS).
- No routing tables or lookups



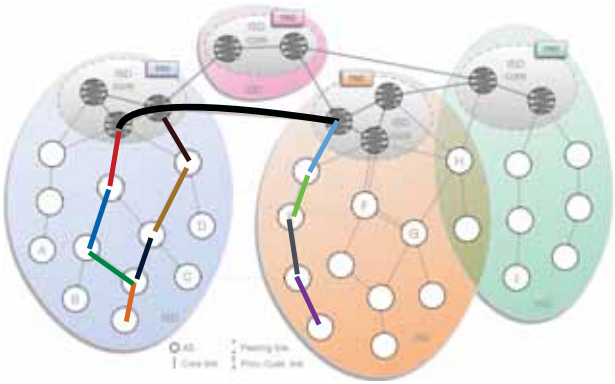
Data Transmission

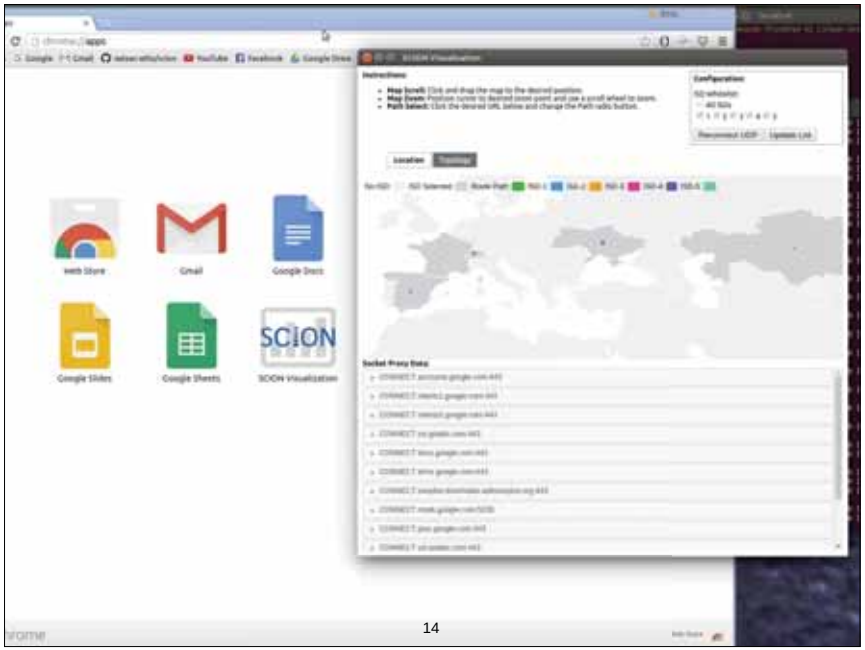






Data Transmission





SCION Extensions

Summary

- SCION is a new inter-domain routing architecture to replace and free us of all the problems with BGP
- SCION provides network foundation for: high availability, DDoS defenses, high-speed anonymous communication, pervasive end-to-end encryption, fault localization, and more!
- Status: SCION routers currently deployed at Swisscom, SWITCH, KDDI, ETH Zurich, CMU, Korea University, etc. Testbed constantly growing
- Try it out: https://SCIONproto.net
- Get more information: https://scion-architecture.net