Protecting Internet Communications with a Secure Backbone

Prateek Mittal
Princeton University
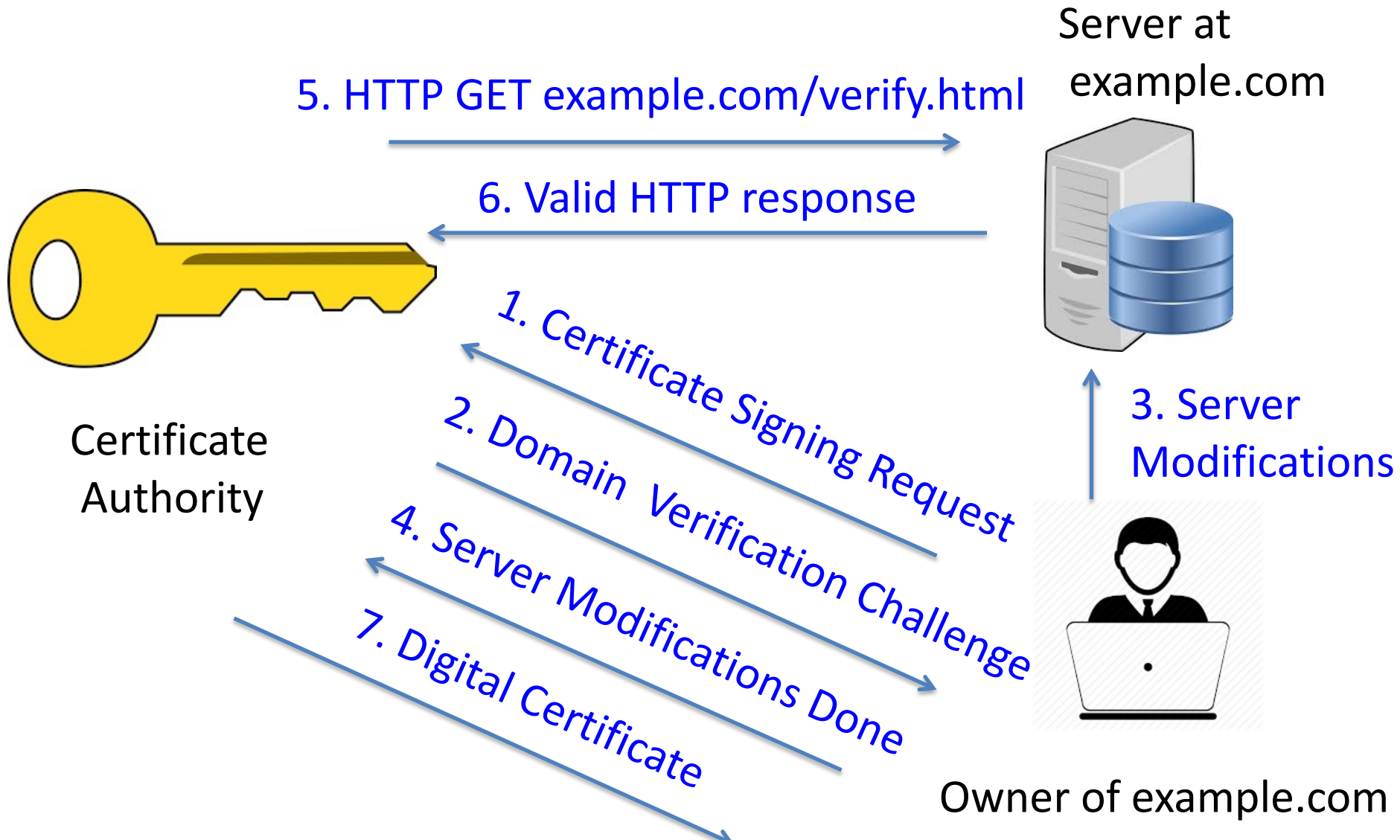
Joint work with Henry Birge-Lee, Joel Wanner, Grace Cimaszewski, Wirz Francois, David Hausheer, Jonghoon Kwon, Liang Wang, Adrian Perrig, Yixin Sun

PRINCETON UNIVERSITY

UNIVERSITY of VIRGINIA

ETH zürich

Status Quo: Insecurity in Internet Routing

1. Border Gateway Protocol (BGP) is vulnerable to routing attacks.

2. Routing attacks can have critical consequences for Internet applications (e.g.,HTTPS/domain validation, Tor, Bitcoin)

Motivating example: Domain Validation Protocol for TLS Certificates

Server at example.com

5. HTTP GET example.com/verify.html

6. Valid HTTP response

Certificate Authority

1. Certificate Signing Request

2. Domain Verification Challenge

3. Server Modifications

4. Server Modifications Done

7. Digital Certificate

Owner of example.com

Routing Attacks can Compromise Domain Validation (USENIX 2018)

Server at example.com

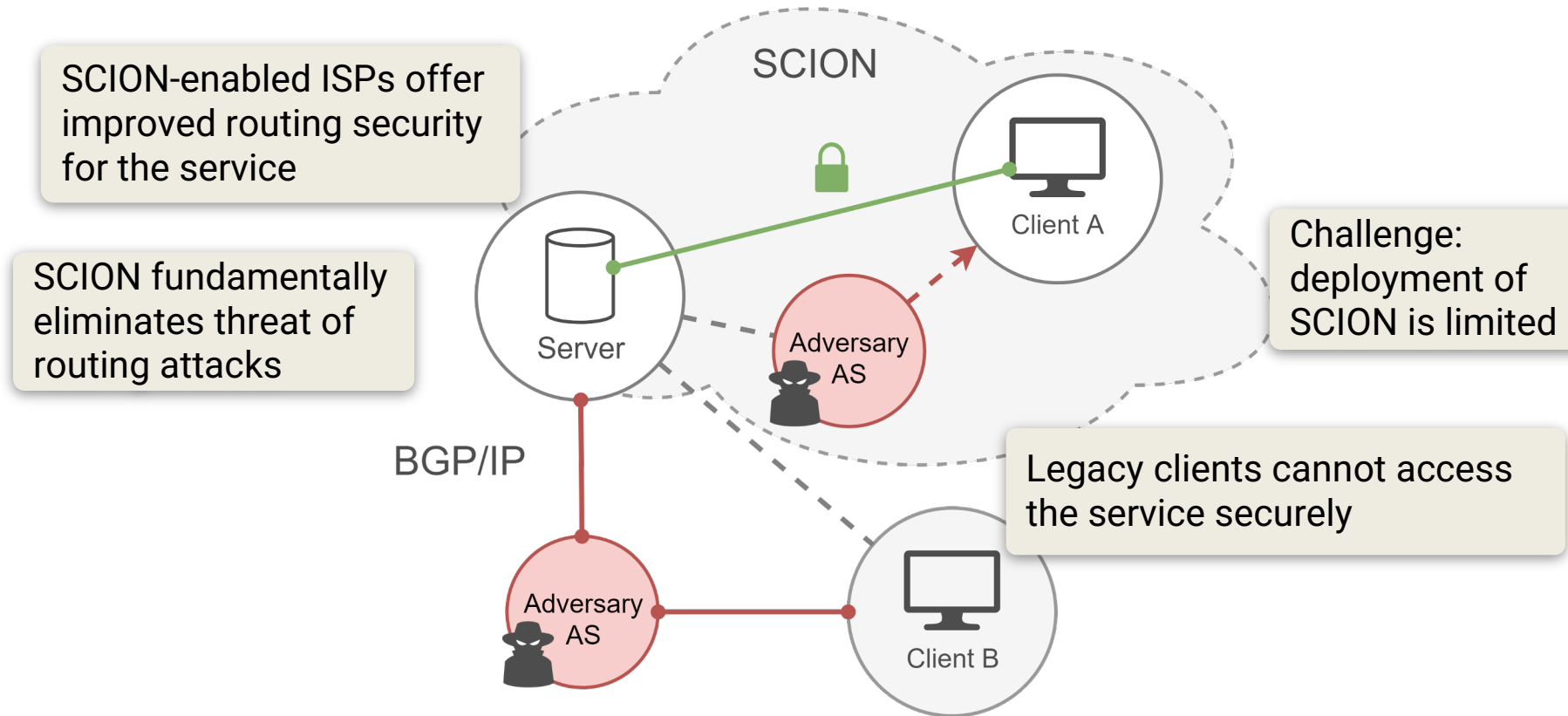5. HTTP GET example.com/verify.html

6. HTTP response

Attacker can launch BGP Hijack attacks to intercept HTTP verification request and spoof HTTP response

Authority

4. Server

Attacker can thus obtain digital certificates → The very foundation for HTTPS is vulnerable

Attacker

Routing Security:
Secure Backbones to the Rescue

SCION-enabled ISPs offer improved routing security for the service

SCION fundamentally eliminates threat of routing attacks

SCION

Client A

Server

Adversary AS

BGP/IP

Challenge: deployment of SCION is limited

Legacy clients cannot access the service securely

Adversary AS

Client B

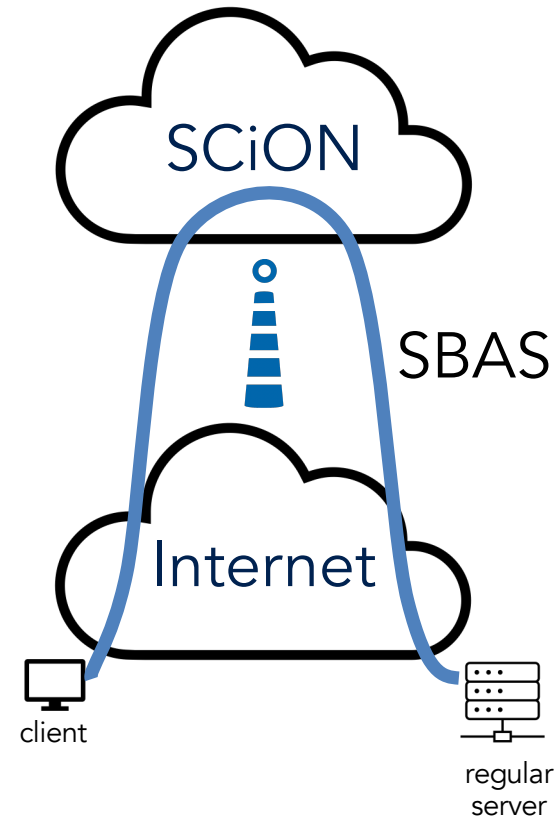Question: Can we extend the security benefits of even a limited SCION deployment to the broader Internet?

Introducing SBAS: SCION Backbone AS
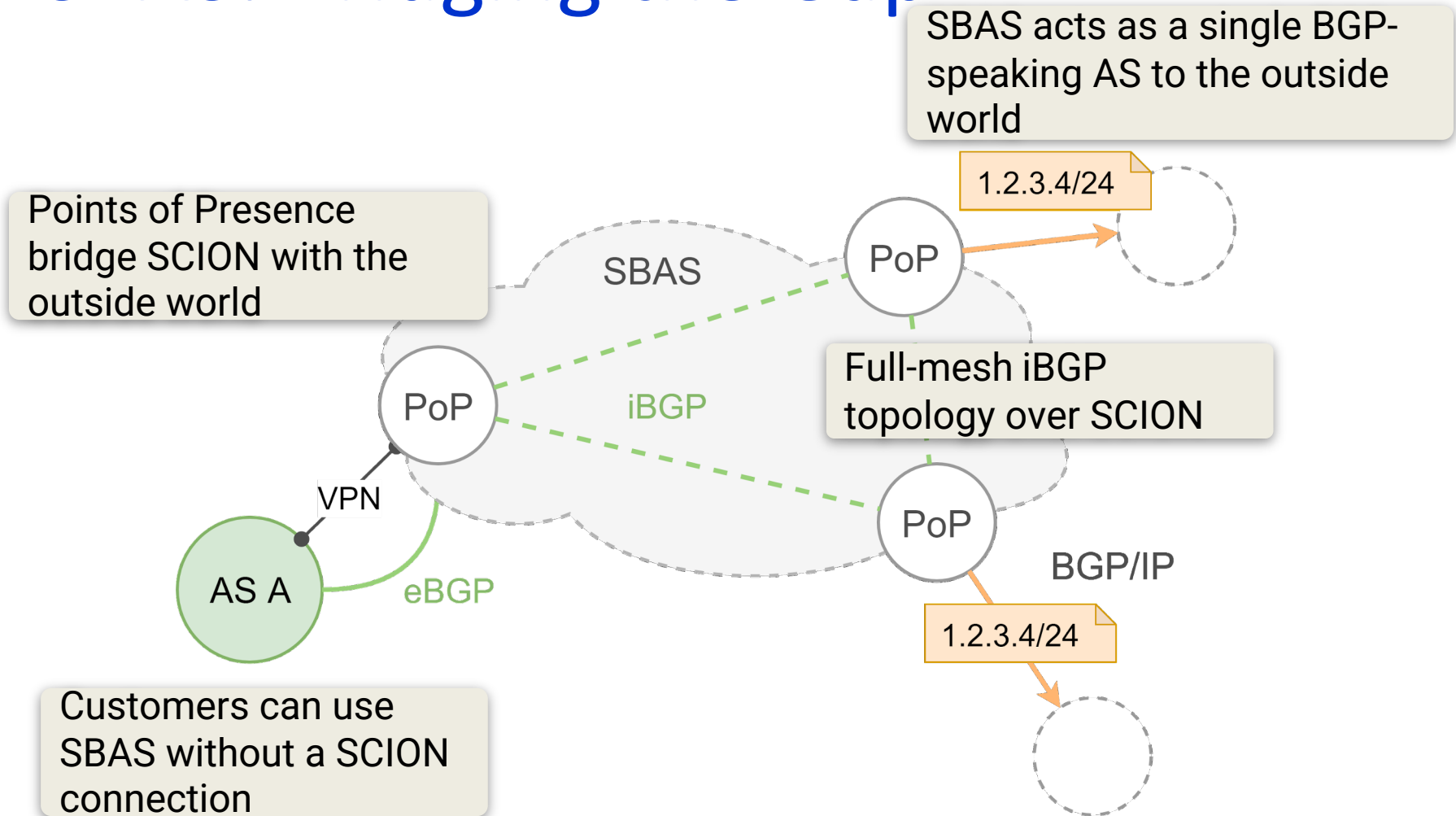
• Bridge the gap

SBAS optimizes **regular** Internet traffic, using the SCiON backbone

• Original motivation: Security
• Can also optimize latency, CO_2
• Transparent to Internet hosts
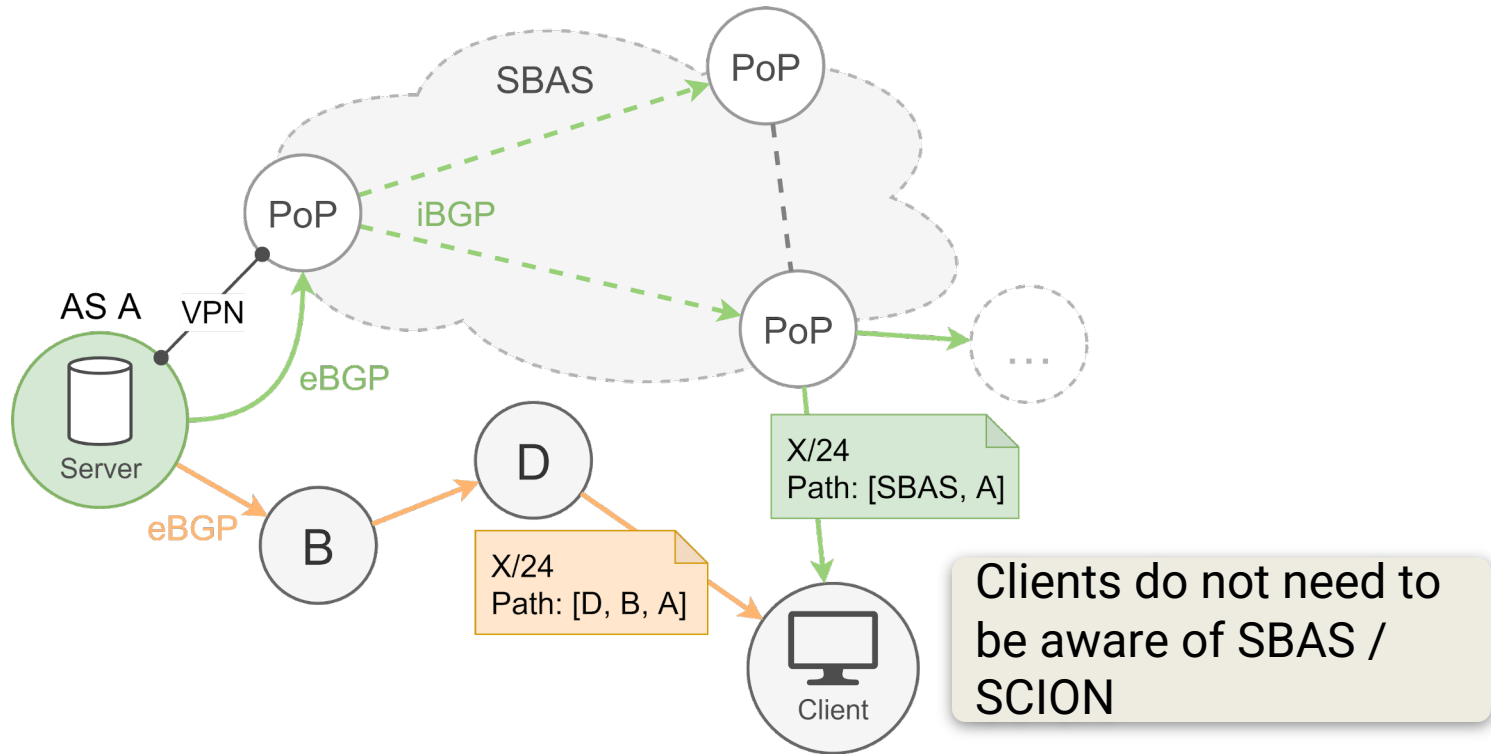• Promising system to get traffic onto the SCiON network

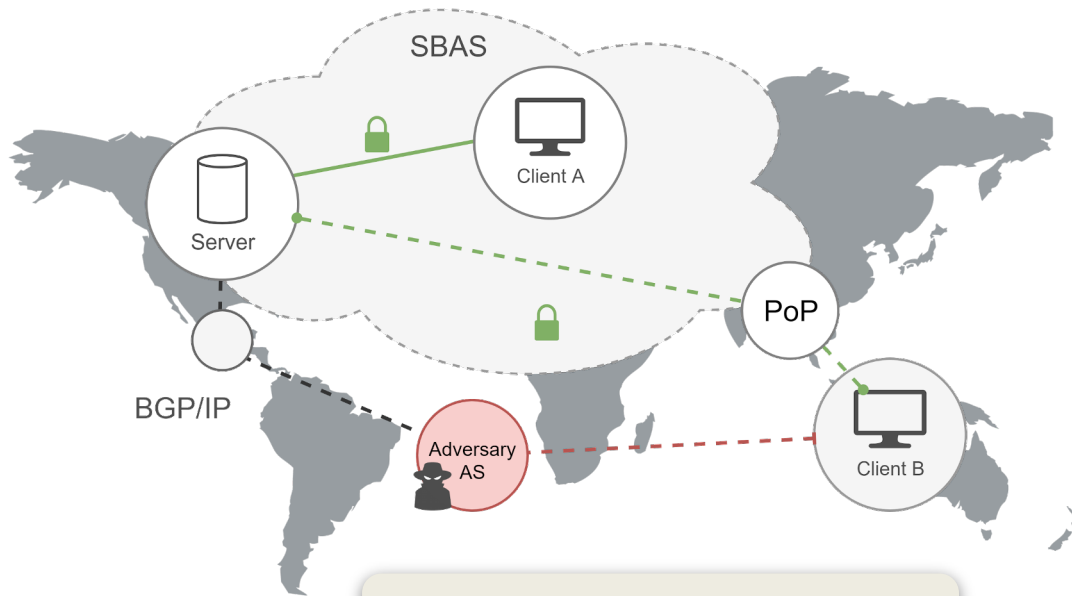**Key point: no upgrade to source or destination!**

SCiON

SBAS

Internet

client

regular server

SBAS: Bridging the Gap

SBAS acts as a single BGP-speaking AS to the outside world

1.2.3.4/24

Points of Presence bridge SCION with the outside world

SBAS

PoP

iBGP

PoP

Full-mesh iBGP topology over SCION

VPN

PoP

AS A

eBGP

BGP/IP

1.2.3.4/24
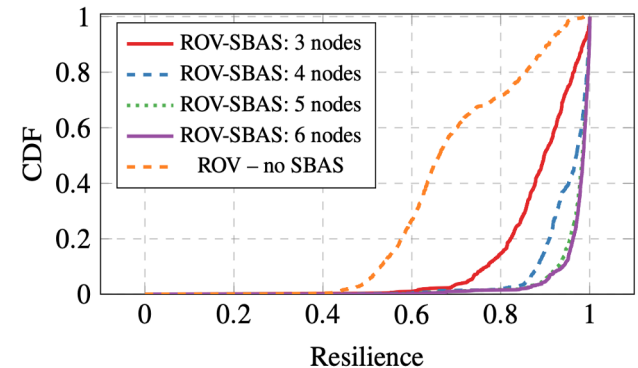
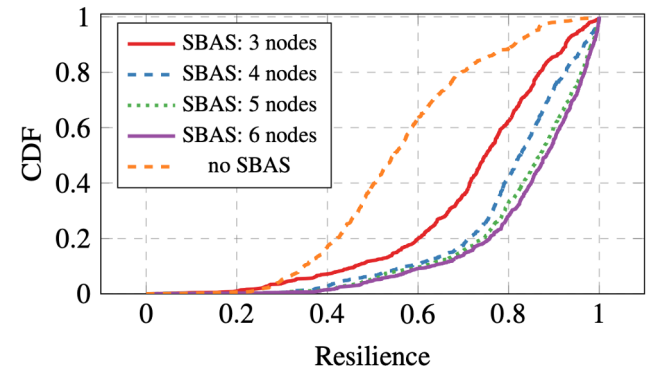Customers can use SBAS without a SCION connection

Security Benefits of SBAS

Security Benefits of SBAS

SBAS achieves improved hijack resilience for customer prefixes

SBAS: SCION Backbone AS

Governance Structure

SBAS PoPs collectively:

- Own an ASN
  → make announcements

- Manage customer relationships
  → re-announce prefixes

Federation of providers

MANRS

Multi-stakeholder organization

SCION FOUNDATION

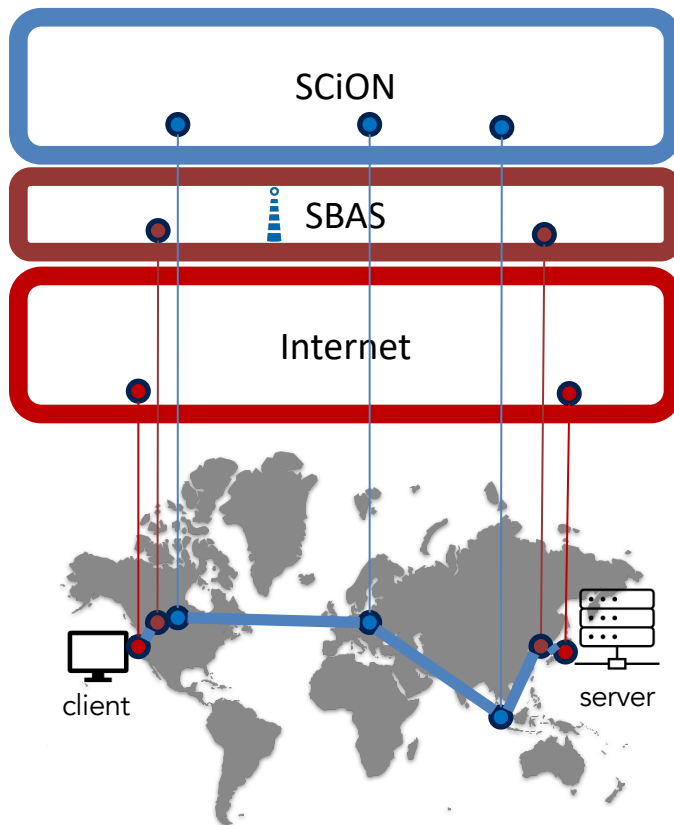Regional Internet Registries (**RIRs**)

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Decentralized model

Tor

SBAS: SCION Backbone AS

- Benefit: Bridge Legacy and SCION networks

Hijack-resilient enterprise network
For security-conscious enterprise customers

Green Internet
Improved carbon efficiency for private customers

Gaming Internet
A latency-optimized home connection for private customers