Creating a Secure Underlay for the Internet

Henry Birge-Lee
Princeton University

Joel Wanner, Grace Cimaszewski,
Wirz Francois, David Hausheer, Jonghoon Kwon, Liang Wang,
Prateek Mittal, Adrian Perrig, Yixin Sun

Status Quo: Weak Inter-domain Routing Security

1. The **Border Gateway Protocol (BGP)** is used by networks on the Internet (known as Autonomous Systems or ASes) to exchange routing information

2. BGP is vulnerable to routing attacks

3. Routing attacks can have critical consequences for Internet applications

BGP Attacks can have Severe Consequences

DISRUPTIONS ... view more

April 25, 2018

BGP Hijack of Amazon DNS to Steal Crypto Currency

Doug Madory
DIRECTOR OF INTERNET ANALYSIS

Public DNS in Taiwan the latest victim to BGP hijack

May 15, 2019 by Aftab Siddiqui Leave a Comment

Catalin Cimpanu

February 14, 2022

Cybercrime | News | Technology

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.

Apple network traffic went through Russia for 12 hours

Vilius Petkauskas , Journalist | Updated on: 28 July 2022

Routing Security with Secure Backbones

- Secure backbones like SCION and BGPsec fundamentally eliminate the threat of routing attacks
- SCION is offered today as a commercial service
- **BUT…** Secure backbones still have limited deployment
  - BGPsec is not deployed
  - SCION is only offered by some ISPs
- **AND…** Legacy clients without access get no benefits

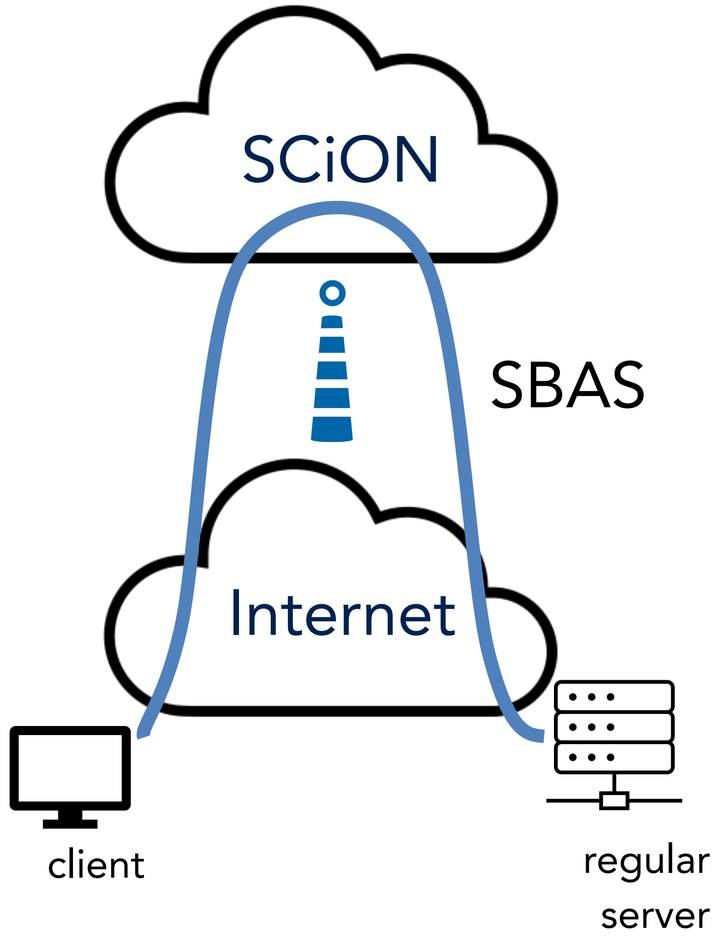
Question: Can we extend the security benefits of even a limited secure backbone deployment to the broader Internet?

Introducing SBAS: Secure Backbone AS

SBAS optimizes **regular** Internet traffic, using the a secure backbone

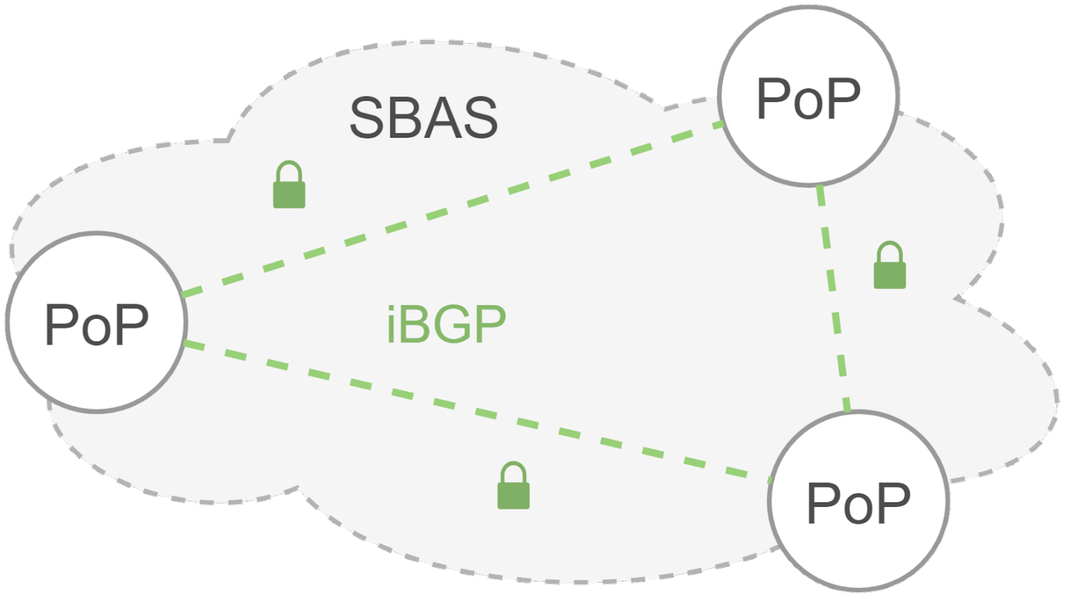
- Current deployment based on SCION
- Offers improved routing security
- Transparent to Internet hosts
- Promising system to get traffic onto a secure backbone

Key point: no upgrade to source or destination!



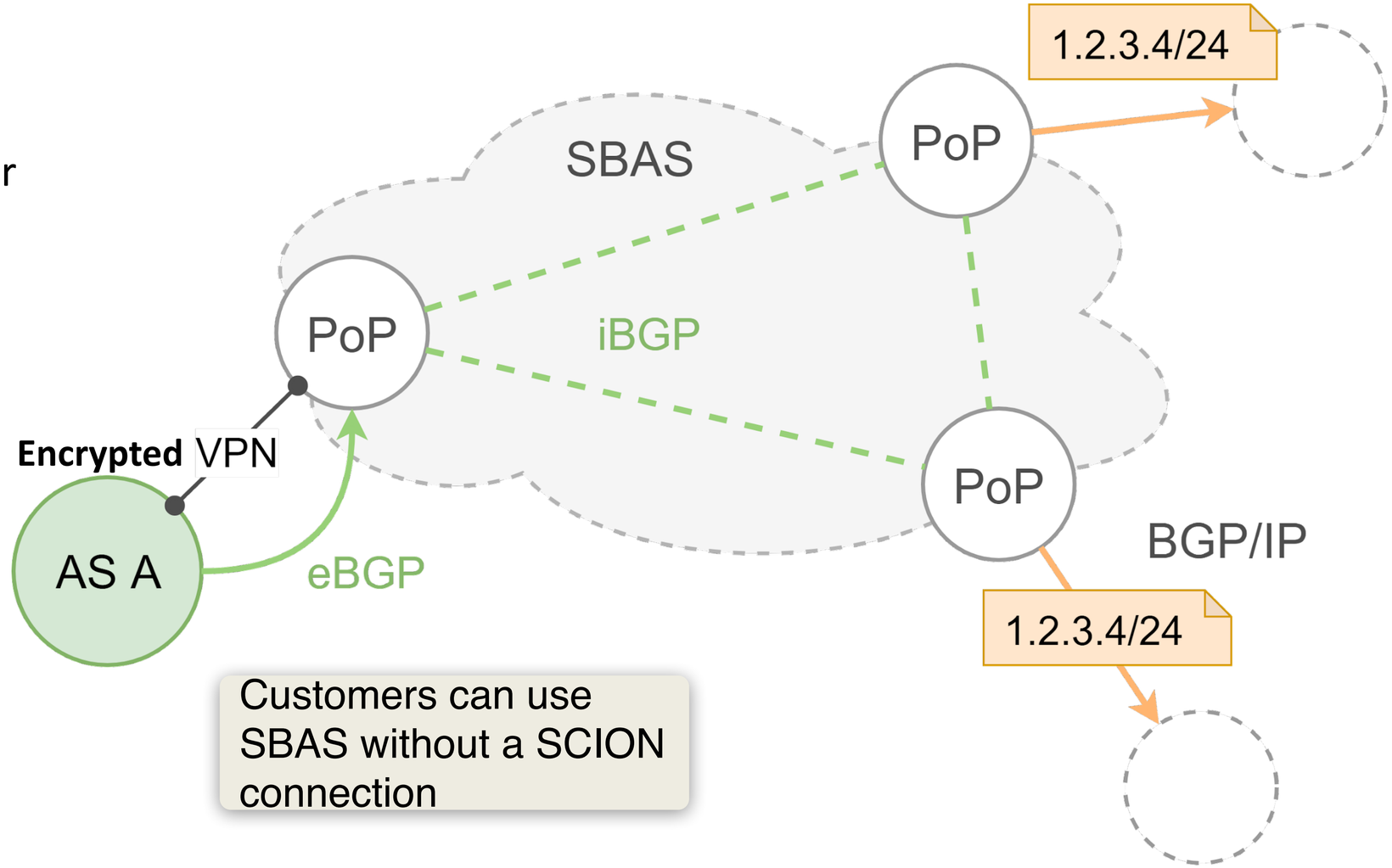
Inside SBAS

- Select ASes in the secure backbone run SBAS PoPs
- Points of Presence bridge the secure backbone with the outside world
- Traffic between SBAS PoPs is routed over the secure backbone
- SBAS PoPs use a full iBGP mesh to exchange routing information

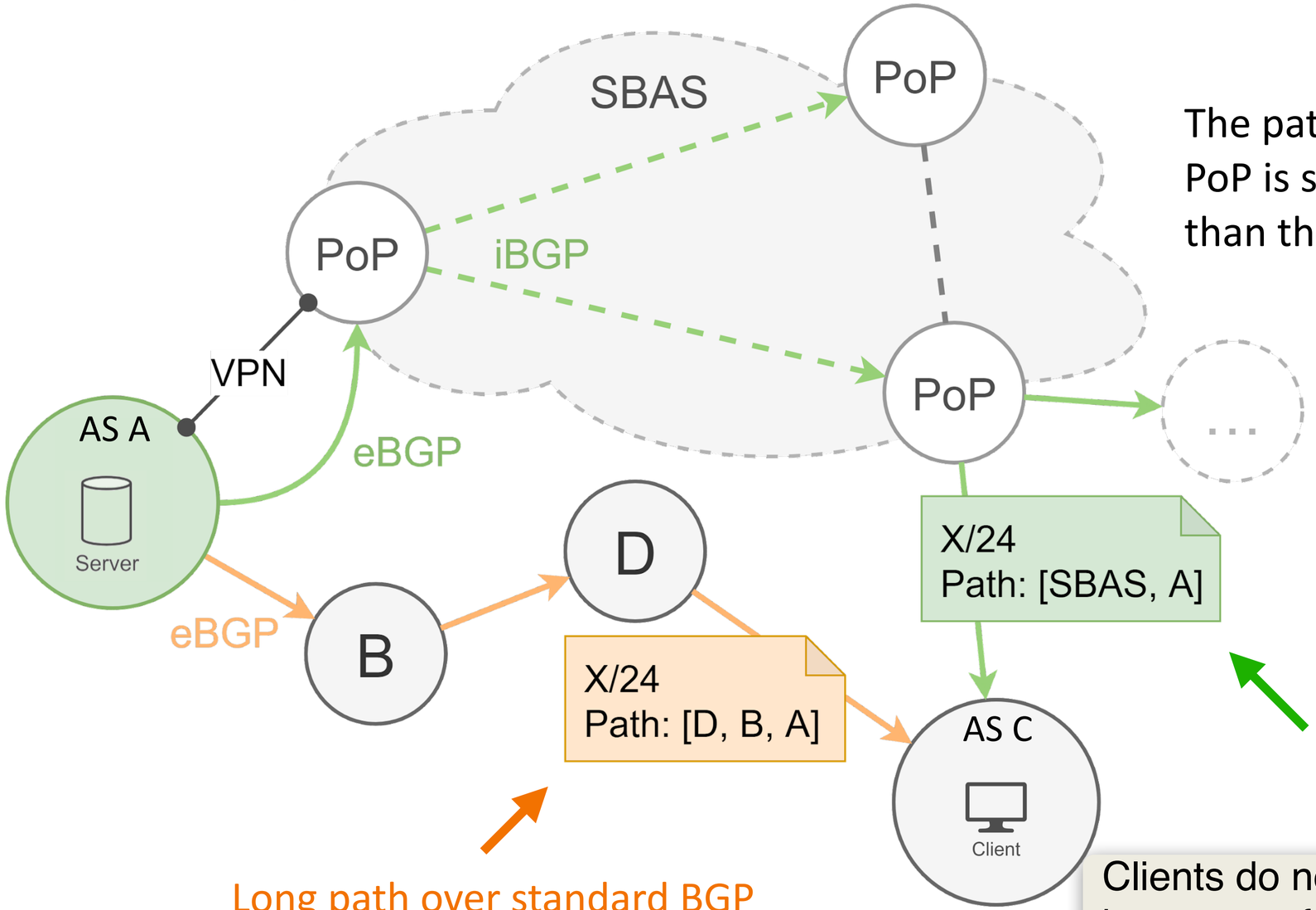


SBAS Connects to the Internet

- SBAS customers:
  - Connect to their nearest SBAS PoP over an encrypted VPN
  - Make BGP announcements for their IP prefixes to this PoP
- SBAS PoPs:
  - Redistribute customer BGP announcements to other PoPs
  - Announce SBAS customer prefixes to the Internet
- Non-participating clients:
  - Route traffic via standard BGP to their nearest SBAS PoP



Security Benefits of SBAS



The path from the client to the SBAS PoP is shorter and harder to hijack than the traditional Internet path

Clients do not need to be aware of SBAS / SCION

Measuring the Security of SBAS

1. Routes within SBAS are all one hop and validated with RPKI

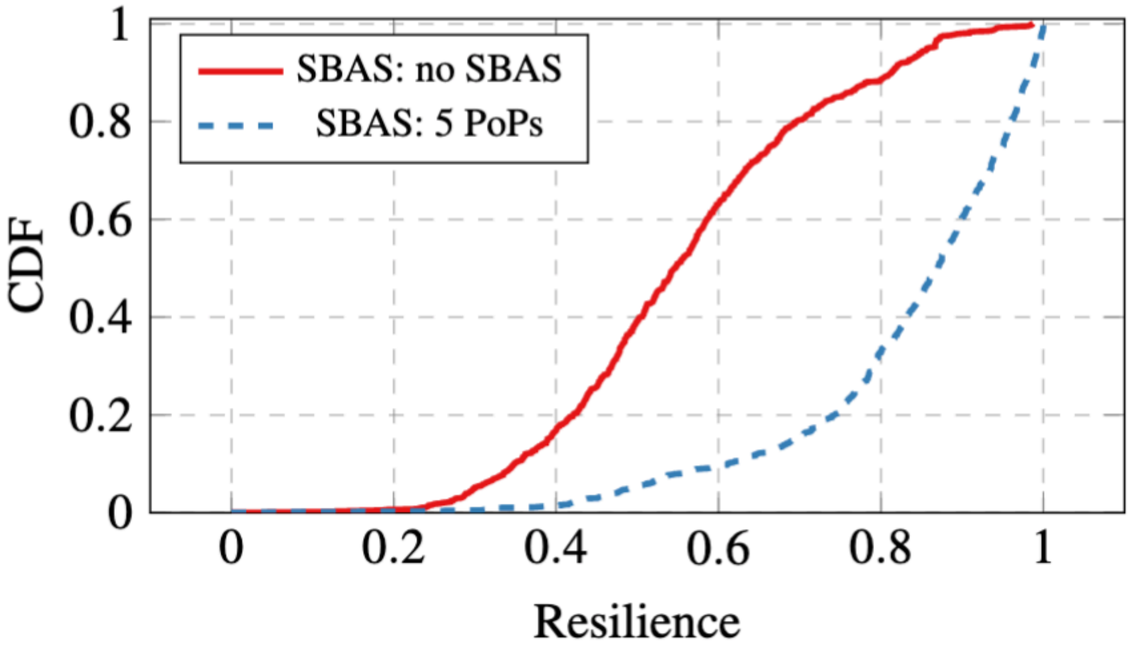
2. SBAS gives priority to validated SBAS customer routes
   - Communication between customers cannot be hijacked

3. We measured the resilience of SBAS prefixes to BGP hijacks
   - Focused on traffic from non-participating clients to SBAS-secured prefixes
   - Resilience measures the probably a random random client's traffic will be properly routed to the victim during a BGP hijack

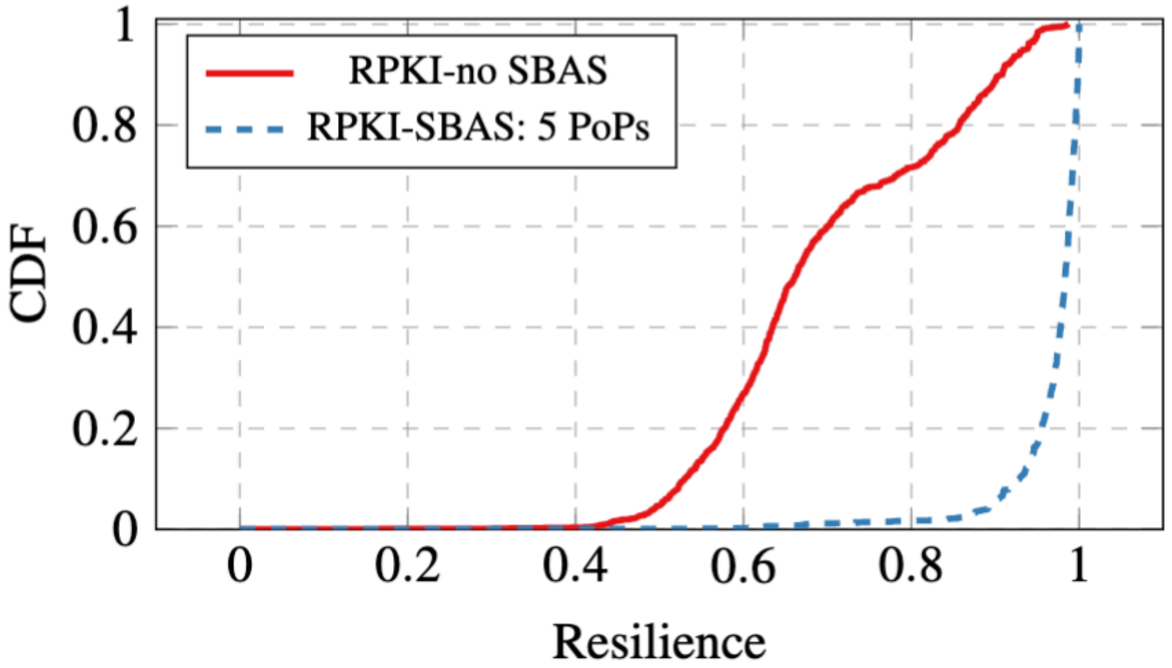
Security Benefits of SBAS

SBAS achieves improved BGP hijack resilience for customer prefixes

No RPKI Deployed



RPKI Deployed



We built this for real: Try It

https://sbas-demo.net/

NJ Traceroute

Traffic only goes over the public Internet to PoP in NJ and is then routed securely to Zurich

Thank you for your attention

Henry Birge-Lee

birgelee@princeton.edu

Open Source Codebase Available

https://github.com/scion-backbone/sbas