# BGP-iSec: Improved Security of Internet Routing against Post-ROV Attacks

**Cameron Morris**
cameron.morris@uconn.edu

Amir Herzberg
amir.herzberg@gmail.com

Bing Wang
bing@uconn.edu

Sam Secondo
samuel.secondo@uconn.edu

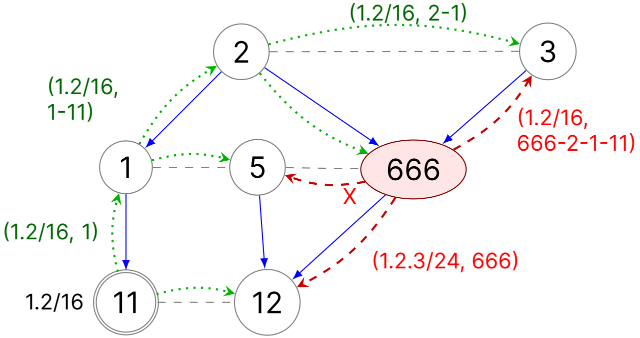
University of Connecticut

February 27, 2024

# Routing Attacks

BGP lacks authentication. BGP sessions are often authenticated against MitM (using TLS, IPSec,...) but BGP is still vulnerable to rogue AS attacks:

- Route Leak: to AS 3
- Prefix Hijack: X=(1.2/16, 666)
- Subprefix Hijack: to AS 12
- Origin Hijack: X=(1.2/16, 666-11)
- Path Manipulation: X=(1.2/16, 666-2-11)
- Attribute Manipulation: add blackhole attribute



# A Brief History of BGP Security (not to scale)

**1989**

*RFC 1105 A Border Gateway Protocol (BGP)*

*Security Problems in the TCP/IP Protocol Suite*

**1994**

*RFC 1654 A Border Gateway Protocol 4 (BGP-4)*

**1999**

Secure Border Gateway Protocol (S-BGP)

**2001**

*Stable Internet Routing without Global Coordination*

**2003**

*Origin Authentication in Interdomain Routing*

*Securing BGP through Secure Origin BGP (soBGP)*

**2004**

*Evaluation of Efficient Security for BGP Route Announcements using Parallel Simulation*

*SPV: Secure Path Vector Routing for Securing BGP*

*Listen and Whisper: Security Mechanisms for BGP*

**2005**

*Aggregated Path Authentication for Efficient BGP Security*

**2006**

*RFC 4272 BGP Security Vulnerabilities Analysis*

*PHAS: a Prefix Hijack Alert System*

**2007**

*On Interdomain Routing Security and Pretty Secure BGP (psBGP)*

**2008**

*Autonomous Security for Autonomous Systems*

**2009**

*Netreview: Detecting When Interdomain Routing Goes Wrong*

# A Brief History of BGP Security (not to scale)

## 2010

- *A Survey of BGP Security Issues and Solutions*
- *How Secure are Secure Interdomain Routing Protocols?*

## 2011

- *Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security*
- *Having your Cake and Eating it too: Routing Security with Privacy Protections*
- *Preventing Attacks on BGP Policies: One Bit is Enough*

## 2012

- *RFC 6480 An Infrastructure to Support Secure Internet Routing*
- *RFC 6481 A Profile for Resource Certificate Repository Structure*
- *Private and Verifiable Interdomain Routing Decisions*
- *A new approach to Interdomain Routing based on Secure Multi-party Computation*

## 2013

- *RFC 6811 BGP Prefix Origin Validation*
- *BGP Security in Partial Deployment: Is the Juice worth the Squeeze?*
- *On the Risk of Misbehaving RPKI Authorities*
- *A Survey of Interdomain Routing Policies*

## 2014

- *Why is it Taking so Long to Secure Internet Routing?*
- *RFC 7132 Threat Model for BGP Path Security*
- *PEERING: an AS for us*
- *A Survey of Interdomain Routing Policies*

## 2015

- *Secure Routing for Future Communication Networks*
- *Investigating Interdomain Routing Policies in the Wild*
- *Self-reliant Detection of Route Leaks in Inter-domain Routing*

# A Brief History of BGP Security (not to scale)

## 2016

- RFC 7908 Problem Definition and Classification of BGP Route Leaks
- *Jumpstarting BGP Security with Path-End Validation*
- *Rethinking Security for Internet Routing*
- *NTT Peer Locking*

## 2017

- RFC 8205 BGPsec Protocol Specification
- *Are We There Yet? On RPKI's Deployment and Security*
- *Design and Analysis of Optimization Algorithms to Minimize Cryptographic Processing in BGP Security Protocols*
- *The SCION Internet Architecture*

## 2018

- *RFC 8374 BGPsec Design Choices and Summary of Supporting Discussions*
- *Practical Experience: Methodologies for Measuring Route Origin Validation*
- *Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering*
- *University of Oregon Route Views Project*
- *The State of Affairs in BGP Security: A Survey of Attacks and Defenses*

## 2019

- *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*
- *RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins*
- *SICO: Surgical Interception Attacks by Manipulating BGP Communities*

## 2020

- *To Filter or Not to Filter: Measuring the Benefits of Registering in the RPKI Today*
- *Limiting the Power of RPKI Authorities*
- *DISCO: Sidestepping RPKI's Deployment Barriers*
- *On Measuring RPKI Relying Parties*
- *Peerlock: Flexsealing BGP*

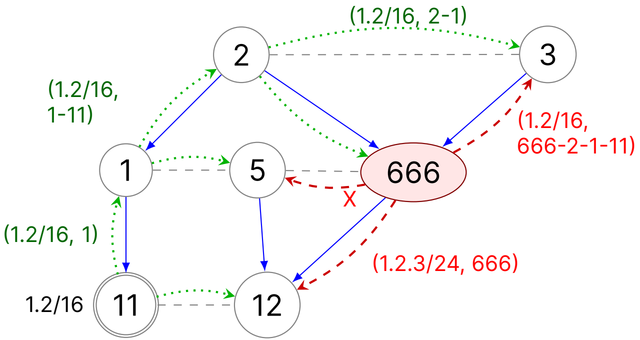
## 2021

- *Revisiting RPKI Route Origin Validation on the Data Plane*
- *ROV++: Improved Deployable Defense Against BGP Hijacking*
- *The Hijackers Guide to the Galaxy:Off-Path Taking Over Internet Resources*

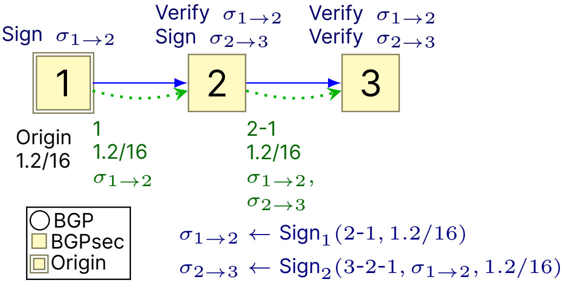
# Post-ROV Routing Attacks

BGP lacks authentication. BGP sessions are often authenticated against MitM (using TLS, IPSec,...) but BGP is still vulnerable to rogue AS attacks:

- Route Leak: to AS 3
- ~~Prefix Hijack: X=(1.2/16, 666)~~
- ~~Subprefix Hijack: to AS 12~~
- Origin Hijack: X=(1.2/16, 666-11)
- Path Manipulation: X=(1.2/16, 666-2-11)
- Attribute Manipulation: add blackhole attribute

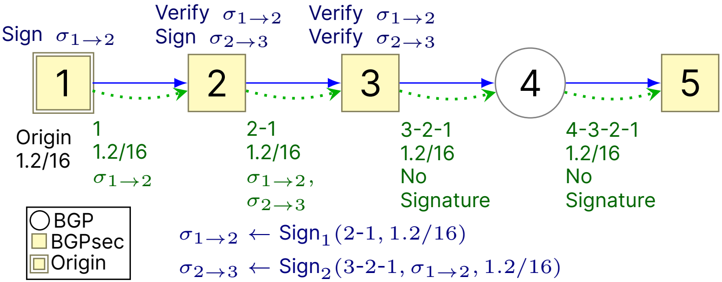


# BGPsec (RFC8205): IETF standard against path manipulations.



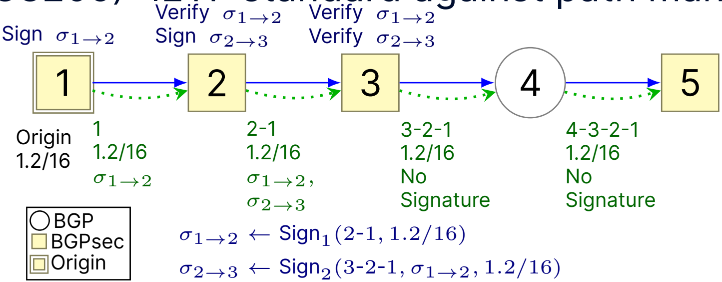

- BGPsec ASes downgrade to BGP for BGP neighbors
  - E.g, AS 5 will not receive signature, can't validate.

# BGPsec (RFC8205): IETF standard against path manipulations.



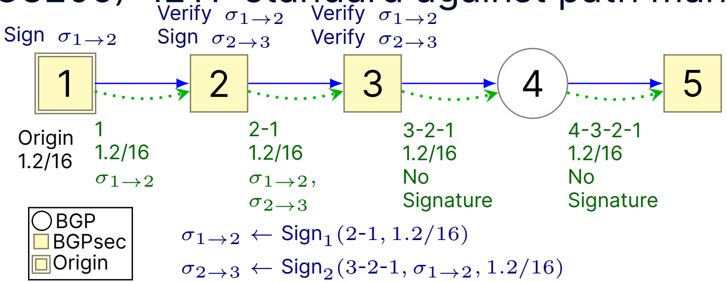

- BGPsec ASes downgrade to BGP for BGP neighbors
  - E.g, AS 5 will not receive signature, can't validate.
- $\Rightarrow$ Very limited benefits for partial deployment [LychevGS13]

# BGPsec (RFC8205): IETF standard against path manipulations.




- BGPsec ASes downgrade to BGP for BGP neighbors
- **Why BGPsec downgrades to BGP?**

# BGPsec (RFC8205): IETF standard against path manipulations.




- BGPsec ASes downgrade to BGP for BGP neighbors
- **Why BGPsec downgrades to BGP?**
- BGPsec ASes do not relay BGPsec info to BGP-only routers.
- Even if they did, a rogue AS could just drop the BGPsec info
  - BGPsec has no registry of adopting ASes
  - And adopting ASes may stop signing at any time

# Areas to Improve on BGPsec

1. Security benefits are limited to islands (only BGPsec ASes in path).
2. Downgrade to (non-authenticated) BGP is trivial for on-path attackers.
3. No defense against route leaks.
4. Only the AS Path is protected; other path attributes can be manipulated.

Signature operations in BGPsec are also computationally expensive, in this work we only focus on items 1-4.

# Contribution: BGP-iSec

**BGP-iSec** aims to improve on the security of BGPsec in partial adoption with few modifications to the existing design. The modifications:

- Identify adopters and their PK, prevent unauthorized downgrades to BGP.
- Enable partial path verification.
- Authenticate integrity-protected attributes.
- Prevent route leaks.

# Evaluating[1] the Components of BGP-iSec

[1]Simulations were performed using custom extensions to BGPy https://github.com/jfuruness/bgpy_pkg

# Evaluation: Attacker Strategies

- **Aggressive**: 1-hop origin hijack. Ex: AS Path = {666, 1}
- **Shortest-Path Export-All**: Attacker shortens the AS Path as much as possible while avoiding detection by any deployed path manipulation defenses. Ex: AS Path = {666, ..., 2, 1}

# Evaluation: Attacker Models

- **Global Attacker**: Receives all BGP announcements sent by every AS, but does not receive BGP-iSec attributes.

# Evaluation: Assumptions

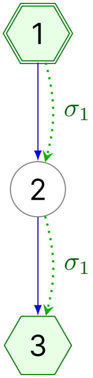
- Post-ROV: ROA for prefixes, ROV by all ASes
- Valley-free Routing (with export-to-all)
- Relationships (topology) from CAIDA [serial 2]
- Identified Adopters and Public Keys (e.g. in RPKI)

# BGP-iSec Components

- Path integrity defense: transitive signatures
- Three route-leak defenses

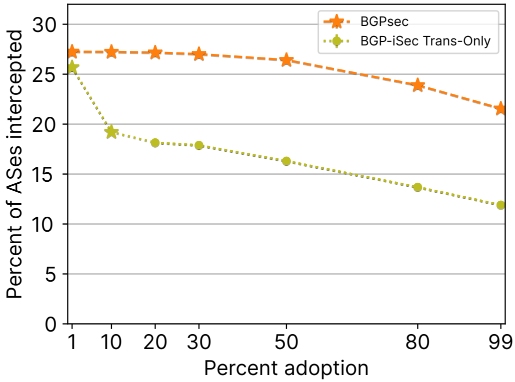
# Transitive Signatures (1/2)

- BGP-iSec sets the transitive bit to **true** and *sends signatures to non-adopting neighbors*.
- Transitive signatures allow BGP-iSec to *enforce downgrade prevention* and *authenticate adopting (sub)paths*.



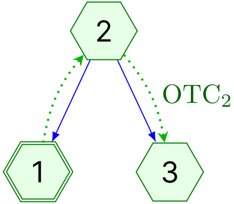
# Transitive Signatures (2/2)

- BGP-iSec prevents fake downgrades: signatures are relayed by all ASes; RPKI identifies adopters, keys
- Overhead - but high security impact!



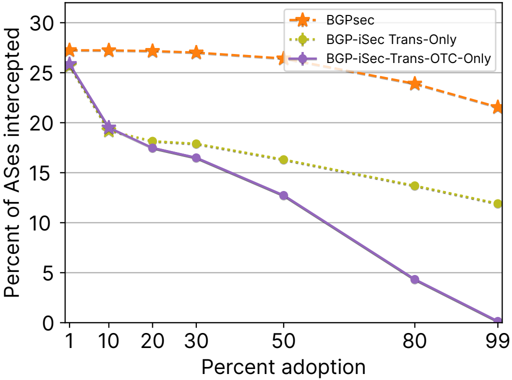
# Signed Only-To-Customer (OTC) (1/2)

- RFC-9234 defines the OTC attribute to indicate when routes should only be propagated downward (to customers).
- The OTC attribute is unauthenticated, so it only protects against accidental route leaks. A malicious attacker can simply remove the attribute.
- OTC prevents unintentional leaks; it is increasingly adopted.
- BGP-iSec authenticates the OTC attribute, preventing also malicious route leaks.



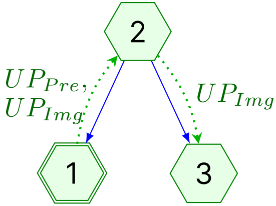
# Signed Only-To-Customer (OTC) (2/2)

- By simply authenticating OTC, a standardized route leak protection measure, the impact of post-ROV routing attacks significantly reduces.
- OTC attributes are already in use today.
- BGP-iSec has two other defenses which improve prevention of intentional leaks: the UP attributes and the ProConID mechanism



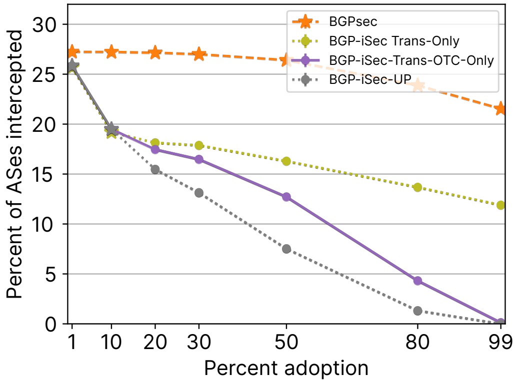
# BGP-iSec UP (Up Permitted) Attributes (1/2)

- The two *Up-Permitted* (UP) attributes, $UP_{Pre}$ and $UP_{Img}$, indicate whether an announcement can be sent to providers (upward).
- $UP_{Pre}$ contains a random string $x$; $UP_{Img}$ contains $h(x)$, where $h$ is a crypto-hash function
- The UP Preimage is removed when an announcement is sent to a customer or peer (downward).
- Since the hash function cannot be reversed, the preimage cannot be re-added.



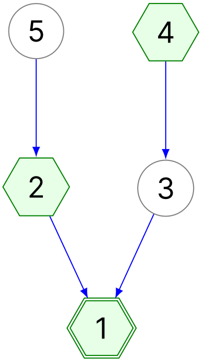
# BGP-iSec Up Permitted (UP) Attributes (2/2)

- Drawback: an eavesdropping adversary can capture the preimage.



# BGP-iSec ProConID (1/2)

- The *ProConID* mechanism protects against route leaks even when the attacker can eavesdrop on BGP session traffic.
- Similar to ASPA[a], an adopting AS publishes a list of the nearest BGP-iSec ASes to it in its provider cone.
- AS 2 and 4 are the only BGP-iSec ASes that will accept signed announcements from AS 1 from a customer interface because they are the ASes in AS 1's ProConID-list.

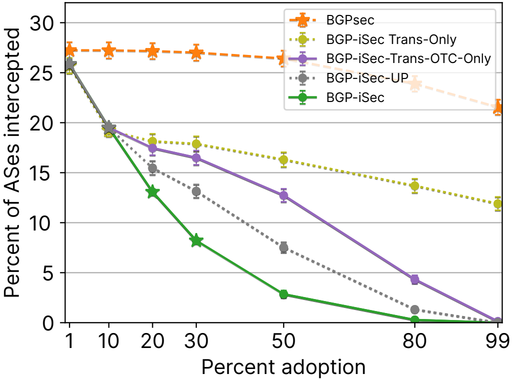



AS 1 ProConID-list: {2, 4}

[a] draft-ietf-sidrops-aspa-verification-16

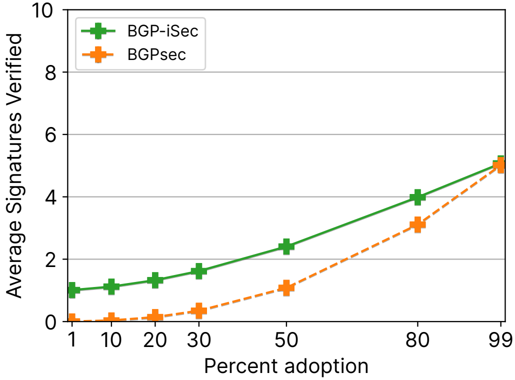
# BGP-iSec ProConID (2/2)

- ProConID provides even stronger protection against route leaks than UP attributes.
- Provider cones are small on average (median size is around 30).
- The overhead of updating and maintaining the ProConID-list is reasonably low. We analyze it in the paper but omit the results here.



# Overhead Comparison with BGPsec

- Both BGPsec and BGP-iSec require the same number of signature verification operations in full deployment.
- More signatures on average are verified in partial adoption because they transit over non-adopting ASes.



# Security Analysis

We also analytically show that under the assumptions of our evaluation, even with stronger attacker models, the following properties hold.

- No false positives
- Prevention of [visible] route leaks
- Announcement integrity under full deployment

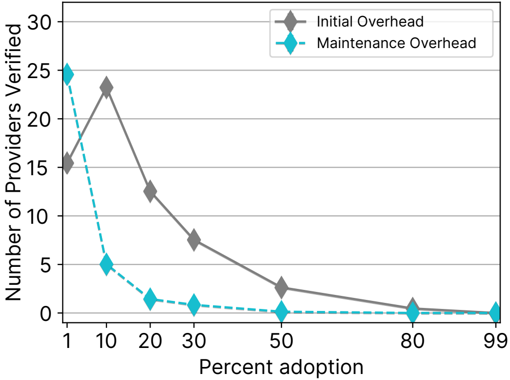
# Conclusions

- We present BGP-iSec, a set of modifications and extensions to BGPsec to provide:
  - Better security against ROV-valid path manipulations in partial deployment
  - Defense against route leaks
  - Defense against attribute manipulations
- BGP-iSec is not meant as a complete proposal, but as a basis to build upon for further designs.

# Backup

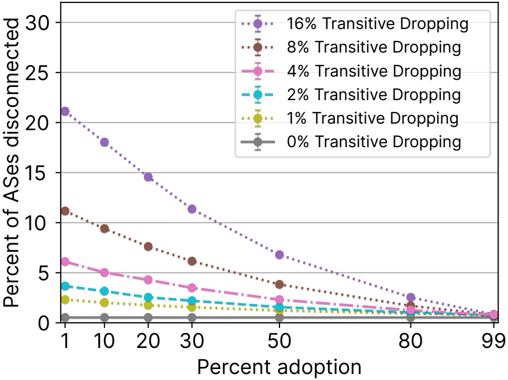
# Overhead of ProConID

- ProConID requires confirming the set of ASes in one's provider cone.
- Initial overhead shows the average number of providers verified when an AS first adopts ProConID.
- Maintenance overhead reflects additional providers they need to verify are in their provider cone as adoption increases.



# Dropped Transitive Attributes?

- Almost all (98-99% of) BGP routers forward transitive attributes they do not recognize, but this behavior is a “SHOULD” requirement in the RFC.
- A dropped transitive signature is indistinguishable from a downgrade attack.
- An AS should ensure its neighbors do not drop unrecognized transitive attributes before enforcing transitive signatures.



# Unknown Adopters?

- So far, we assumed BGP-iSec adopters and their public keys would be known to other adopters, via the RPKI or some other mechanism.
- The overall impact of even a large number of unknown adopters is small.