FC-BGP: Towards Secure Inter-domain Routing and Forwarding via Verifiable Routing Commitments

Zhuotao Liu
Tsinghua University

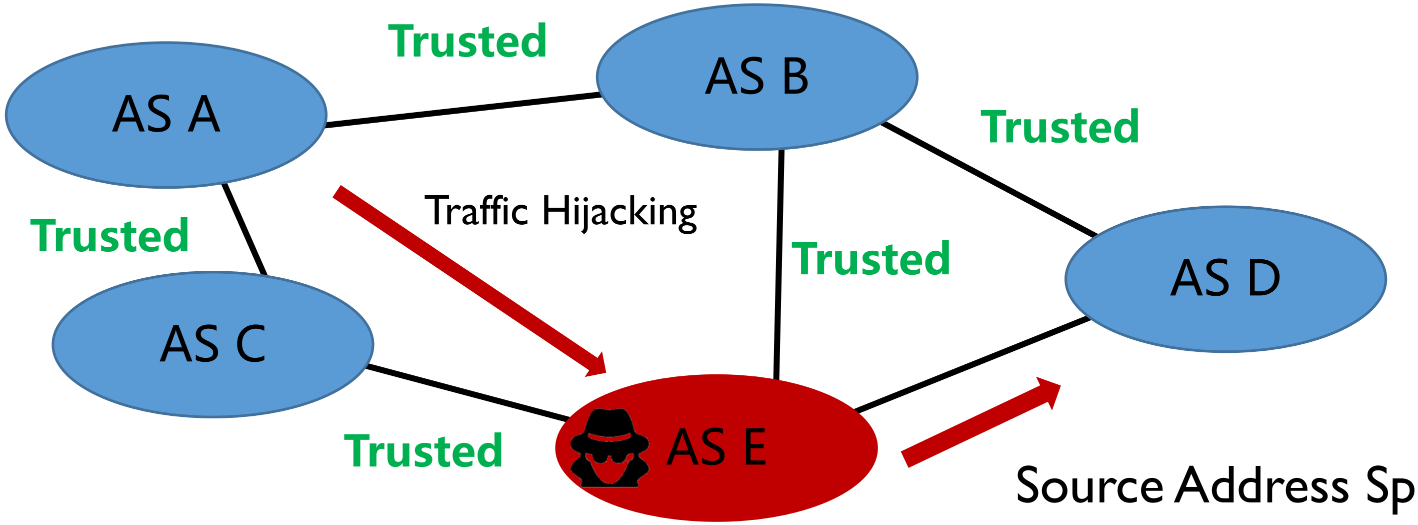
On behalf of other coauthors: Ke Xu, Xiaoliang Wang, Qi Li, and Jianping Wu

https://datatracker.ietf.org/doc/draft-wang-idr-frameworkoffcbgp/

Problem Statement

The current Internet inter-domain routing has vulnerabilities in both the control plane and the data plane.

- Control plane: no built-in mechanism that is widely deployed to verify the BGP announcements
- Data plane: the actual data forwarding path may not be consistent with the BGP path, which raises security issues



Source Address Spoofing

Forwarding Path Manipulation

Related Work

BGP Security Enhancements	S-BGP, RPKI and BGPsec, SoBGP, psBGP, Path-end, SBAS
Forwarding Path Validation	SCION, ICING, OPT, OSP, PPV, MASK, EPIC
Source Address Validation	SAVA, DPF/IDPF, BCP 38, uRPF, SPM, Passport, IPsec

Design Goals of FC-BGP

Control Plane

Full Deployment: FC-BGP can guarantee that any BGP path authenticated by our protocol is a real path announced by the on-path ASes, i.e., it is infeasible for the adversary to claim that a forged BGP path is authenticated.

Partial Deployment: FC-BGP is fully compatible with the native BGP, and incrementally deployable (i.e., FC-BGP offers strictly positive security benefits for BGP paths whose on-path ASes are not fully deployed).

Data Plane

Unwanted traffic (including traffic with spoofed sources or sent via undesired paths) can be detected by the upgraded ASes.

Problem Space

Assumption and Scope:

(i) ASes have access to an Internet-scale trust base, namely Resource Public Key Infrastructure (RPKI), that stores authoritative information about the mapping between AS numbers and their IP prefixes, and their public keys.

(ii) Multi-path forwarding (for instance due to traffic engineering / ECMP) is not considered to be a violation of data plane security

Adversary:

(i) The adversary can intercept all the BGP update messages (also referred to as BGP announcements) in the network.

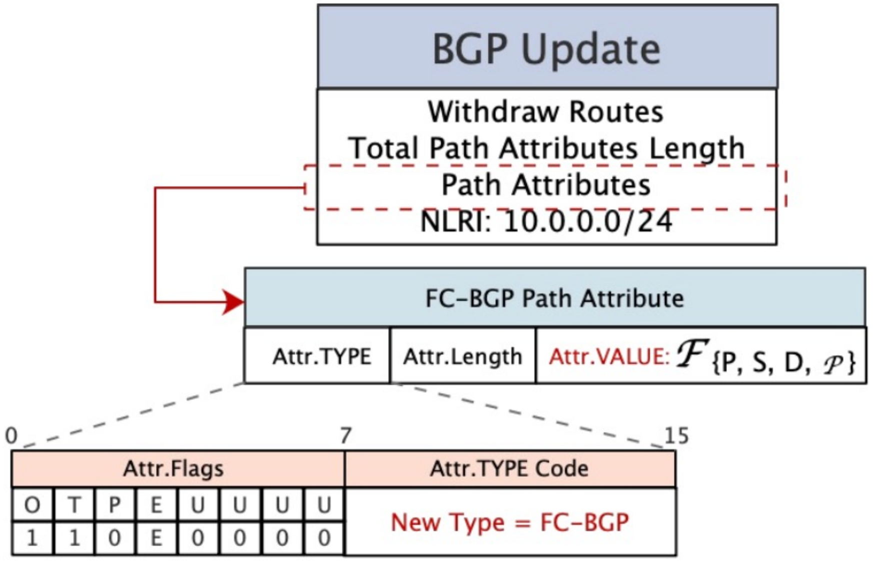
(ii) On the control plane, the adversary can launch path manipulation attacks (i.e., hijacking a BGP path with a shorter path)

(iii) On the data plane, the adversary can spoof source addresses and / or reroute the traffic to its desired ASes.

(iv) Two compromised ASes will not collude.

Primitive: Verifiable Routing Commitments

Suppose AS B receives a BGP update P:$S \leftarrow A$, AS B uses the following Verifiable Routing Commitment (or FC) to publicly certify its routing intent over the next hop to the AS C



BGP Update

Withdraw Routes

Total Path Attributes Length

Path Attributes

NLRI: 10.0.0.0/24

FC-BGP Path Attribute

Attr.TYPE	Attr.Length	Attr.VALUE: $\mathcal{F}_{\{P, S, D, \mathcal{P}\}}$

0 7 15

Attr.Flags								Attr.TYPE Code
O	T	P	E	U	U	U	U	New Type = FC-BGP
1	1	0	E	0	0	0	0	

$$\mathcal{F}_{\{A,B,C,\mathcal{P}\}} = \left\{\mathcal{H}(A,B,C,\mathcal{P})_{\mathrm{Sig}_B} \,||\, \mathsf{A} \,||\, \mathsf{B} \,||\, \mathsf{C}\right\},$$

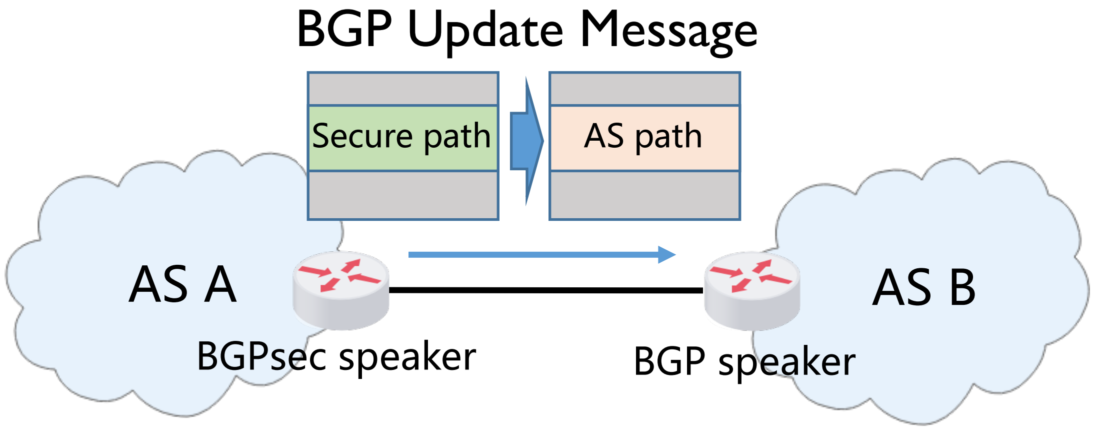
(i) FC-BGP adopts a per-pathlet validation scheme for validating BGP updates, instead of the per-path validation scheme used in BPGsec, which has two benefits

1) Same security guarantees as BGPsec in full-deployment, but with much lower path validation overhead in dynamic networks, like the Internet

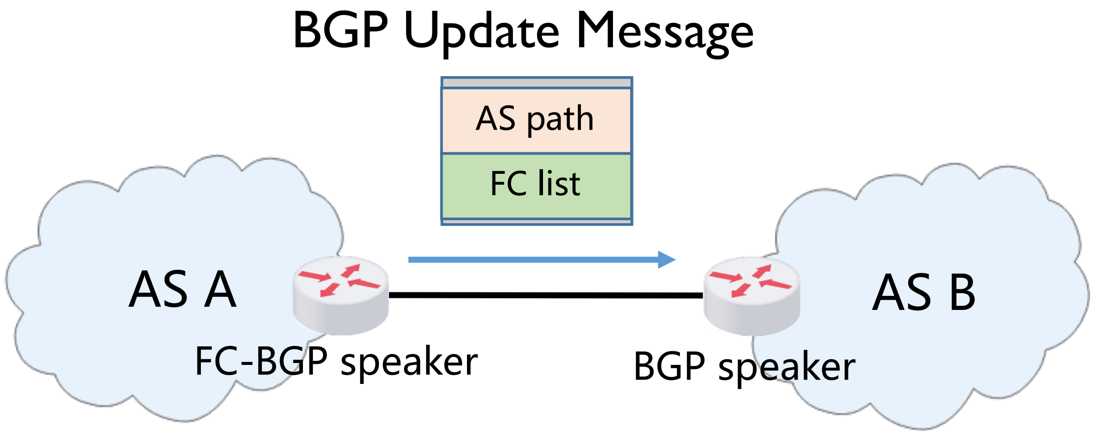
2) (Strictly) more security benefits than BGPsec in case of partial deployment

(ii) The routing intent in form of FCs does not disclose extra information about the routing policies.

FC-BGP and Native BGP



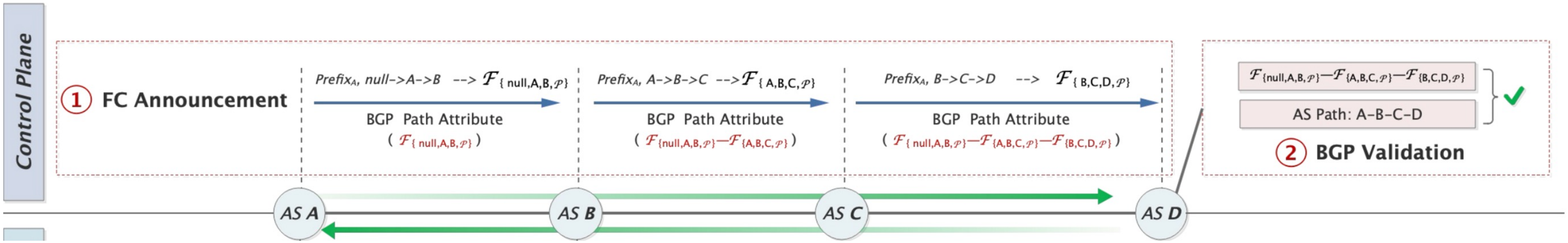
Deploying BGPsec with native BGP



FC-BGP is natively compatible with BGP

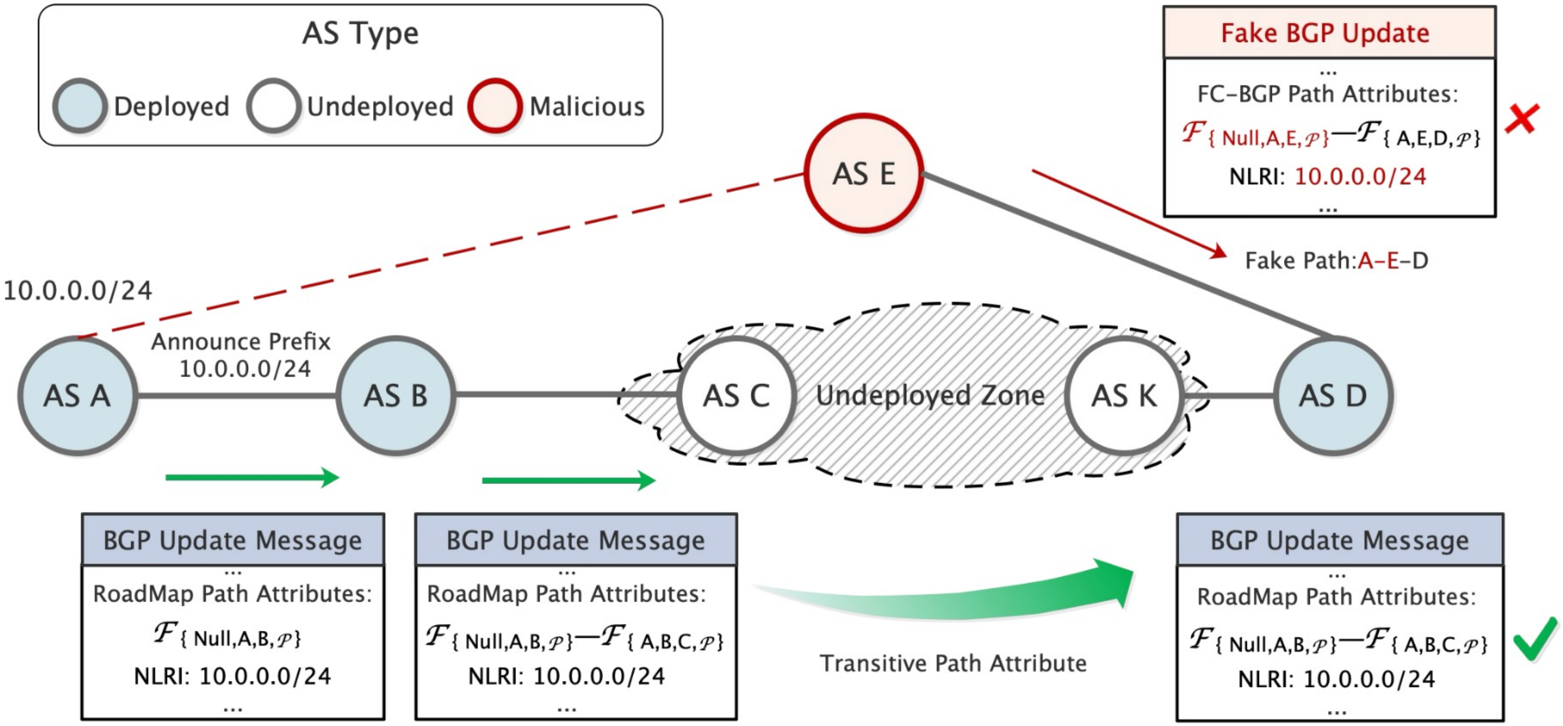
- FC-BGP does not modify the "AS Path" attribute. Instead, it defines a new transitive path attribute to carry FCs so that the legacy ASes can forward this attribute to its peers without changing any protocol.
- Thus, FC-BGP is natively compatible with the BGP. This is different from BGPsec which replaces the AS path attribute with a new "Secure path" attribute.

BGP Path Validation


Control Plane
① FC Announcement
$Prefix_A$, null->A->B --> $\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$
BGP Path Attribute
($\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$)
$Prefix_A$, A->B->C --> $\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$
BGP Path Attribute
($\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$)
$Prefix_A$, B->C->D --> $\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$
BGP Path Attribute
($\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$)
$\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$
AS Path: A-B-C-D
✓
② BGP Validation
AS A
AS B
AS C
AS D

Full Deployment

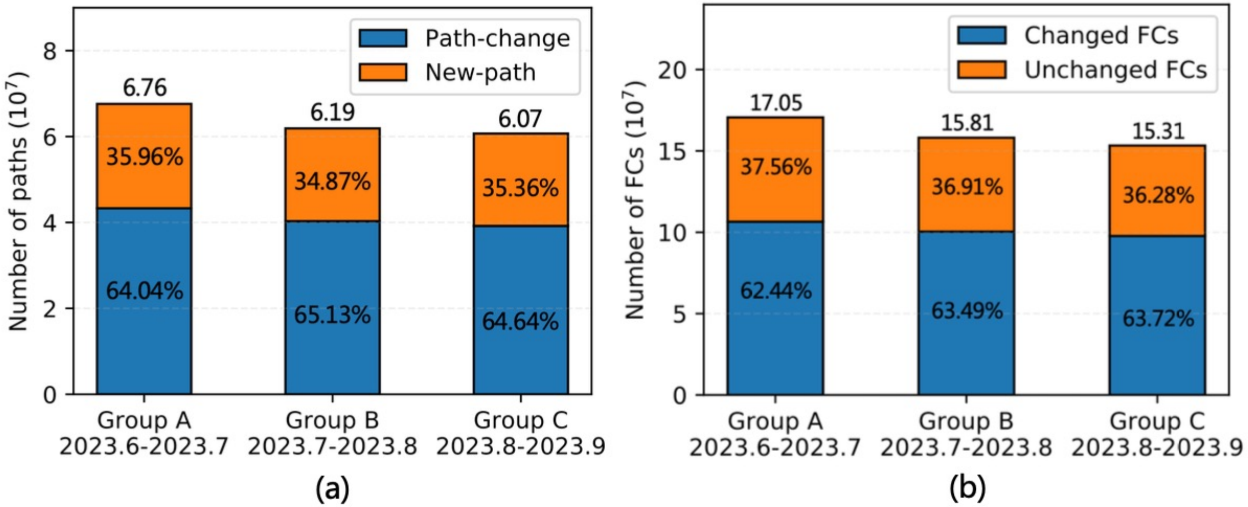
Parital Deployment



Overhead of Commitment Generation

- Using the CAIDA dataset in September 2023, we measured that the busiest AS (i.e. generating the highest number of BGP UPDATES (AS 6939)) needs to generate 138,286,813 routing commitments in one month.
- We implement a prototype of FC-BGP on the x86 platform with FRRouting and VPP.
- A single generation of the routing commitment (signed using ecdsa) takes about 0.03ms (measured on a virtual machine with 3.7Ghz CPU and 4G memory).
- A simple math: it takes 71 minutes to generate all these 138 million FCs. But these FCs are actually generated over a one-month period.

Internet-Scale Evaluation

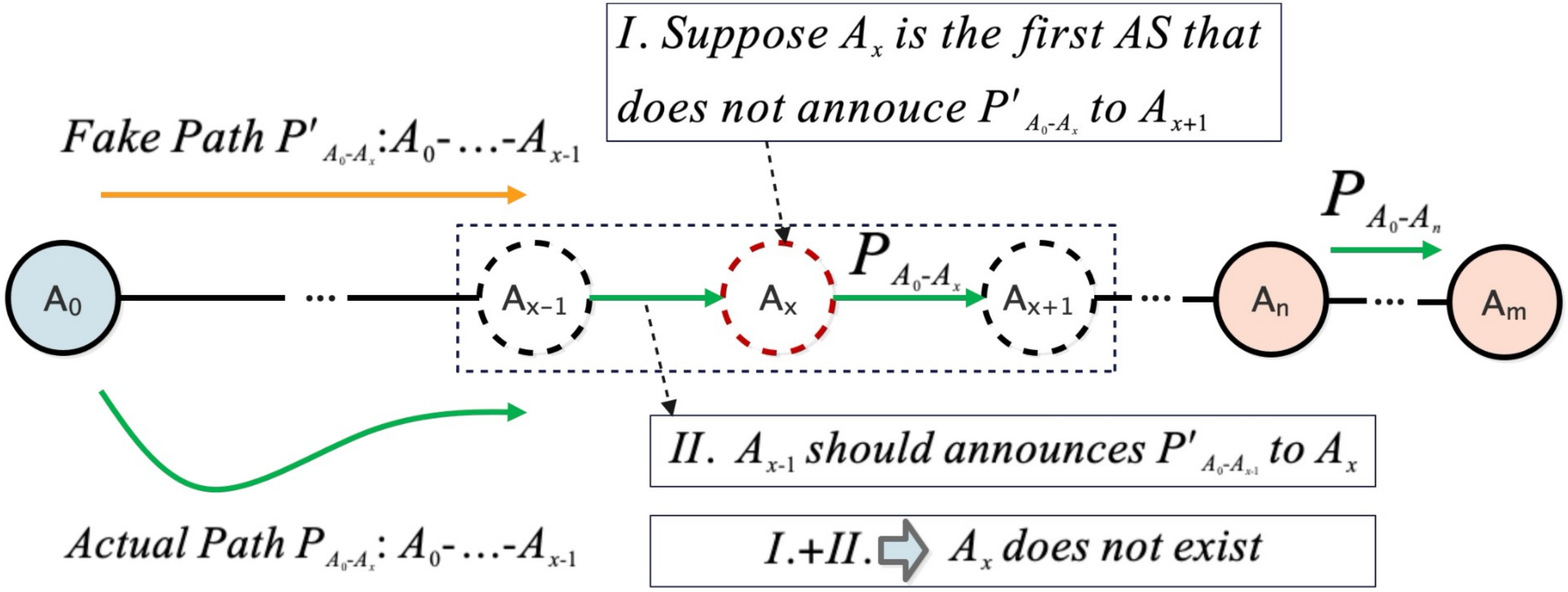


Statistical results of the BGP updates.

- We analyze the CAIDA BGP announcement datasets from June to Sep 2023
- Roughly 65% of BGP updates are path-change updates, within with over 36% of the 2-hop pathlets remain the same

Pathlet-based path verification has much smaller **dynamic verification overhead** than the path-based verification scheme (like BGPsec)

Security Analysis in Full Deployment



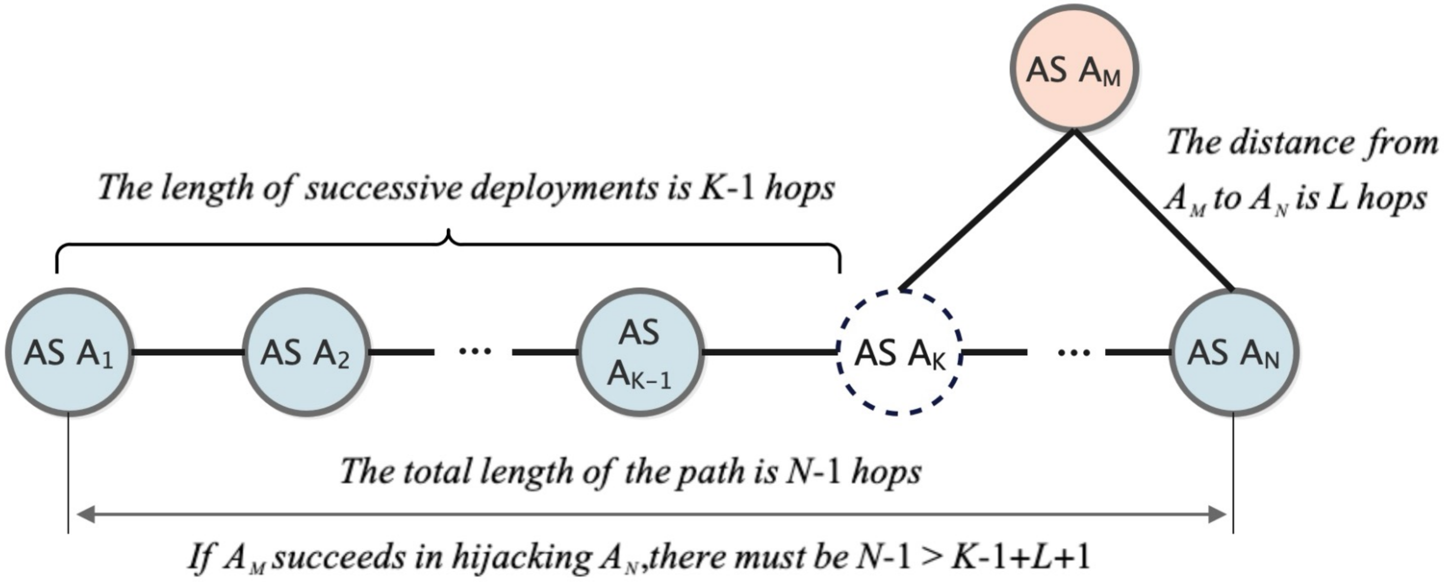
I. Suppose A_x is the first AS that does not annouce $P'_{A_0\text{-}A_x}$ to A_{x+1}
Fake Path $P'_{A_0\text{-}A_x}$: A_0-…-A_{x-1}
$P_{A_0\text{-}A_n}$
A0
…
Ax−1
Ax
$P_{A_0\text{-}A_x}$
Ax+1
…
An
…
Am
II. $A_{x\text{-}1}$ should announces $P'_{A_0\text{-}A_{x\text{-}1}}$ to A_x
Actual Path $P_{A_0\text{-}A_x}$: A_0-…-A_{x-1}
I.+II. ⇨ A_x does not exist

Key takeaways:

- Any path that can be validated by strategically combining FCs is a legitimate path announced by all the on-path ASes
- Caveat: non-colluding assumption and replay attack

See additional details in our preprint: https://arxiv.org/abs/2309.13271

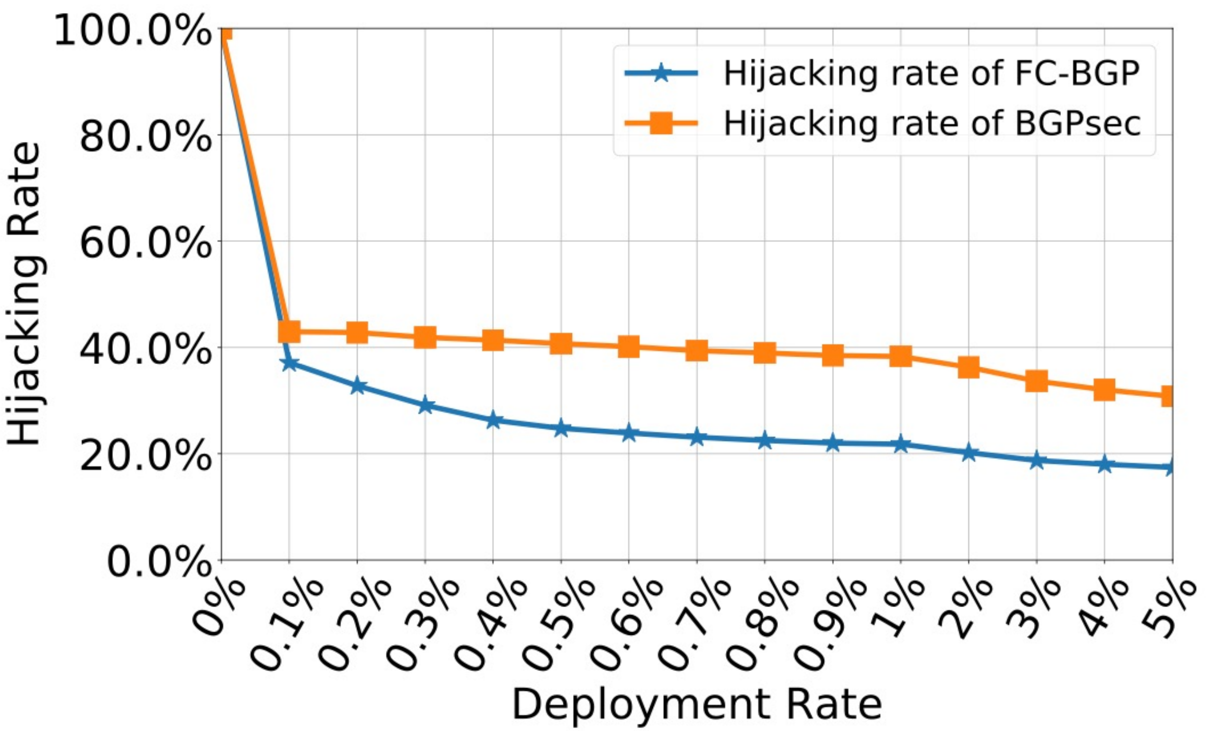
Security Analysis in Partial Deployment


AS A_M
The distance from
A_M to A_N is L hops
The length of successive deployments is K-1 hops
AS A_1
AS A_2
…
AS A_{K-1}
AS A_K
…
AS A_N
The total length of the path is N-1 hops
If A_M succeeds in hijacking A_N, there must be $N-1 > K-1+L+1$

Key takeaways

- FC-BGP is compatible with naïve BGP so that the authenticated pathlets can be passed along the way when extending the BGP path.
- Lemma: if the consecutive deployment is sufficiently long, the entire path is secured even if some of the on-path ASes are not upgraded

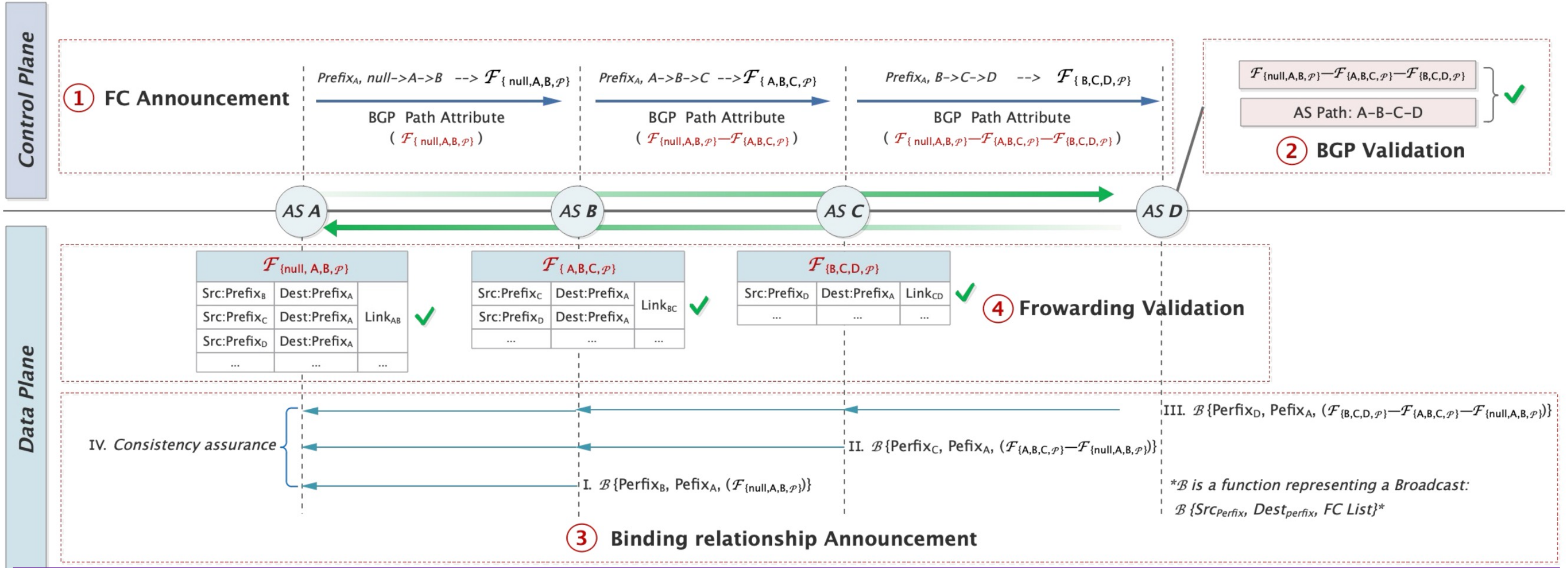
Quantified Security Benefits in Partial Deployment



- We sort the ASes according to the numbers of their negihbors
- Given a deployment rate r, we select the top r ASes to deploy FC-BGP
- Then for all the BGP updates in the CAIDA datset, we check whether the adversary can hijack a BGP update by constructing a forged but shorter AS path.
- We report the hijact rate for differnet deployment rates.

Key takeaways from this data-driven analysis:
FC-BGP provides strictly more security benefits than BGPsec in partiall deployment.

Data Plane Forwarding Validation



Control Plane

① FC Announcement

Prefix$_A$, null->A->B --> $\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$

BGP Path Attribute

($\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$)

Prefix$_A$, A->B->C --> $\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$

BGP Path Attribute

($\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$)

Prefix$_A$, B->C->D --> $\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$

BGP Path Attribute

($\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$)

$\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$

AS Path: A–B–C–D

✓

② BGP Validation

AS A

AS B

AS C

AS D

Data Plane

$\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$		
Src:Prefix$_B$	Dest:Prefix$_A$	Link$_{AB}$
Src:Prefix$_C$	Dest:Prefix$_A$	
Src:Prefix$_D$	Dest:Prefix$_A$	
...	...	...

✓

$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$		
Src:Prefix$_C$	Dest:Prefix$_A$	Link$_{BC}$
Src:Prefix$_D$	Dest:Prefix$_A$	
...	...	...

✓

$\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$		
Src:Prefix$_D$	Dest:Prefix$_A$	Link$_{CD}$
...	...	...

✓

④ Frowarding Validation

III. $\mathcal{B}$\{Perfix$_D$, Pefix$_A$, ($\mathcal{F}_{\{B,C,D,\mathcal{P}\}}$—$\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$)\}

II. $\mathcal{B}$\{Perfix$_C$, Pefix$_A$, ($\mathcal{F}_{\{A,B,C,\mathcal{P}\}}$—$\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$)\}

I. $\mathcal{B}$\{Perfix$_B$, Pefix$_A$, ($\mathcal{F}_{\{null,A,B,\mathcal{P}\}}$)\}

IV. *Consistency assurance*

**$\mathcal{B}$ is a function representing a Broadcast:*

*$\mathcal{B}$ \{Src$_{Perfix}$, Dest$_{perfix}$, FC List\}**

③ Binding relationship Announcement

Key takeaways:

- By back-propagating (and broadcasting) the verifiable routing commitments in FC-BGP, the on-path (and off-path) ASes can learn the desired forwarding path on the data plane, based on which they can choose to enforce certain policies (such as filtering unwanted traffic).

Conclusion

- ✓ FC-BGP is a novel secure inter-domain routing system that can simultaneously authenticate BGP routing updates and validate data plane forwarding in an efficient and incrementally-deployable manner.
- ✓ FC-BGP is built upon a unified primitive, named Verifiable Routing Commitment, to enhance the security of control plane routing and data plane forwarding.
- ✓ FC-BGP is fully compatible with BGP, and incrementally deployable by offering strictly positive security benefits in partial deployment. FC-BGP has the same security guarantee as BGPsec in full deployment, while imposing much lower verification overhead.

See additional details: *https://datatracker.ietf.org/doc/draft-wang-idr-frameworkoffcbgp/*

Thank You！