BGPSecurity in Partial Deployment
Is the Juice Worth the Squeeze?

Robert Lychev, SHaron Goldberg, Michael Schapira

Presenter: Mingwei Zhang

October 8, 2015

Table of Contents

Border Gateway Protocol

Border Gateway Protocol

The de-facto inter-domain routing protocol

Functionality:

- Connect Autonomous Systems (ASes), e.g. ISPs
- Exchange IP block reachability information

BGP Security Issues

There are two main security issues in BGP:

- IP prefix hijacking
- AS path forgery

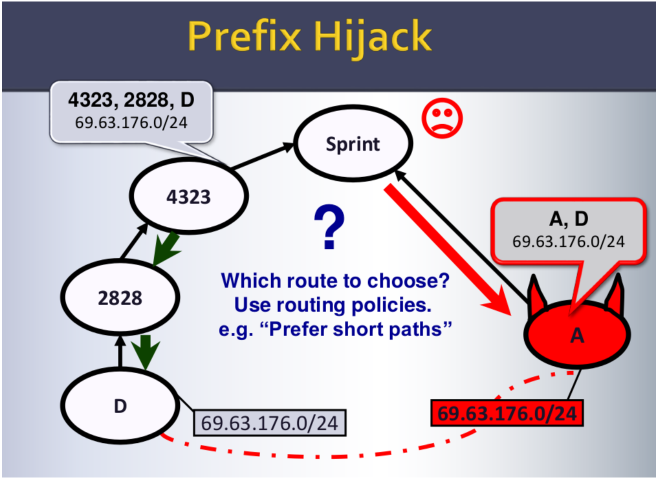
IP prefix hijacking

The attacker claims to be the origin AS of certain prefixes.

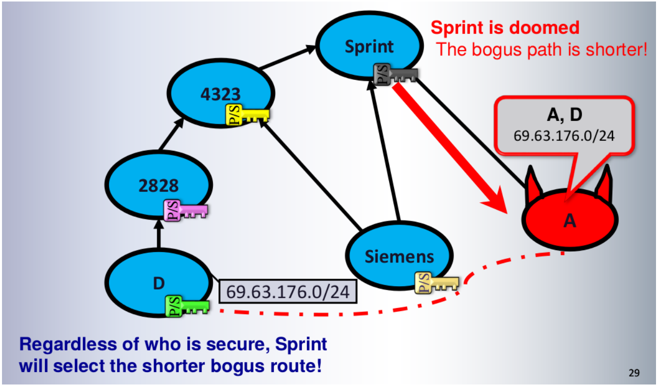
AS path forgery

The attacker claims to have a non-existing path toward the prefixes.

Prefix Hijacking Example



Path Forgery Example



BGP Security Solutions

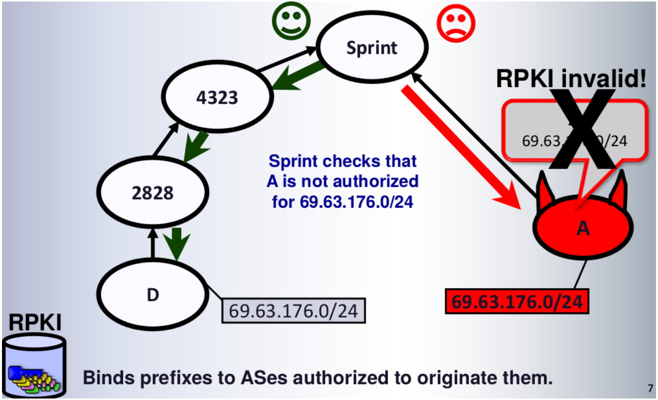
RPKI (resource public key infrastructure) cryptographically secure the prefix ownership information.

- it stores all the secure objects in several centralized repositories
- a router can verify a prefix announcement by compare the origin information with RPKI database
- the results can be valid, invalid, or unknown

BGPSEC tries to secure AS paths updates by requiring all ASes sign their updates.

- On each propagation, an AS will sign the path with its own private key
- a verifier can look at the signatures of all the ASes in the path and verify against their public key

RPKI Example



BGPSEC Example

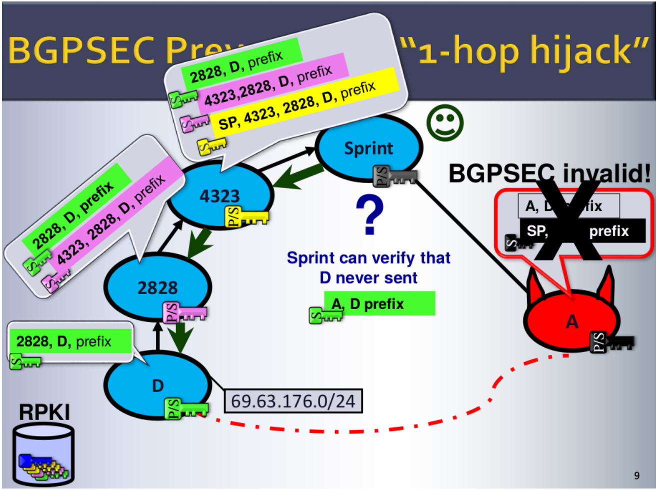


Table of Contents

BGP Decision Making

Each autonomous system (AS) operates on its own policy, and a BGPSEC secured route may not represent its best interests.

The million dollar question:

Are the ASes going to prefer a more secure route over a legacy route?

BGP Decision Making

For each BGP update, the following aspects needs to be considered to decide whether to accept the update or discard it:

- **Security:** whether the path is secure, and the origin is authorized
- **Local preference:** whether the nexthop is a customer (making money), or a provider (losing money), or a peer.
- **AS paths:** which path is shorter
- **Tie breakers:** e.g. geographic location, priority, etc.

BGP Decision Making with Security

The authors defined three levels of securities, and surveyed 100 network operators.

- **Security 1st: (10%)** always prefer secure routes over insecure routes.
- **Security 2nd: (20%)** cost is more important than security. (i.e. customer is preferred)
- **Security 3rd: (41%)** cost and path distance is more important than security.

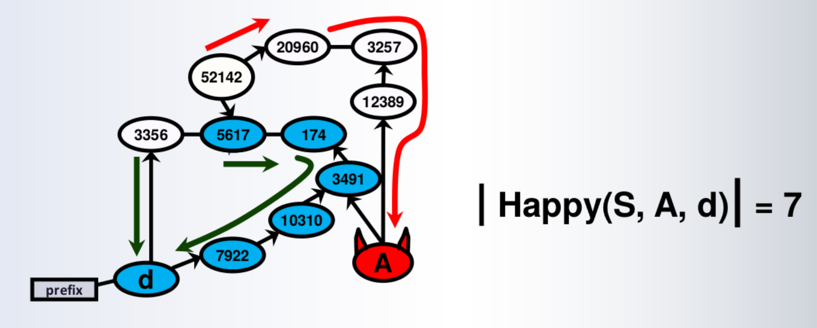
Threat Model

The attacker

- claims to be directly connected to the target AS, shortens the path
- announces the updates using legacy BGP protocol

Happiness

If a AS does not use the attacker's fake path, it is "happy".



Quantifying Security

$$H_{M,D}(S) = \frac{1}{|D|(|M-1|)(|V-2|)} \sum_{m \in M} \sum_{d \in D \setminus \{m\}} H(m, d, S)$$

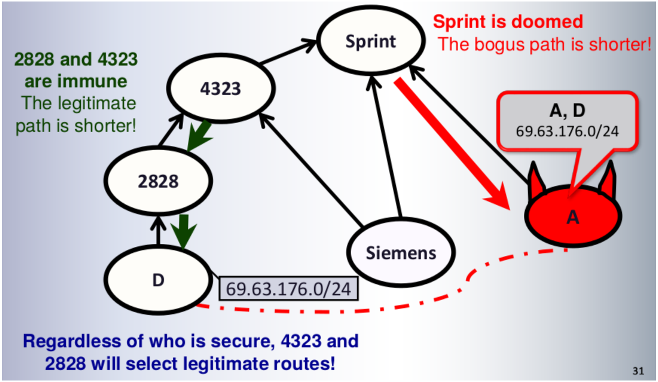
or

$$H_{M,D}(S) = \frac{1}{|V|^3} \sum_{m \in M} \sum_{d \in D \setminus \{m\}} H(m, d, S)$$

- S – BGPSEC enabled ASes
- M – Set of attacker ASes
- D – Set of target ASes
- V – All ASes
- H – **Happiness**: number of ASes that will not select the attacker's path

Observations

Under Security 3^{rd} model, Sprint is doomed, Siemems has a chance, 2828 and 4323 are immune.



Observations

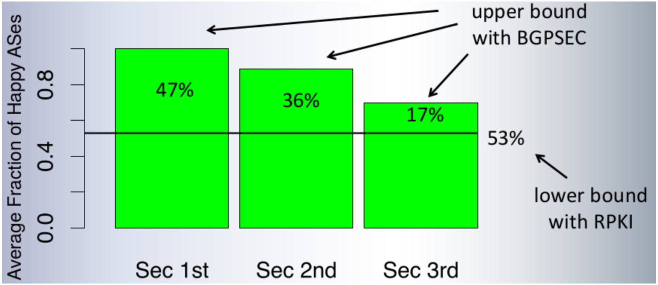
Regardless of the BGPSEC deployment:

- Doomed ASes: always choose bogus routes
- Immune ASes: always choose legitimate routes

Upper bound and lower bound of the overall happiness:

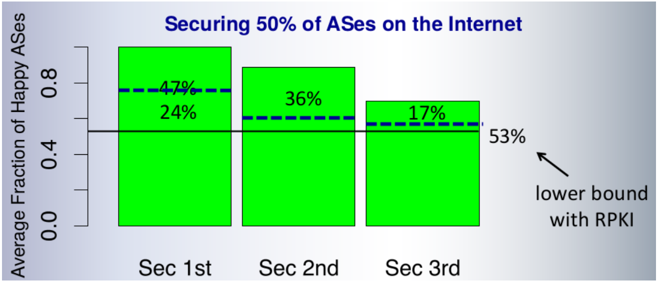
- Upper bound: 1 - fraction of doomed ASes
- Lower bound: fraction of the immune ASes

Security Improvement - Full Deployment



With full deloyment, in the most realistic security 3^{rd} model, we can only achieve 17% more security than simply doing RPKI (lower bound).

Security Improvement - Half Deployment



Security 3^{rd} – 4%
Security 2^{nd} – 8%

Takeaway

Main takeaway

Unless reaching very high deployment percentage, BGPSEC cannot provide much security improvement under the most popular security 3^{rd} model.