BGP Community-based Attacks and Community Origin Authentication

draft-liu-sidrops-community-authentication

Yunhao Liu, Jessie Hui Wang, Yangyang Wang, Mingwei Xu
Tsinghua University

IDR WG, IETF 118

Presenter: Jessie Hui Wang <jessiewang@tsinghua.edu.cn>

BGP Community

- Definition: BGP community is a group of destinations which share some common property [RFC1997].
- In practice, it is an optional transitive BGP attribute used to tag meta-data in route announcements. It provides the ability to signal opaque information within separate namespaces to aid in routing management [RFC8092].
- Its usage in the Internet has continued to increase during the past decade. Two types [RFC8195]:
  - Informational community: labeling the routes that have particular properties
  - Action community: notifying upstream ASes to conduct some actions

BGP Community Values

- The values and semantics of communities must be negotiated between the two ASes.
  - One AS defines a BGP community value (definer), can be viewed as providing a service
  - Other ASes can then tag the value on some routes to request the service from the definer. They are community taggers and service requesters.

Community-based Attacks

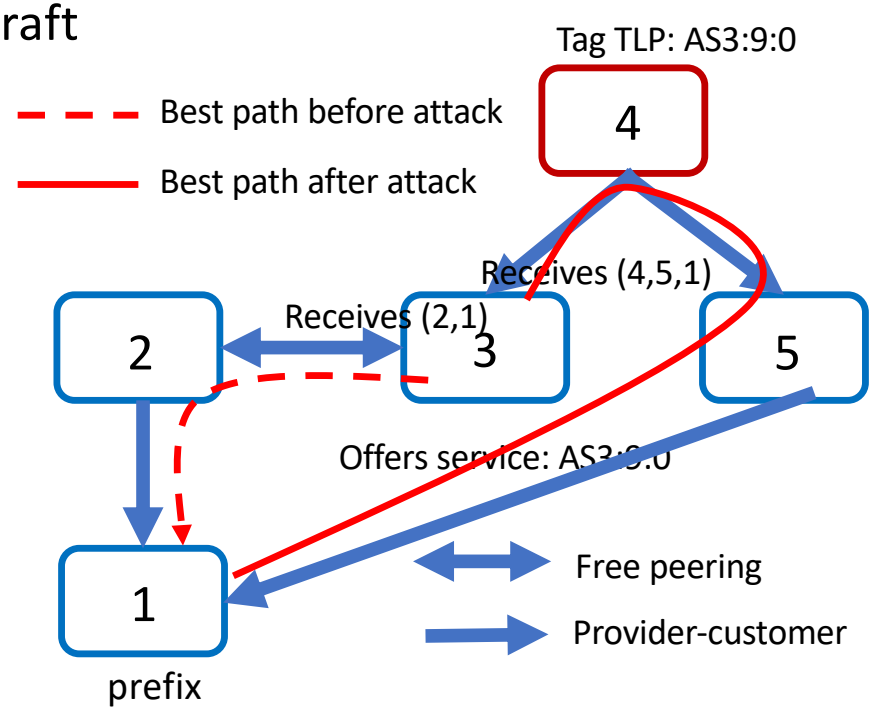
- Currently, any AS on the forwarding path can add any community values to a routing announcement.
- The recipient cannot determine which AS on the path added any of the community values.
- As stated in [RFC7999], "BGP contains no specific mechanism to prevent the unauthorized modification of information by the forwarding agent."
- Therefore, BGP community values may be used to influence the routing system in unintended ways.

Community-based Attacks

- Take one type of community as an exampe: Tuning local preference (TLP)
- More examples and more analysis are in the draft

Preference Class	Example Community Value
Above customer route	ASX:7:0
Normal customer route	ASX:8:0
Backup customer route	ASX:9:0
Peering route	ASX:10:0
Upstream transit route	ASX:11:0
Fallback route, to be installed if no other path is available	ASX:12:0

Preference Classes and Example Community Values in TLP Service



AS3 suffers financial loss since it needs to pay AS4

It is necessary for AS3 to check whether AS 4 is allowed to use this community value.

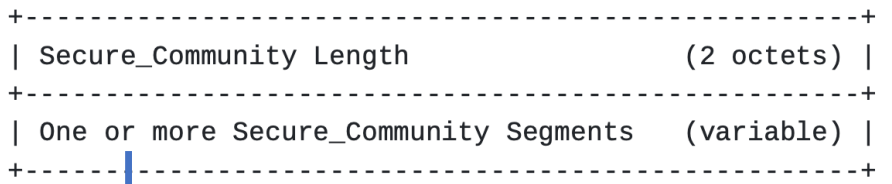
Community-based Attacks in the Wild

- It is difficult, if not infeasible, to detect community-based attacks, since business agreements are usually private.
- One reported case is in July 2018, in which BGP community-based attacks were used to increase the propagation of hijacked routes.
- A research effort tried to explore the effectiveness of community-based attacks in the Internet.
  - They send routes with 307 verified RTBH community values identified in [GV17], and compare the routing before and after attacks.
  - among the 307 RTBH community values , 25 community values successfully blackholed the traffic from at least one vantage point, which means the attacks using them are successful.
- The attacks do not modify AS_PATH attribute, so RPKI and BGPSec cannot prevent them.

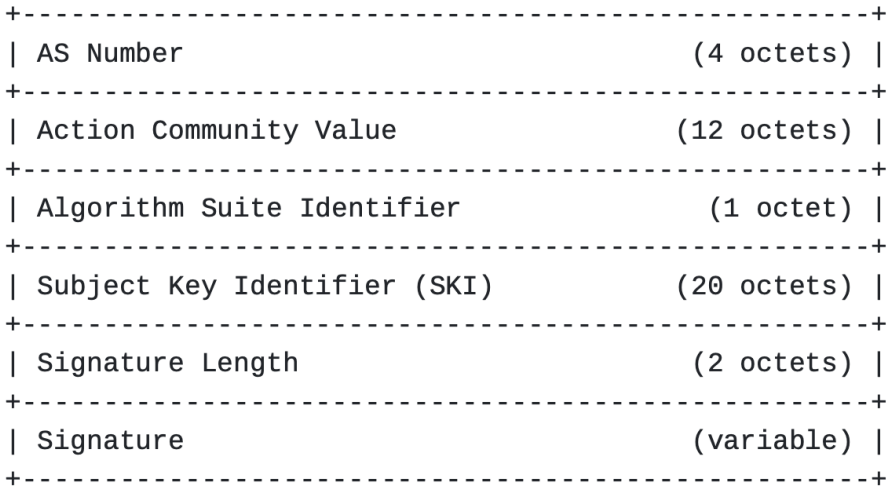
Community Origin Authentication

- Add a new BGP attribute, SecCommunity
- Based on RPKI certificates.
- Community tagger
  - Must have a RPKI certificate to generate digital signatures to make sure its identity is authentic and knowable to the recipient.
- Community definer (the route recipient and the one to take action)
  - define a community access control list (**CACL**) that specifies which ASes are granted or denied access to a particular action community value it defines.
  - verify the digital signature to know the identity of the community tagger and then check whether the community tagger is allowed to add this community value by consulting its pre-configured CACL.
  - Conduct actions if permitted by the list. Then remove the community value from the route.

Community Origin Authentication



SecCommunity Attribute Format



Secure_Community Segment Format

- Each SecCommunity speaker should have a RPKI certificate to generate signatures.

The tagger

RFC 8092: The first 4 octets is the ASN. The last 8 octets is operator-defined value.

The identifier in the SKI field of the router certificate, to associate the private/public key when validation.

The signature for validation

Practical Considerations and IANA Considerations

- Incremental Deployment
  - SecCommunity does not need all ASes on the path to do signatures or validations. It only needs to be signed by the AS who uses action community service and verified by the AS who provides this service to get the benefits.
  - Other Ases just ignore the new attribute.
- IANA
  - register a new path attribute "SecCommunity" in the "BGP Path Attribute" registry under the "Border Gateway Protocol (BGP) Parameters" registry group.

BGP Community in Other RFCs

- Restricting the usage of BGP community in [RFC5635] and [RFC7999]
  - [RFC7999] point out that "BGP announcements carrying the BLACKHOLE community should only be accepted and honored if the neighboring network is authorized to advertise the prefix".
  - [RFC5635] These announcements must NOT be propagated outside the local AS and should carry the NO_EXPORT community.
- However, they only focus on one type of BGP community, i.e., blackholing, and require that community values should only convey information between two neighboring As.
- Measurements showed that almost 30% of the blackholing community values traveled more than one hop, which indicates that these recommendations are not respected.
- The restriction of one-hop significantly reduces the value of BGP communities and cannot work for all community values.

Next Steps

- Comments and discussions via emails or on the IDR list
- Keep improving the draft
- Attend IETF 119 in person
- Implementations if we get positive feedback