Preventing Route Leaks using a Decentralized Approach

Miquel Ferriol Galmés
Roger Coll Aumatell
Albert Cabellos-Aparicio
Universitat Politècnica de Catalunya
Barcelona, Spain
{mferriol, roger.coll.aumatell, acabello}@ac.upc.edu

Shoushou Ren*
Xinpeng Wei
Bingyang Liu
Huawei Technologies Co.,Ltd.
Beijing, China
{renshoushou, weixinpeng, liubingyang}@huawei.com

Abstract—**In the inter-domain routing infrastructure, a route leak is defined as a violation of the routing policy agreed between two Autonomous Systems (AS). Specifically, one AS leaks a route from another AS. There are many examples where route leaks have resulted in large-scale outages on the Internet, taking down several services. Although route leaks seem a simple problem, the solution is complex because: (i) ASes consider -partially- routing policy private, (ii) lack of a formal and standard language to express routing policy and (iii) BGP lacks adequate cryptographic-based security. In this paper, we present a novel architecture that provides a solution to route leaks by addressing these three key issues. We define a formal language to express routing policy and we design a blockchain-based architecture to securely communicate it. Our decentralized architecture allows having private policies and interfaces with the current BGP infrastructure seamlessly.**

I. Introduction

The Border Gateway Protocol (BGP) is the inter-domain routing protocol that *glues* the Internet. BGP provides reachability and path selection, but as the Internet evolved and business-oriented Autonomous Systems (AS) started to provide connectivity, there was a need to convey complex, rich and fine-grained policies. As a result, BGP was extended with BGP Communities [1].

Route leaks occur when one AS violates the routing policy agreed with another ASes. The most common violation is when an AS incorrectly leaks a route learned from another AS. To illustrate this, consider two ASes that have a *peering* relationship. In such a relationship, the cost of the connection is shared among the ASes since the goal is to exchange traffic originated in the peering ASes (or its customers). As a result, ASes must not propagate routes learned from peering connections. This is typically signalled using BGP communities. If these routes are leaked to other ASes then one of the peering ASes is effectively providing *transit*. Route leaks are considered an important security threat. In today's Internet route leaks are common and result in large-scale disruption, see [2] as an example. Even

Route leaks are a simple problem but hard to fix. The main reasons for this are that first, the BGP protocol lacks of cryptographic-based security mechanisms. Although the IETF has introduced proper security protocols for BGP: RPKI [3] and BGP-SEC [4], such protocols have not seen widespread deployment and adoption, mainly because of the high deployment cost [5]. And second, because inter-domain routing lacks a standard mechanism to communicate routing policy among ASes. This is typically done out-of-band (website, email, etc) thus, the overall inter-domain routing is prone to misconfiguration. To further exacerbate this issue, some ASes consider -partially- its routing policy as confidential and they avoid full public disclosure.

One of the most common mechanisms to define and signal routing policy in today's internet is BGP communities. BGP Communities are an optional attribute attached to a BGP message. This attribute can be used to tag the message and convey meaningful information or request a specific action from an AS. For instance to request that a prefix is not announced through certain links.

BGP communities are not formally defined, this means that the meaning of the community value is agreed among groups of collaborating ASes indepen-

*Corresponding author.

This work was supported by the Spanish MINECO under contract TEC2017-90034-C2-1-R (ALLIANCE) and the Catalan Institution for Research and Advanced Studies (ICREA).

Annex to ISBN 978-3-903176-28-7© 2020 IFIP

dently, this is often done using an out-of-band mechanism such as the phone or a central website. This issue, coupled with the lack of security mechanisms protecting BGP communities, means that communities are error-prone and again, a source of many misconfiguration and security threats in inter-domain routing.

In this paper, we present a solution to the route leak problem. Our solution is based on proposing a formal and expressive language for BGP communities. This addresses the inherent error-prone nature of BGP communities. The formal language is then authenticated and transmitted to the different participating ASes in a secure way using a blockchain-based solution. Once the policy is securely stored in the distributed ledger, participant ASes can download and automatically install standard BGP route filters, that will ultimately enforce the routing policy. We have prototyped and open-sourced both our formal language as well as the distributed ledger [16].

In our proposed solution, the formal language prevents misconfigurations, while the distributed ledger provides cryptographic-based security, preventing security threats. Since our solution ultimately outputs standard BGP route filters, it does not require changes to BGP routers or to protocol itself, resulting in a low deployment cost. Finally, the distributed ledger has a flexible consensus algorithm that allows representing the existing trust relationship between ASes.

II. Problem Statement

This section describes the main problem addressed in this paper: Route leaks.

A. Route Leak

The security of the Border Gateway Protocol (BGP) lacks of a specific mechanism, and it is fundamentally based in trust among the different participating ASes. This makes this protocol vulnerable to a different number of security threads [6] [7] [8] [9].

An important BGP security threat are *route leaks*. Route leaks have produced large-scale disruptions on the Internet. As described by the IETF [10] a route leak is the propagation of routing announcements beyond their intended scope. In other words, a BGP route leak occurs when an announcement from an AS violates the policies of one of the ASes along the AS path. Indeed, the different ASes usually define their different policies for importing and exporting routes according to the business relationship between them. We can divide the existent business relationships between two ASes as follows: 1) Customer-Provider; 2) Peer-Peer; 3) Sibling-Sibling relation. In the first one, the provider AS offers transit to the customer. In the second one, two neighbours AS usually only exchange their customers' traffic. And finally, in the third one, both ASes offer transit for each other. In this context, a route leak is a violation of such routing policies.

As a result of a route leak, traffic can be redirected through an unintended path, traffic loss due to sub-optimal routing, blackholing a prefix or traffic hijacking. Route leaks can be malicious, but often they are the result of accidental misconfigurations. The fundamental reason behind this is that BGP does not have an effective mechanism to define and communicate policy.

BGP route leaks cause important service disruption on the Internet. As a recent example, on June 24, 2019, several websites started to have performance issues, including Discord, AWS services, and privacy management services such as OneTrust. According to [11], on that day Allegheny Technologies Inc. propagated prefixes received from one of its providers (DQE Communications) to another provider (AS701 - Verizon).

As shown in figure 1, AS33154 sent to his customer AS396531 routes for several popular Internet destinations such as Amazon, Facebook and Cloudflare. Due to a misconfiguration, AS396531 leaked such routes to AS701 (another AS396531 transit provider). In a normal scenario, a customer should never send such routes. As a result, AS701 accepted these routes and advertised them, leaking them on a global scale. In turn, some ASes used this new route to reach the popular services, but AS701 was not suitably equipped to deal with this drastic increase in traffic, resulting in packet loss. As a consequence, there was a major outage of such popular customer-facing services, this lasted for roughly 126 min.

III. Background: BGP Communities

BGP *does* provide a mechanism to communicate routing policy: BGP communities. This is a transitive attribute attached to BGP signalling messages that allow for tagging routes and for modifying BGP routing decisions on upstream and downstream routers. BGP communities can be added, removed, or modified as the message travels from AS to AS.

In the BGP community attribute, the first 16 bits represent the AS Number (ASN) of the entity defining the community, while the last 16 bits indicate an action or label. The human-readable community format separate the ASN and the action/label with a colon, e.g. 174:3020.

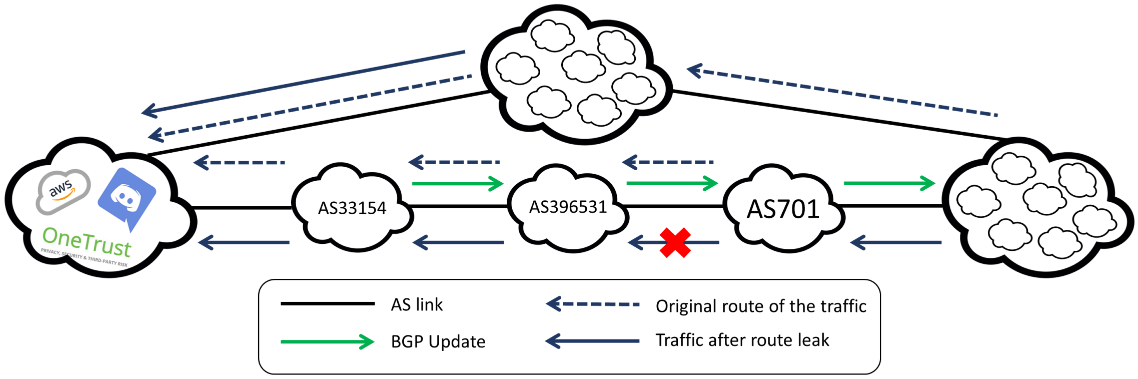

Fig. 1: DQE (AS33154) announces these specific routes to their customer (AS396531 - Allegheny Technologies Inc). This BGP Update is forwarded to another AS396531's transit provider (AS701), who proceeded to further propagate this new path. Then, a big portion of the traffic with destination AWS, Discord, OneTrust, etc was redirected via these 3 ASes. AS701 was not able to handle the increase of traffic resulting in an outage.

The RFC1997 [1] predefines a small set of predefined:

- NO_EXPORT(65535:65281): the route should not be propagated over eBGP.
- NO_ADVERTISE(65535:65282): the route should not be propagated over BGP at all.
- NO_PEER (65535:65284): The route should not be advertised over peering relationships.

The use of communities has increased considerably within the last years. *F. Streibelt et al.* [13] experimentally measure this aspect finding that the number of communities has increased by 18% over 2017. They also found that ASes use communities to advertise routing policies, bias paths, peer selection, tagging origins, selective advertising traffic engineering, dropping of traffic to a target destination to mitigate Denial-of-Service-Attacks, among others.

However and fundamentally, BGP communities are *ill-defined*. Indeed, each AS is free to define the optional BGP communities. As an example, an AS can define its own 2^{16} set of communities. This definition is typically done through documentation and using natural language by the network administrators. The scope of this definition spans a set of ASes that have a business relationship [14].

Besides, BGP does not provide any mechanism to *secure* communities. BGP communities travel as plain text in the BGP data-plane. This means that communities can be spoofed, forged, modified or removed while in transit. As a result, it is well-documented that BGP communities represent an important attack vector and can be manipulated to influence routing in unintended and disruptive ways [13].

A. *BGP Communities: An Example*

Figure 2 shows an example of how communities are commonly used. In this scenario, AS1 initiates the BGP update process by sending a message to AS2. Then AS2 tells to AS5 and AS3 that the learned route comes from North America (using the community 1:200). Also, AS2 asks to AS3 to prepend itself 3 times by using the community 3:103. This is done to perform route selection, once AS4 receives both announcements for p1, it will prefer the shortest path via AS5.

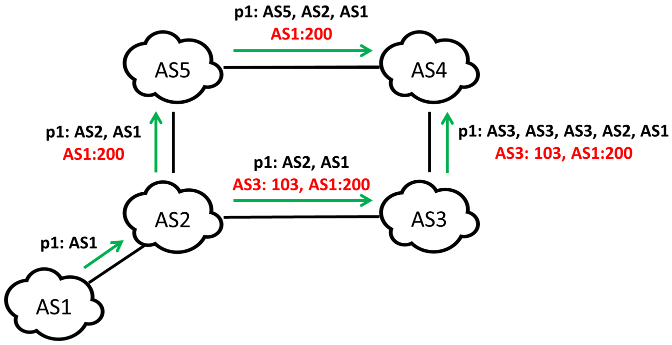

Fig. 2: Example of the use of BGP communities. AS1 request a path prepending by adding AS3:103 to the BGP message sent to AS3, and informs that prefix p1 is a North America located prefix by attaching community AS1:200.

IV. Proposed Architecture

A. *Overview*

In this paper, we take advantage of BGP communities to address the challenges of route leaks. Specifically, we propose an architecture that provides a formal definition of routing policy and a secure mechanism to communicate it to participating ASes.

An important design principle of our architecture is that it does not require any change on BGP routers, the BGP protocol or BGP communities. Our solution interfaces with the current infrastructure while providing the above-mentioned advantages.

Figure 3 shows a step-by-step example of our architecture. First, we define an expressive and formal language used to describe routing policy. The language is used by network operators to define their routing policy. This prevents misconfigurations due to ambiguity or the ill-defined nature of BGP communities. Once the policy has been defined by the network administrator, it is uploaded to a distributed ledger (top figure).

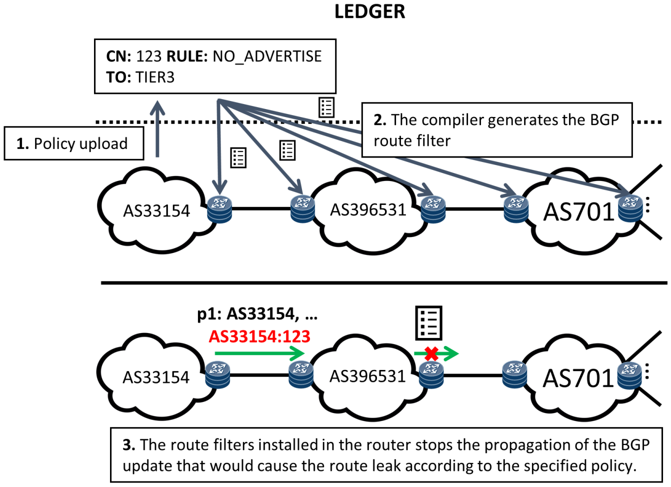
LEDGER
CN: 123 RULE: NO_ADVERTISE
TO: TIER3
1. Policy upload
2. The compiler generates the BGP route filter
AS33154
AS396531
AS701
p1: AS33154, ...
AS33154:123
AS33154
AS396531
AS701
3. The route filters installed in the router stops the propagation of the BGP update that would cause the route leak according to the specified policy.

Fig. 3: Overview of the architecture

The distributed ledger is shared among the participants ASes and it is used to securely communicate the routing policy. We expect that participants are ASes that have already an existing business relationship and thus, have an incentive to participate and a certain amount of trust.

The distributed ledger makes the routing policy from the source AS available to the participants AS in a secure way, providing privacy (when needed) and authentication. With this, the destination ASes can download the policy and configure it in their existing BGP routers.

Specifically, we provide a compiler that translates the formal language used to define the policy to standard BGP route filters. Ultimately, these BGP route filters are enforcing the policy and preventing route leaks.

B. Formal Language for BGP Routing Policy

This section defines an expressive and formal language used to define routing policy. In order to define the language we have analyzed a wide variety of real-world routing policy datasets [15] [17] as well as the available literature [18] [19]. This methodological approach is used to make sure that the language is expressive enough to cover any BGP policy, including policy related to route leaks. The proposed language contains 5 parameters, specifically:

- ASN: The Autonomous System Number.
- CN: The Community Number.
- Rule: The policy, most common ones are LOCAL_PREFERENCE, PREPEND, NO_ANNOUNCE, NO_EXPORT.
- Value (optional): This attribute is only applied to some type of rules. Normally it is an integer and defines the quantity of a given effect.
- To (optional): what the rule refers to. When this attribute refers to a certain geographical location, the ISO 3166-1 is used.

C. Distributed Ledger

BGP security is strongly related to business and trust relationships, as a result, the distributed ledger has a set of requirements to support such scenario:

- The different participant ASes on the network must be able to authenticate.
- The distributed ledger needs to be permissioned. In a BGP scenario, the participant ASes have certain business relationships. This means that the distributed ledger can be governed based on this existing trust.
- Privacy and confidentiality of transactions and data about different business transactions. The data must be kept private and should only be accessible to intended ASes.

The process used to upload a new policy to the ledger is summarized below:

- Execute a transaction and verify its correctness.
- Order transactions via a consensus protocol.
- Validate a transaction against a specific endorsement policy before committing them to the ledger.

The aforementioned endorsement policy specifies which peer nodes (ASes), or how many of them, need to vouch for the correct execution of a given transaction. Thus, each transaction needs only to be executed (endorsed) by the subset of the peer nodes required to satisfy the endorsement policy. Once again, this policy is highly configurable and can be adapted to the existing trust model of the participant ASes.

V. State-of-the-Art

Currently, route leaks are prevented using the information available at Internet Route Registries (IRRs) to create different routing filter, however, this solution is mainly manual and thus, costly and error-prone. Several automatic solutions have been implemented (e.g, [20], [21]), but they are based on monitoring several vantage points and thus, are only useful in such points.

Researches have attempted to use anomaly detection techniques to detect route leaks, specifically by looking at the history of the announcements and trying to identify anomalies, which can potentially be a route leak [22], [23], [12].

A third approach is by extending the BGP protocol itself, a notable example is BGP-SEC that provides formal security to BGP signalling, requiring each BGP hop to perform certain cryptographic operations over each BGP message [24]. BGP-SEC operates in conjunction with Resource Public Key Infrastructure (RPK) [3], which defines and stores certificates for inter-domain routing assets (prefixes, AS numbers, etc), providing formal authentication. This solution has not been widely deployed, mainly to the high deployment cost, particularly by the required cryptographic operations performed at the BGP routers.

The most similar work to this paper is a method based on secure multi-party computation (SMPC) that outsources the route computation where the different ASes send information about the existing relationships with their neighbours [25]. Also, this work [26] proposes a blockchain used by the ASes to record all BGP updates and check for misconfiguration.

VI. Conclusions

In this paper, we have introduced a blockchain-based solution to prevent route leaks. Our solution uses a formal language to unambiguously define the routing policy, store and communicate it securely using the chain and automatically configuring the appropriate BGP route filters.

Although not specifically discussed in the paper, the proposed architecture is flexible enough to enforce arbitrary routing policy and not just route leaks. Indeed, both the formal language and the resulting BGP route filters are expressive enough to define and enforce arbitrary routing policies. This gives network administrators a fundamental tool to operate BGP formally and securely, within the scope of the business relationship of the ASes.

References

[1] R. Chandra, P. Traina, and T. Li. B, “BGP Communities Attribute” IETF RFC 1997, 1996.

[2] Aftab Siddiqui, ”Route Leak Causes Major Google Outage”, https://www.internetsociety.org/blog/2018/11/route-leak-caused-a-major-google-outage/

[3] M. Lepinski, S. Kent ”An Infrastructure to Support Secure Internet Routing”, Internet Engineering Task Force (IETF), 2012

[4] M. Lepinski, Ed., K. Sriram, Ed. ”BGPsec Protocol Specification”, Internet Engineering Task Force (IETF), 2017

[5] Geoff Huston, An Update on Securing BGP, https://labs.ripe.net/Members/gih/an-update-on-securing-bgp

[6] Zhao, Meiyuan, Sean W. Smith, and David M. Nicol. ”Aggregated path authentication for efficient BGP security.” ACM, 2005.

[7] Lychev, Robert, et al. ”BGP security in partial deployment: Is the juice worth the squeeze?.” ACM SIGCOMM Vol. 43. No. 4. ACM, 2013.

[8] Butler, Kevin, et al. ”A survey of BGP security issues and solutions.” Proceedings of the IEEE 98.1 (2009): 100-122.

[9] Zhao, Meiyuan, , et al. ”The performance impact of BGP security.” IEEE network 19.6 (2005): 42-48.

[10] Sriram, et al. ”Problem Definition and Classification of BGP Route Leaks”, IETF RFC 2016, 2016.

[11] BGP Leak Highlights the Fragility of the Internet with Real Consequences, https://blog.catchpoint.com/2019/06/26/ bgp-leak-internet-fragility/

[12] Siddiqui, Muhammad Shuaib, et al. ”Route leak identification: A step toward making Inter-Domain routing more reliable.” 2014 DRCN. IEEE, 2014.

[13] Streibelt, Florian, et al. ”BGP Communities: Even more Worms in the Routing Can.” Proceedings of the Internet Measurement Conference 2018. ACM, 2018.

[14] Donnet, B., & Bonaventure, O. (2008). On BGP communities. ACM SIGCOMM Computer Communication Review, 38(2), 55-59.

[15] BGP Community Guides, https://onestep.net/communities/

[16] SecuringBGP, https://github.com/MiquelFerriol/SecuringBGP

[17] BGP Community Dictionary Dataset, https://www.caida.org/data/bgp-communities/

[18] Donnet, Benoit, , et al. ”On BGP communities.” ACM SIGCOMM Computer Communication Review 38.2 (2008): 55-59.

[19] Quoitin, Bruno, et al. A survey of the utilization of the BGP community attribute. No. UCL-Université Catholique de Louvain. 2002.

[20] I. Shrubbery Networks. (2004). RANCID—Really Awesome New Cisco Config Differ. http://www.shrubbery.net/rancid/

[21] A. Lutu, M. Bagnulo, and O. Maennel, “The BGP visibility scan-ner,” INFOCOM WKSHPS, pp. 115–120.

[22] Urbina Cazenave, et al. ”An anomaly detection framework for BGP.” 2011 INISTA. IEEE, 2011.

[23] Ćosović, Marijana, et al. ”Classifying anomalous events in BGP datasets.” CCECE. IEEE, 2016.

[24] Jin, Jian. ”BGP Route Leak Prevention Based on BGPsec.” 2018 VTC-Fall. IEEE, 2018.

[25] D. Gupta, A. Segal, et al. ”A new approach to interdomain routing based on secure multi-party computation”, HotNets, 2012, pp. 37–42.

[26] A. Hari, T.V. Lakshman, The internet blockchain: a distributed, tamper-resistant transaction framework for the internet, HotNets, 2016, pp. 204–210.