Enhancing the Trust of Internet Routing with Lightweight Route Attestation

Qi Li, *Student Member, IEEE,* Mingwei Xu, *Member, IEEE,* Jianping Wu, *Fellow, IEEE,* Xinwen Zhang, *Member, IEEE,* Patrick P. C. Lee, *Member, IEEE* and Ke Xu, *Member, IEEE*

***Abstract*—The weak trust model in Border Gateway Protocol (BGP) introduces severe vulnerabilities for Internet routing including active malicious attacks and unintended misconfigurations. Although various secure BGP solutions have been proposed, the complexity of security enforcement and data-plane attacks still remain open problems.**

We propose TBGP, a trusted BGP scheme aiming to achieve high authenticity of Internet routing with a simple and lightweight attestation mechanism. TBGP introduces a set of route update and withdrawal rules that, if correctly enforced by each router, can guarantee the authenticity and integrity of route information that is announced to other routers in the Internet. To verify this enforcement, an attestation service running on each router provides interfaces for a neighboring router to challenge the integrity of its routing stack, enforced rules, and the attestation service itself. If this attestation succeeds, the neighboring router updates its routing table or announces the route to its neighbors, following the same rules. Thus, a router on a routing path only needs to verify one neighbor's routing status to ensure that the route information is valid. Through this, TBGP builds a transitive trust relationship among all routers on a routing path.

We implement a prototype of TBGP to investigate its practicality. In our implementation, we use identity-based signature (IBS) and trusted computing (TC) techniques to further reduce the complexity of security operations. Our security analysis and performance study shows that TBGP can achieve the security goals of BGP with significantly better convergence performance and lower computation overhead than existing secure BGP solutions.

***Index Terms*—Routing, BGP, Hijacking, Secure BGP, Prevention**

I. Introduction

The Border Gateway Protocol (BGP) is the only widely deployed inter-domain routing protocol connecting different IP networks or autonomous systems (ASes) to construct the whole Internet [1]. In ordinary BGP, every AS announces its route information with different prefixes. However, its neighboring ASes cannot validate this route information, but rather directly propagate it across the Internet. Obviously, this weak trust model allows forged route announcement propagations, which is a fundamental security weakness of BGP. Forged routes, which can be generated by configuration errors or malicious attacks, can cause large-scale network connectivity problems. For instance, on Feb. 24th, 2008, Pakistan Telecom (AS17557) started an unauthorized announcement of the prefix 208.65.153.0/24. One of Pakistan Telecom's upstream providers, PCCW Global (AS3491) forwarded this announcement to the rest of the Internet, resulting in the hijacking of YouTube traffic on a global scale [2]. The situation could be worse if forged routes are generated by remote attacks [3].

In order to effectively eliminate false announcements and improve the security of BGP, several security-enhanced BGP solutions have been proposed. They generally can be classified into two categories: *cryptography-based prevention* [4], [5], [6], [7], [8], and *anomaly detection* [9], [10], [11]. Cryptographic approaches, such as SBGP [4] and SoBGP [5], use a centralized routing registration authority and public key infrastructure (PKI) to ensure the authentication of routing announcements. These solutions are not sufficient to prevent data-plane attacks, where an AS can announce a route not adopted by itself [12]. Moreover, they usually consume a significant amount of extra router resources including computation and storage, and exacerbate the routing convergence performance. It is obvious that pure cryptography-based solutions are not cost-efficient to defend against routing attacks, and this impedes their deployment on the Internet. On the other hand, anomaly detection approaches aim to discover underlying hijacks in BGP announcements, e.g., by comparing BGP announcements with out-of-band information and querying third-party routing services [10]. However, most of the anomaly detection solutions raise false positives and require network operators to take actions in order to block detected anomalous routes [9], [10], [11].

In this paper, we propose a trusted BGP scheme called TBGP, which aims to *use minimal computation cost to achieve BGP security goals.* Unlike existing cryptography-based approaches, we do not solely rely on cryptography mechanisms to secure routing. Instead, we propose a set of well-defined route update and withdrawal rules that are enforced by the filters of each BGP router along a routing path. These rules guarantee that route announcements comply with the BGP specification [1]. Thus, the enforcement of these rules provides automatic route authenticity in each router and prevents the spread of forged routes over the Internet. In order to ensure that these rules are not misconfigured or maliciously modified, and hence correctly enforced on each router, TBGP introduces an attestation service running on each router. With this service interface, a neighbor router can challenge this router's current

Q. Li, M. Xu, J. Wu and K. Xu are with the Department of Computer Science, Tsinghua University, Beijing, China e-mail: {liqi,xmw,jianping,xuke}@csnet1.cs.tsinghua.edu.cn.

X. Zhang is with Huawei America Research Center, Santa Clara, CA USA. e-mail: xinwen.zhang@huawei.com.

P. Lee is with the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong e-mail: pclee@cse.cuhk.edu.hk.

running state, including the integrity of its routing protocol stack, the routing rules, and the attestation service itself. When this attestation verification succeeds, the attesting router has the assurance that the route information it receives from this router is legitimate and follows the routing specification. Thus, the router can use the route information to update its own routing table, or announce it to its neighbors based on the same set of rules. In turn, its routing state and enforced rules can be challenged by other router. Thus, a *transitive trust relationship* can be built by attesting and verifying only one neighboring router along a routing path. TBGP exploits the transitive trusts among routers to extensively save computation and network resources compared to traditional secure BGP approaches.

The above attestation does not prevent a malicious router from claiming to own a particular AS number and generating forge routes. In order to verify the owner of an AS number and the authorization of using it, each route update is digitally signed by the attestation service upon the successful attestation challenge. A router is authorized to use its own private key to sign any valid announcement only when routes are successfully attested in OUT filters. The signature is then verified by its neighbors via their own attestation service. As the private key is bound with the AS number owned by the router, the attestation process can guarantee the authenticity of announced routes of a benign router.

We implement a prototype to demonstrate the practicality of TBGP, and use commodity techniques to further improve its performance. First, with the advent of Trusted Computing (TC) technologies, we note that TC-enabled chips are equipped in almost all commodity PCs and are ready for embedded systems [13], [14], [15]. Thus, we use this facility to securely store the private keys in each router, and bind the integrity of router software and the correct enforcement of BGP rules with authorized signing operations using the protected keys. Furthermore, we accomplish the verification of prefix originals and AS_PATH with the identity-based signature (IBS) scheme [16], [8], which eliminates the centralized certificate management infrastructure and the aggregated signatures as in traditional RSA- and DSA-based algorithms. This significantly reduces the overhead of runtime security operations.

The security analysis shows that TBGP achieves the security requirements of BGP, including AS number authentication, BGP speaker (router) authentication, AS path authentication, and prefix origin authentication. It also effectively prevents data-plane attacks such as traffic attraction attacks [12] by guaranteeing normal BGP execution routines and enforcing route attestation rules in each BGP speaker. We evaluate the performance of TBGP with both experimental studies and simulations. The experimental studies show that TBGP only introduces by an average of 2-ms delay in route selection and announcement of every route (per-prefix). We then seed the experimental data as the parameters into large scale simulations. Our simulation results show that TBGP has significantly lower performance overhead and resource consumption than existing secure BGP approaches. When compared to prior secure BGP solutions, TBGP has an improvement of at least 1.25 times in convergence time and 9.26 times in memory consumption. This evidently shows that TBGP could be a potential solution for building a trustworthy Internet routing infrastructure.

The remainder of the paper is organized as follows. In Section II, we introduce the problem statement of BGP security and existing solutions, and the design goals of TBGP. In Section III, we propose the BGP route rules to build trust between different ASes. The implementation details of our prototype are illustrated in Section IV. Section V presents performance evaluation results. We discuss some issues of TBGP deployment in Section VI. Section VII concludes this paper.

II. Background and Design Goals

A. BGP Security Threats

Current BGP is always under attacks from maliciously misconfigured speakers or intercepted unauthorized BGP sessions, both of which can cause BGP routing anomaly and further Internet disruption. Since BGP speakers fail to verify the origins of BGP announcements, a BGP speaker can announce any prefix that does not belong to its AS. Similarly, a BGP speaker cannot validate the AS path of a received BGP announcement. Thus, the announced route may be invalid and redirect traffic to wrong/malicious destinations. In general, there are two types of attacks in BGP: *prefix hijacks* and *invalid path attacks* [17].

Prefix hijacks include the *complete prefix* and *sub-prefix* hijacks. It is easy to carry out complete prefix hijacks on the Internet, but it is relatively hard to detect them. For example, a complete prefix hijack can occur when an AS announces itself as the origin of a prefix that it does not own, and its neighboring ASes then reroute any traffic with corresponding destination to the hijacker. The attack (1) shown in Figure 1 is a complete prefix hijack, in which a malicious speaker in AS 6 announces that AS 6 is the owner of the prefix 12.34.8.0/24 and advertises AS path $\{6\}$ to AS 4. The sub-prefix hijack is similar to the complete prefix hijack except that its announced prefix is a subset of another announced prefix.

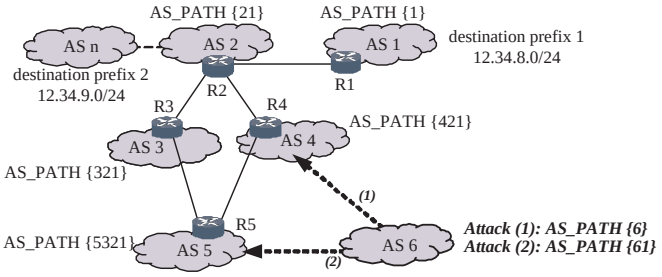

Fig. 1. Examples of normal route and malicious route announcements of BGP. (1) indicates a complete prefix attack, and (2) an invalid path attack.

An invalid path attack occurs when the AS path of a BGP announcement includes fake AS numbers. For instance, the attack (2) illustrated in Figure 1 is an invalid path attack, where AS 6 advertises a forged AS path $\{61\}$ to AS 5 and any traffic to AS 1 is redirected to AS 6 if AS 5 adopts this route. Because BGP is a policy vector routing protocol, it cannot detect relationships between ASes. Therefore, it is also very hard to detect invalid path attacks.

B. Related Work

Several security-enhanced BGP solutions have been proposed in literature, and they can be classified into two types in general. The first type uses cryptographic algorithms to provide the authentication of ASes and AS_PATHs (i.e., sequences of ASes that represent routes), such as SBGP [4], SoBGP [5], psBGP [6] and SPV [8]. The second type is to deploy invalid route detection mechanisms, such as IRV [10], Listen and Whisper [9], PGBGP [11], iSPY [18] and NetReview [19].

SBGP is the first proposed secure BGP solution [4], which uses public key infrastructure (PKI) to issue AS and prefix certificates for verification of announced prefixes and AS paths. In SBGP, aggregated signatures are used to guarantee the authenticity and integrity of BGP announcements. For a specific route, different signatures of prefix and AS_PATH are attached in announcements by traversed ASes. To improve the performance of SBGP, S-A and SAS apply cryptographic operation speedup and sequential aggregate signature, respectively [20]. SPV adopts a more efficient cryptographic mechanism [8]. However, these solutions have the drawback of large computation and memory costs. To address these issues, Secure origin BGP (SoBGP) uses a distributed trust model [5], in which a new BGP message is introduced to deliver certificates. Unfortunately, SoBGP cannot prevent invalid AS path attacks. Pretty secure BGP (psBGP) uses a signed prefix assertion list (PAL) that consists of a number of bindings of AS numbers and (zero or more) IP prefixes [6]. Similar to SBGP and SoBGP, it is difficult to apply psBGP in real application scenarios where customer ASes may obtain IP addresses from different ISPs in a hierarchical way.

Towards trusted route update in individual router platform, BIND [21] uses Trusted Computing (TC) mechanism to run routing process in an isolated memory space and sign and verify the integrity of AS_PATH. Similar to TBGP, BIND aims to achieve a transitive trust between routers so as to reduce integrity verification complexity. However, the transitive trust of BIND and TBGP are achieved with different mechanisms. BIND focuses on attesting the AS_PATH of a neighbor router, and uses a shared-key protected MAC value of the result of a routing update. On the other hand, TBGP achieves transitive trust with attesting valid security rules enforcement of routing updates. Thus, TBGP and BIND complement each other. The path authentication proposed by Butler *et al.* [22] leverages a cryptographic proof system to reduce signature validations by carrying proofs in routing updates based on reference locality of BGP announcements, which introduces more communication overheads than SBGP.

In summary, these solutions usually need to consume large computation resources and cannot meet the practical requirements of real scenarios. Moreover, they usually cannot prevent data-plane attacks [12], because they cannot detect the inconsistency between BGP's control-plane (calculated routes) and data-plane (routes to forward packets).

Inter-domain route validation (IRV) [10] introduces an additional route validation service in BGP, through which the authenticity of BGP route information is verified. However, IRV cannot detect forged AS attacks. The Listen and Whisper solution [9] monitors all exchanged route announcements to detect underlying anomalies but offers weaker detection capability [20]. Moreover, Pretty Good BGP (PGBGP) [11] blocks large-scale attacks by delaying the propagation of suspicious routes. Recently, several improved prefix hijack detection approaches have been proposed. Lad *et al.* [23] propose an alert system to detect prefix hijacks by detecting the changes of prefix origins. Hu *et al.* [24] improve the detection accuracy by analyzing conflicts in data-plane footprints. Zhang *et al.* [18] propose iSPY to detect hijacks by analyzing prefix reachability in prefix owner networks. N-BGP [25] is proposed to build a trusted third party to realize a policy monitor using trusted computing (TC). N-BGP enforces route attestation rules for routing anomaly detection with a BGP monitor, but not in individual BGP speakers. These solutions can be easily deployed on the Internet without modifications to BGP and provide incremental approaches to secure BGP and are orthogonal to cryptography based secure BGP solutions.

Recently, Haeberlen *et al.* [19] propose NetReview to detect routing anomaly caused by attacks and misconfiguration using fault patterns and checking tamper-evident logs with these patterns in NetReview servers of ASes. In NetReview, routing messages are recorded in a tamper-evident log to analyze anomalous behaviors of BGP routes based on defined fault patterns. In this way, NetReview can detect invalid routes caused by attacks or configuration faults and policy conflicts. However, NetReview does not address the response mechanism to detected faults. Different from NetReview, which detects BGP faults based on fault patterns, TBGP enforces route attestation rules to guarantee normal behaviors of BGP routes. TBGP focuses on the prevention of forged routes caused by unintended or malicious misconfiguration, but does not address detection/prevention of policy conflicts, which we believe can be improved by configuration static analysis [26].

C. Design Goals of TBGP

From a security perspective, TBGP seeks to defend against different kinds of BGP attacks and guarantee the availability of BGP routes and normal packet forwarding in the presence of adversaries. We identify the following security goals [6] [1].

- *AS Number Authentication.* BGP speakers can verify whether an AS is the real owner of an AS number and is authorized to use the AS number.
- *BGP Speaker Authentication.* BGP speakers can verify whether a speaker is legal to announce prefixes, so as to guarantee that the BGP speaker is associated with an AS number.
- *AS Path Verification.* BGP speakers can verify whether the AS_PATH $\{AS_1, AS_2, \cdots, AS_n\}$ of a BGP route m for a prefix f_i is in the specified order. That is, m is generated from the prefix owner of AS_1, and has traversed $AS_2, \cdots, AS_n$.

[1] Since the consistency between control- and data-plane is a basic BGP property according to the BGP specification [1], we do not explicitly specify it here.

- *Prefix Origin Authentication.* BGP speakers can verify whether an AS_n is authorized to generate an IP prefix f_i. In order to achieve that, one of the following three conditions should be verified: (1) The prefix f_i is indeed held by AS_n; or (2) AS_n is authorized to be the owner of f_i; or (3) AS_n is assigned by a set of prefixes F_i and has received another set of prefix F_j, such that f_j is aggregated from F_i, F_j, or both, and $\exists f_j \subseteq f_i$, where $f_j \subseteq F_i \cup F_j$.

Furthermore, in order for a secure BGP solution to be practically deployable on the Internet, the following goals should be satisfied.

- *Acceptable Performance.* A secure BGP solution should introduce minimal performance overhead (e.g., CPU cycles, memory footprint, and communication cost) over ordinary BGP, and does not significantly degrade the performance of a BGP speaker and the convergence performance of BGP.
- *Incremental Deployment.* A secure BGP solution should be partially deployable without disruption, which means that a subset of entities (e.g., routers, ASes, or ISPs) can deploy the solution without incurring loss of network connectivity.

III. Design of TBGP

For clarity, we initially assume that TBGP is fully deployed (i.e., on all participating routers in the network), and the allocation of AS numbers and IP prefixes to ASes is certified by authorities. We then relax this assumption for efficient cryptographic operations and incremental deployment.

A. Overview

Ordinary BGP provides configurable filters called *IN filters* and *OUT filters*, which filter incoming and outgoing routes, respectively. With the filters, operators can configure their routers to discard routes that violate certain conditions. Filters are used by providers to ensure that they only accept or announce routes from/to their neighbors. If all providers perform this correctly, the network would be safe from attacks. However, many networks cannot filter violated routes effectively, due to the difficulty to infer the validity of routes from different ISPs. Basically, TBGP is designed to attest routes to check whether they comply with the BGP specification in filters and provide an automatic route filtering mechanism.

In TBGP, a BGP speaker signs a route if it complies with a set of route attestation rules in the OUT filters. By verifying the signatures in the IN filter, a neighboring router can easily know whether the route is valid in terms of BGP specification. With this mechanism, a *transitive trust relationship* can be built among the routers along a routing path. The root of this trust relies on the prefix owners that sign the route with prefix private keys. Each BGP speaker verifies, in its IN filter, the signature piggybacked in a received route update from its neighbor. A successful verification means that the route is attested by the neighbor and is authentic, and the route in Adj-RIB-IN is updated. The BGP speaker selects the best route for the prefix. If the best route is changed, the BGP speaker announces the selected routes to its neighbors. Before that, the BGP speaker attests the route under propagation according to route attestation rules. A route is signed by the private key of the AS number only if it has been successfully attested, and thus neighbor routers can easily check whether the route is trusted and authenticated by verifying the signature.

To illustrate the idea of TBGP, we refer again to Figure 1. Suppose AS 1 announces that it is the owner of prefix 12.34.8.0/24. Then R1 is authorized to announce the AS PATH $\{1\}$ signed with its private key. R2 in AS 2 receives the route update and updates it in Adj-RIB-IN for route selection only if it successfully verifies the signature in the IN filter. If the route is selected as the best route to the destination 12.34.8.0/24 in R2, then R2 checks whether the route under propagation complies with the attestation rule. The route is authenticated only if the route is successfully attested. In this example, the AS_PATH of route under propagation is $\{21\}$, which prolongs the AS_PATH in the previously received route update. Then, AS 1 and AS 2 build trust between themselves. R2signs the AS PATH using its private key that correspond to the AS number. Similarly, R3, R4, and R5 verify the route in their IN filters and announce the route to their ASes with the correct signature. Thus, AS 1, AS 2, AS 3, AS 4, and AS 5 build a trust relationship for prefix 12.34.8.0/24.

Now, the routers in AS 6 cannot launch the prefix hijack attack (see Section II) by announcing the ownership of the prefix 12.34.8.0/24 because they do not have the correct private keys to sign the routes for the prefix. Similarly, it cannot launch the invalid path attack (see Section II) by propagating the forged route $\{61\}$ because the route cannot be successfully attested by AS 5 (assuming that no router is compromised). In Section IV, we will discuss how to prevent forged routes if some routers are compromised.

Thus, TBGP well considers different route attestation requirements for different types of BGP sessions and effectively eliminates aggregate signatures of a full AS path in route attestations as in existing cryptography-based secure BGP solutions. The next two subsections explain more details of the route attestation rules and establishing transitive trust relationships between different ASes/routers.

B. Route Attestation Rules for TBGP

The trust of a BGP system depends on the expected behavior of each router when selecting and announcing route information. A set of route attestation rules is defined in TBGP, which, if correctly enforced by a router system, can guarantee the authenticity and correctness of its announced information.

First, let us consider the basic attestation rules for BGP sessions among different ASes in TBGP, where we assume an AS only has one BGP speaker. The OUT filter of a BGP speaker checks whether an announced route follows the route attestation rules based on the information in the IN filter. The announcement is signed and further propagated only when it passes the check. A neighboring BGP speaker, upon receiving the announcement, first verifies if it is actually sent by a speaker that owns the AS number. If attestation verification succeeds, then it means the route is trusted, and

the announcement is accepted. Thus, these two BGP speakers can build a trust relationship. This is done recursively along an AS_PATH. Thus, *there is no need for a BGP speaker to check and verify every hop in the AS_PATH*, i.e., prefix verification and AS_PATH verification for all speakers in the path. A neighboring BGP speaker only needs to verify limited information, such as the signature of prefixes or AS but not both. These attestation operations are enforced by a BGP attestation service (see Section IV). Through the built trust relationship, aggregated signatures are eliminated. Before we introduce the detailed rules, Table I gives the symbols used in these rules.

TABLE I
SYMBOLS USED IN ROUTE ATTESTATION RULES

f_i, AS_n	IP prefixes, AS number
$AS[f_i]$, $AS(f_i)$	A set of AS_PATH for prefix f_i, a specific AS_PATH
$\Downarrow AS[f_i]$	AS_PATH in a received update for f_i
$\Uparrow AS[f_i]$	AS_PATH in the update for f_i under propagation
$Withdraw(f_i)$	A received withdrawal to prefix f_i
$PreList(AS_n)$	Prefix list owned or received by AS_n

Definition 1: BGP Route Announcement Rule: A BGP speaker is authorized to send a valid BGP announcement, $Update(f_i, AS(f_i))$, if and only if one of the following three conditions is true:

- $f_i \subseteq PreList(AS_n) \wedge (\Downarrow AS[f_i] == \emptyset) \wedge (\Uparrow AS[f_i] == \{AS_n\})$;
- $((\{AS_n\}^+ \cup \Downarrow AS[f_i]) == \Uparrow AS[f_i]) \vee (\Uparrow AS[f_j] \subseteq (\{AS_n\}^+ \cup \Downarrow AS[f_i]) \wedge f_i \subseteq f_j)$;
- $(Withdraw(f_i) \vee AS_n \in AS[f_i]) \wedge ((\{AS_n\}^+ \cup AS(f_i)) == \Uparrow AS[f_i])$.

This rule illustrates that an announcement is valid if and only if (i) f_i is the owner of AS_n, (ii) or it is a re-announcement after a previous announcement, or (iii) it is an announcement after a previous announcement that does not include valid routes. We note that since a route update triggered by ISP policy changes is similar to that specified by the third condition of this rule, we do not discuss it explicitly. Note that this security rule considers the address aggregation and legal AS prepending issues during route propagation. $\{AS_n\}^+$ in this rule denotes that it is legal to prepend its own AS number in an AS path.

The first condition in this rule describes that the advertisement speaker in AS_n is authorized to announce the prefix if it is the owner of the prefix, and the announced route should only contain itself in the AS Path. For example, AS 1 in Figure 1 is allowed to advertise AS path $\{1\}$ to its neighbors. The second condition describes that the BGP speaker is allowed to advertise a route if it is a re-advertisement of a previous route and prolongs the AS path with its AS number, or the AS path in the re-advertisement route is a subset of the full AS path which is prolonged by including its AS number[2]. For instance, in Figure 1, AS 2 advertises the AS path $\{21\}$, which is legal if the AS path in the previously received route update from AS 1 is $\{1\}$. Suppose that AS 3 receives the AS path $\{21\}$ for the destination 12.34.8.0/24 and receives the AS path $\{2n\}$ (for some AS number n) for prefix 12.34.9.0/24 in the route from AS 2. The announced route whose AS path is $\{21\}$ for prefix 12.34.0.0/20 is allowed because it is the intersection of these two prefixes, and thus it is a legal route aggregation based on the second condition.

The third condition describes the situation that the announced route is legal if the route under propagation is the union of a record in previous received route updates and its own AS number after receiving a route withdrawal. For example, assuming that the link between AS 2 and AS 3 in Figure 1 fails, AS 3 then withdraws the route to AS 5. Since AS 5 has received a route update with AS_PATH $\{421\}$, which is recorded in the attestation service, the route attestation rule allows AS 5 to advertise the route with AS_PATH $\{5421\}$ to its neighbor ASes. If AS 5 advertises a route whose AS path is not recorded, then the route under propagation is regarded as a forged one and dropped. In addition, if a BGP speaker receives a route containing its own AS number, e.g., the route oscillation cases discussed in [27], then it announces another recorded route, which is similar to the route withdrawal case above.

Definition 2: BGP Route Withdrawal Rule: A BGP speaker is authorized to send a valid BGP withdrawal, $Withdraw(f_i)$, if and only if the following condition is true:

- $(Withdraw(f_i) \wedge AS[f_i] == \emptyset) \vee f_i \in PreList(AS_n)$.

Similarly, this rule describes that a route withdrawal is allowed if and only if AS_n is the owner of f_i or there is no available route record for prefix f_i in the attestation service. For example, assuming that the link between AS 1 and AS 2 fails in Figure 1, AS 2 does not have an available route to AS 1. Then, the BGP speaker in AS 2 is allowed to send route withdrawals to AS 3 and AS 4.

C. Trust Establishment

The above route attestation rules guarantee the validation of BGP announcements if they are really enforced on each router. We can use these rules to verify this via attestation service in the IN and OUT filters of a BGP speaker. As aforementioned, when a BGP speaker in AS 1 receives an announcement, it is firstly checked and verified by the attestation service in the IN filter. If the received announcement is sent by the owner of a prefix, the prefix string is used to verify the signature. As shown in Figure 2, through verification, the identity of the originating BGP speaker in AS 1 and the ownership of the prefix are validated in AS 2. This is the first level of a trust relationship for prefix 12.34.8.0/24. If the announcement is propagated to AS 3 by a delegated BGP speaker in AS 2, then we need to verify whether the speaker of AS 2 is authorized to propagate this route. Thus, the AS number of AS 2 is used to verify whether the BGP speaker is an authentic owner of AS 2. If the announcement is verified in the IN filter of AS 3, then AS 3 can trust the announcement because the successful verification means that the received AS_PATH is composed with previous consecutive trusted ASes. Thus, the received route should be updated as an active record and stored in the route database for further attestation by the OUT filter. Similarly, AS 4 can build trust with AS 2 by verifying the announcement.

[2]Actually, route disaggregation is similar to the route aggregation. In general, AS should achieve another type of secret keys different from the prefix owner keys if it announces itself as the origin of the aggregated/disaggregated prefix. However, this process is application-specific, and we do not discuss it in this paper.

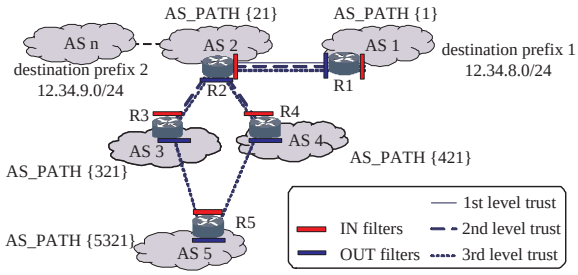

Fig. 2. Building transitive trust between ASes/routers.

After a BGP speaker completes a route selection process, the chosen route is further propagated if there is a change in the route. The route announcement is then checked in the OUT filter. First, the active record *R* of the route record updated in the IN filter, which triggers the route re-computation, is located. If the record does not exist or does not match a received route, which means that the route is sent by the owner or the route update follows a received route not including a valid AS path, then all the records of the prefix are fetched from the route database. Then the attestation service checks whether the announcement is allowed based on the route attestation rules. If the announcement is legal, then it is signed and sent to the neighboring speaker. The signature is either based on the private key of f_i (i.e., $sQ_{ID_{f_i}}$) if the AS is the owner of f_i, or based on the private key of AS_n (i.e., $sQ_{ID_{AS_n}}$) otherwise. As Figure 2 shows, after AS 3 and AS 4 successfully attest the route in OUT filters, the trust relationship is extended to AS 5 if it adopts the route.

With these two attestation procedures in IN and OUT filters, the validity of BGP announcements is guaranteed by enforcing verifications and route attestations in the IN/OUT filters of BGP speakers. That is, the identity of a BGP speaker is verified and its route authenticity is guaranteed by the route attestation rules, through which different speakers build a transitive trust relationship. Specifically, when a BGP speaker in AS_y receives a route update of a prefix with the correct signature from a speaker in AS_x (i.e., the route update is attested by AS_x itself), it attests the route update by verifying the signature and puts this route in Adj-RIB-IN for future route selection. Thus, AS_x and AS_y build trust between them for this prefix. Similarly, if the route for this prefix is adopted and further propagated to AS_y's neighbors $\{AS_k,...AS_n\}$, the update is attested in the OUT filter of AS_y speaker and then is signed by its private key. Thus, all ASes can build trust with each other, and the trust relationship is transitive by signing/verifying signatures and enforcing the rules in the IN and OUT filters. For example, as shown in Figure 2, the second level of the trust relationship among ASes 1, 2 and 3 is built if AS 1 attests the route in the OUT filter and ASes 2 and 3 successfully verify the route in their IN filter. Similarly, the third level trust relationship is built among ASes 1, 2, 3, 4 and 5 if AS 3 and 4 attest the route in their OUT filters and AS 5 verify it in its IN filter. Any forged routes cannot be successfully attested by the attestation service. That is, an AS can trust routes from neighbor ASes if and only if the routes are verified, which means that the routes are strictly attested by neighbor ASes themselves. Therefore, TBGP can effectively defend against forged BGP routes no matter whether they are generated by configuration errors or malicious attacks. Each AS only needs to attest route updates with the keys of the last hop and does not need to attest them with the information of every hop. Thus, we can achieve the following theorem.

Theorem 1: In TBGP, to verify a received route update $[AS_1, AS_2, AS_3, ..., AS_n]$ for prefix f_i, a speaker only needs to verify the signature of the route update with the key of last hop AS_n.

Proof: We prove the theorem based on the following three cases.

Case 1: n=0. It means that the prefix is owned by AS_1. The permission for TBGP speakers in AS_1 to announce or withdraw prefix f_i is obtained by checking the prefix keys in AS_1, i.e., $f_i \in PreList(AS_1)$. TBGP speakers owning the private keys can successfully sign the route update.

Case 2: n=1. The ownership of prefix f_i is verified in AS_2 by verifying the signature of AS_PATH $[AS_1]$ with the key of prefix f_i if the route update is an announcement, or verifying the signature of the prefix f_i if the update is a withdrawal. If AS_2 receives the announcement, it is only allowed to re-announce the route and prolongs the AS path with its own AS number, i.e., $((\{AS_2\}^+ \cup \Downarrow AS[f_i]) == \Uparrow AS[f_i])$, or re-announce the aggregated route, i.e., $(\Uparrow AS[f_j] \subseteq (\{AS_2\}^+ \cup \Downarrow AS[f_i]) \wedge f_i \subseteq f_j)$ (see Definitions 1 and 2). Similarly, if AS_2 receives a withdrawal, it is only allowed to announce the route if $(Withdraw(f_i) \vee AS_2 \in AS[f_i])$ or withdraw the prefix if $(Withdraw(f_i) \wedge AS[f_i] == \emptyset)$. The BGP speakers in AS_2 can successfully obtain private keys to sign the route update if and only if it has one of the operations above.

Case 3: $n \geq 2$. AS_n trusts the route from its previous AS AS_{n-1} if and only if the route update is verified, i.e., AS_n successfully verifies route update $[AS_1, AS_2, AS_3, ..., AS_{n-1}]$ from AS_{n-1}, which means that the route update is strictly attested by AS_{n-2} and is re-announced by AS_{n-1}. If AS_n receives the announcement, it is only allowed to re-announce the route and prolongs the AS path with its own AS number, i.e., $((\{AS_n\}^+ \cup \Downarrow AS[f_i]) == \Uparrow AS[f_i])$, or re-announce the aggregated route, i.e., $(\Uparrow AS[f_j] \subseteq (\{AS_n\}^+ \cup \Downarrow AS[f_i]) \wedge f_i \subseteq f_j)$. If AS_n receives a withdrawal, it is only allowed to announce the route if $(Withdraw(f_i) \vee AS_n \in AS[f_i])$ or withdraw the prefix if $(Withdraw(f_i) \wedge AS[f_i] == \emptyset)$. Thus, AS_n has the permission to sign the route update to announce it to its neighbors.

By combining the above three cases, TBGP only needs to verify the signature of route update with the key of last hop AS_n to verify received route update $[AS_1, AS_2, AS_3, ..., AS_n]$ for prefix f_i. □

According to Theorem 1 and Definitions 1 and 2, we have the following theorem.

Theorem 2: Each TBGP speaker verifies a received route update $[AS_1, AS_2, AS_3, ..., AS_{n-1}]$ for prefix f_i by verifying that it is originally announced by AS_1 and re-announced exactly through the path $\{AS_2, AS_3, ..., AS_{n-1}\}$.

Theorem 2 states that TBGP achieves the following four security goals: AS number authentication, BGP speaker authentication, AS path authentication, and prefix origin authen-

tication.

D. Extending TBGP for iBGP and Incremental Deployment

In general, each AS can have more than one BGP speaker, and different BGP speakers connect each other by iBGP sessions to announce their learned eBGP routes. It is obvious that the basic route attestation rules we discussed above cannot directly apply to the Internet because the AS_PATH of routes is not changed in iBGP sessions. We solve the problem by adopting the rules as follows.

- If a route is announced to an iBGP neighbor, then the router does not need to attest[3] it in the OUT filters but simply forward, because all attributes of the route are not changed;
- If a route is announced from an iBGP neighbor and the next hop address encoded in the announcement is loopback, then it means that the route is generated within its own AS, and the router does not need to attest it in the IN filters but simply accept it;
- If a route is announced from an eBGP neighbors or it is from an iBGP neighbor but the next hop address encoded in the announcement is not loopback, then the router needs to attest it in the IN filters;
- If a route is announced to an eBGP neighbor, then the router needs to attest it in the OUT filters.

Let us follow an example in Figure 3 which is extended from that in Figure 1 and illustrates an example of route attestation with the presence of iBGP and eBGP sessions and is an extension of the example in Figure 1. Assuming that AS 1 announces 12.34.8.0/24, BGP speakers R1, R3, R4, R7, and R8 attest routes in their OUT filters of their eBGP sessions according to the route attestation rules, and R2, R5, R6, and R9 need to attest routes in their IN filters and forward the received route updates in their iBGP sessions if they are adopted as the best routes.

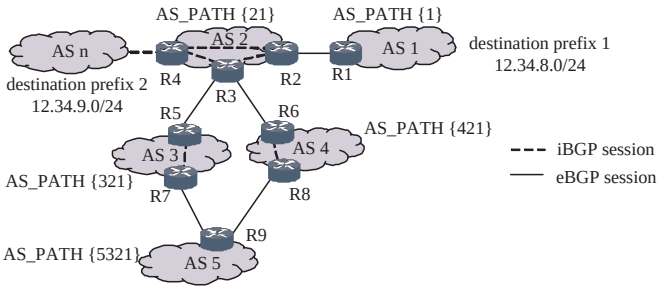

Fig. 3. A route attestation example in the presence of iBGP and eBGP sessions.

Since TBGP eliminates signature aggregate and routers can accept/reject received announcements without signatures signed by neighbors based on their configurations, we can easily enable *incremental deployability* of TBGP. Basically, we need to modify route attestation procedures in the IN and OUT filters. In the IN filter, TBGP should use any AS number in AS_PATH to verify the update if it is not firstly announced and path is not fully trusted. For instance, as shown in Figure 3, we assume that AS 5 receives a route announced by AS 3, (AS 3, AS 2, AS 1) where AS 2 and AS 1 are trusted AS but AS 3 is not trusted for prefix f_1. That is, the route update is not fully trusted, TBGP should indicate the last trusted AS number, i.e., AS 2. Thus, TBGP will directly use the public key of AS 2 to attest if the update is partially trusted instead of using the public key of AS 3. In the OUT filter, if adopted routes are not fully trusted, i.e., routes are received without signatures signed by the last hop of AS_PATH, TBGP will not sign these routes then.

In TBGP, we can filter routes without fully trusted AS paths. However, in practice, network operators are not willing to do so for the network availability issue. Thus, we need to change local preference value (which indicates the degree of preference for learned routes [1]) of each route according to different trust level of AS paths based on network operators' configuration. That is, we can assign a high local preference value to fully trusted AS paths and low local preference value to partial trusted AS paths in the IN filters. Let us follow the example above (shown in Figure 3). If AS 5 receives another route (AS 4, AS 2, AS 1) where ASes 4, 2, 1 are all trusted AS for prefix f_1, TBGP can detect that (AS 4, AS 2, AS 1) is fully trusted AS_PATH but (AS 3, AS 2, AS 1) is not. TBGP enables that BGP speakers in AS 5 set a low preference value for routes without fully trusted AS paths, e.g., setting the local preference value to 0, and then the fully trusted route (AS 4, AS 2, AS 1) is preferred in Adj-RIBs-IN in route selections. If an untrusted route is selected as the best route in trusted ASes, the re-advertisement route is still untrusted though these ASes adopts TBGP. In this way, TBGP can be incrementally deployed.

IV. Prototype Implementation

We implement a prototype of TBGP and demonstrate its practices. Our prototype solves the following two questions which are important for real deployment on the Internet:

1) How to reduce the complexity of cryptographic operations in TBGP? Is it possible to eliminate distribution and management of thousands of public keys in traditional secure BGP proposals?

2) How to realize a tamper-resistant TBGP such that it can guarantee the integrity execution of route attestation algorithms and rules, and thus preserve the consistency of routing control- and data-plane? In other words, can we ensure that a TBGP router cannot pretend to be a trusted one if the system is compromised, e.g., the route attestation service is disabled or routing control- and data-plane are not consistent?

Our TBGP solution is built on two existing key techniques: identity-based signature (IBS) and trusted computing (TC). In this section, we present three primitive functions used in TBGP based on these two techniques: (i) secure storage of BGP keys, (ii) signing/verifying BGP announcements, and (iii) BGP attestation service.

A. Preliminaries

Identity-Based Signature Algorithm Identity-based cryptography (IBC), which is an alternative to the traditional

[3]Here, route attestation means checking if a route complies attestation rules and then signing/verifying the route.

certificate-based public key cryptography, uses user identity information (e.g., email address) as the public key [28]. The private key in an IBC system is generated by a private key generator (PKG) according to the user identity information. IBC is firstly designed by Shamir and resolves the problem of key storage and management in certificate-based cryptographic algorithms. IBC includes identity-based encryption (IBE) and identity-based signature (IBS) algorithms [28]. In our implementation of TBGP, we use IBS to verify and validate announced prefix and AS_PATH, which potentially provides an efficient approach for attesting routing updates [8]. Specifically, an IBS system consists of four basic algorithms: *Setup* algorithm generates a set of public system parameters and private master secret; *Extract* algorithm extracts the private key corresponding to a given public key, which takes the system parameter, the master secret, and the public key (a public ID) as inputs; *Sign* algorithm returns the signature of a given message using the system parameters, a private key, and the message as inputs; *Verify* algorithm uses the system parameters and an ID to check whether a signature is valid, i.e., the message is signed with the corresponding private key and is not altered. With IBS, TBGP routers do not need to obtain different public keys before route attestation in advance. Thus, TBGP eliminates the centralized certificate distribution and storage, and reduces the complexity of security operations.

One of the benefits of using IBS is to reduce the complexity of public key distribution and management for individual routers. However we note that the focus of TBGP implementation is not on the key and certificate management, but on transitive trust relationship between routers for AS originators and AS_PATH verifications. Similar to SPV [8], any other certificate distribution and management mechanisms can satisfy our requirement.

Trusted Computing The Trusted Computing Group (TCG) [29] has defined a set of hardware and software specifications for Trusted Computing (TC) technologies. The root-of-trust of the TCG architecture is the Trusted Platform Module (TPM), a discrete chip which performs certain cryptographic functions and provides secure storage. TPM provides secure storage for high level applications and services, which is leveraged by TBGP to protect IBS private keys and guarantees that a signature can only be generated when a BGP routine is correctly executed and route attestation rules (cf. Section III-B) are enforced without disabled or maliciously modified. Specifically, a router receives a private key from a PKG and seals (encrypts) it with a key protected by its TPM when it joins the Internet. When generating a signature, the TPM unseals (decrypts) this key only when certain configurations of the system can be identified, which are represented by Platform Configuration Registers (PCRs) inside the TPM. Through this mechanism, the private key is always protected, the resulting signature is guaranteed to be signed by the proper private key, and the signature is signed only under known good platform state, e.g., the integrity of the attestation service and rules is maintained.

Remote attestation is another important TC mechanism used by TBGP. When a router initially joins the Internet, in order to get permissions to announce routes, it needs to get its private keys. For this purpose, its platform should be attested by the authorities before the router provides its routing service. The TPM on the router signs the value of system state and sends it to an authority, which verifies if the current platform is in a good state. Upon successful verification, the authority releases corresponding private keys to the router, which in turn seals them with TPM. This guarantees that a private secret is only released to a good router. Once private keys are achieved in a router, TPM protects the keys locally. Combined with the secure storage mechanism above, a protected key is only available for signing when the system is in the same good state as when the key is retrieved and installed. Thus, it lays the foundation for trust establishment between BGP speakers, which is the prerequisite to ensure that route attestation rules are enforced in TBGP. In TBGP, we assume that the policy information (i.e., routing attestation security rules) is certified by some trusted authorities, e.g., IANA. For the router platform and protocol stack, known-good system state can be certified by router vendors. Sharing this information between ASes or ISPs may introduce the privacy issue, which has been discussed extensively in the TC community. Some privacy-preserving attestation mechanisms have been proposed, such as privacy CA and Direct Anonymous Attestation (DAA) [30].

B. Primitive Functions of TBGP

TBGP leverages three core mechanisms to achieve the security goals: secure storage of BGP keys, signing/verifying BGP announcements, and BGP attestation service. These mechanisms jointly provide the functions of route attestation. Before introducing the details, we assume that BGP speakers in TBGP are equipped with TCG-compatible TPM chips for key storage and the attestation of the BGP process and route attestation rules. Several designs of TPM for embedded systems have been proposed [13], [29]. Alternatively, secure software TPM (swTPM) [31], a kernel module in the router OS, can be used if hardware TPM is not available. As we focus on relatively closed router platforms (compared to general-purpose computing systems), we believe a software TPM module is reasonably good enough for attestation in TBGP since TBGP focuses on attesting user-space routing protocol stacks and data and trusts the integrity of underlying OS.

Secure Storage of BGP Keys The secure storage mechanism in TBGP is realized by directly applying the secure storage primitive provided by TPM. In TBGP, all sealed keys can be unsealed from TPM and used by the BGP attestation service only when the BGP system running on a router is not maliciously changed. In general, TPM in a BGP speaker seals private keys sQ_{ID}, which includes $sQ_{ID_{f_i}}$ corresponding to its owned prefixes, and $sQ_{ID_{AS_n}}$ corresponding to AS number AS_n. In TBGP, similar to traditional BGP security solutions [4], [6], [8], we also assume some trusted address assignment authorities, such as ICANN and IANA, and other trusted delegation organizations act as PKGs to generate and distribute private keys and public parameters to routers before they are deployed on the Internet. Note that, for the strong security purpose, address assignment authorities should collab-

orate with router vendors who provide fingerprints of different BGP software with route attestation rules to accurately attest BGP systems before assigning private keys. Once a router obtains its private keys, all keys are sealed into the TPM.

When a BGP router is in a good state, all the keys can be unsealed for later signing operations. The good state means that the values represent the expected software runtime of the router, e.g., identical to the values when the keys are sealed. That is, the BGP system is not compromised and the security configurations of TBGP are not maliciously changed. Thus, we have the assurance that: 1) announced routes to neighbors are identified to be used for forwarding packets, which guarantee the consistency of control and data planes; 2) the route attestation rules of TBGP are well enforced during the runtime of a BGP system and are not changed/disabled by its operators. All these are checked during router bootstrapping (cf. Section IV-B). To preserve a good runtime environment, several runtime protection mechanisms can be used, such as ARM TrustZone, Intel's Trusted Execution Technology and AMD's Pacifica technology [14], which are out of the scope of this paper.

Signing/Verifying BGP Updates In TBGP, all outgoing BGP updates (i.e., the routes that a router propagates to others) need to be signed by the router, and all incoming BGP updates (i.e., the routes that a router receives from others) need to be verified by the router before adopting them. The prefixes and AS_PATH specified by an announcement is signed and verified by each BGP speaker. After obtaining the keys and system parameters of IBS, a BGP speaker A signs an announced route using its keys associated with its owned prefix (if the prefix is owned) or its AS number (if the prefix is not owned), and a neighbor speaker B verifies the received announcement using the corresponding public key of speaker A (e.g., the ID string corresponding to the prefix keys or AS keys in the signing procedure). Speaker B can easily determine which string to use to verify the announcement because the prefix and AS public keys are denoted in the BGP update. For example, if speaker B receives a prefix announcement from speaker A, then it uses the AS number ID of speaker A to verify the signature of the announcement. Thus, the public key distribution and management problem in PKI-based BGP schemes is well eliminated in TBGP. If the signature verification fails, speaker B drops the announcement. As aforementioned, a successful signature verification by speaker B implies that the announcement is signed with speaker A's appropriate private key within a good BGP runtime system, i.e., the route attestation rules are correctly enforced by speaker A. To prevent route replay attacks, speaker A also signs route announcement with a timestamp.

BGP Attestation Service The attestation service in TBGP provides interfaces for verifying and attesting BGP updates by a BGP speaker, and provides the mechanism to verify if route attestation rules are enforced by the speaker. Through this, transitive trust relationships can be built between BGP speakers. Basically, there are three major interfaces for BGP speakers: service initialization, validation in the BGP ingress filter (IN filter), and validation in the BGP egress filter (OUT filter) [17]. We will discuss route attestations with the attestations service in Section III.

The BGP attestation service initialization is invoked by a router system during its bootstrap phase after the integrity of the BGP system, including the BGP software and the route attestation rules, are validated by the trusted components on the platform built upon TPM. This interface requires two parameters: the hash values of BGP routing system and the route attestation rules. Note that different routers from different router vendors have different BGP system releases and thus different hash values. If these two parameters are not tampered, then the routing system can be launched successfully. Otherwise, it is launched without any keys achieved from TPM. After the BGP system is launched successfully, all these parameters are reported into PCRs of its TPM. After this, the BGP system and attestation service can use private keys sealed by the TPM. The procedure is discussed in Section IV-A. If the attestation service is disabled, the BGP system cannot achieve the private keys and thus is unable to sign any route update. We will demonstrate this in Section IV-C.

The IN filter and OUT filter interfaces in TBGP are placed in the same places as those in existing BGP protocol on a router [1]; that is, they are invoked after receiving BGP updates and before sending BGP updates, respectively. When a speaker receives a BGP update, its attestation service verifies and validates the prefix string or AS number in the announcement in the IN filter of BGP protocol. If the verification fails, the announcement is dropped; If the verification succeeds, the attestation service will record the route information for later route attestation [4]. After BGP route selection process completes, the speaker may announce updated routes to neighbors. In the OUT filter, the attestation service is invoked again, which first locates the recorded route information corresponding to routing re-computation, and checks whether the announced routes comply with route attestation rules together with the located information. The outgoing routes are dropped when they do not comply with the route attestation rules, e.g., they are tampered by network operators.

C. Prototype Implementation

We implemented the TBGP in Zebra BGP daemon [32] with software TPM [5]. We use the IBS implementation in MIRACL cryptographic library from Shamus Software [33]. Our prototype implements three primitive functions described above using less than 3,000 lines of C codes.

Figure 4 shows the high level view of the prototype with TPM. If the BGP process is tampered, it cannot achieve the private keys, although it still can be booted and executed. This ensures that all route updates cannot be signed no matter whether they comply with attestation rules or not. If key unsealing succeeds, the BGP attestation service obtains private keys and attests route updates received (sent) from (to) neighbors in the IN (OUT) filter. The route updates are also signed and verified in IN and OUT filters if they are successfully attested.

[4]In our prototype, we directly leverage Adj-RIBs-IN to realize the database since it is tamper-resistant in our prototype.

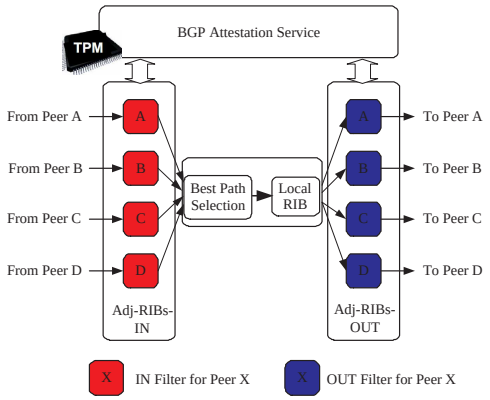

Fig. 4. The architecture of TBGP.

In many existing BGP solutions, data-plane attacks [12] can be launched by modifying the records in Adj-RIBs-OUT and hence making the records in Local RIB and Adj-RIBs-OUT inconsistent. Since the BGP process is attested with TPM and the consistency between a router's control-plane and data-plane can be attested and verified by its neighbors, any tampered BGP process whose records in the control- and data-plane are not consistent cannot announce routes with correct signatures, and hence the routes announced by them will not be adopted by their neighbors. Thus, data-plane attacks can be prevented in TBGP. Note that TBGP focuses on the prevention of the routing attacks which allow ASes to announce routes not really used by themselves, e.g., smart interception attacks pointed by Goldberg *et al.* [34]. However, TBGP does not address other attack strategies proposed in [34] that may violate routing configuration guidelines [26]. For example, announcing longer paths may violate valley-free property of inter-domain routing and raise routing instability [35].

V. Performance Evaluation

We use both experiments and simulations to evaluate the performance of TBGP. For our experiments, we deploy our TBGP prototype in five Linux-2.6.21 machines which have Pentium 4 1.7GHz CPU and 1GB memory and form a topology of 3 ASes shown in Figure 5. ASes 1 and 2 have two eBGP peering links between R1 and R2 and between R1 and R3, and ASes 2 and 3 have two eBGP peering links between R4 and R5 and between R2 and R5. R3 and R4 are connected via an iBGP peering link. We only configure different number of prefixes in AS 1, and AS 2 only forwards the learned route to AS 3. We study the overhead of different operations in TBGP: 1) *IN Filter Attestations*: the duration between the time when route updates are received and the time they are sent out to iBGP neighbors, during which route updates are only attested in IN filters; 2) *Out Filter Attestations*: the duration between the time when routes received from iBGP neighbors and the time they are sent out to eBGP neighbors, which route updates are only attested in OUT filters; 3) *both Filter Attestations*: the duration between the time when route updates are received from eBGP neighbors and the time they are sent out to neighbors, which route updates are attested in both IN and OUT filters. We evaluate the overhead in IN filter attestations in R3 in AS 2, the overhead in OUT filter attestations in R4 in AS 2, and the overhead in both filter attestations in R2 in AS 3. We also evaluate the route processing time in ordinary BGP without attestation.

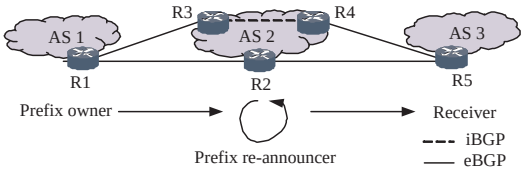

Fig. 5. AS topology in our experiments. AS 1 announces prefixes, and AS 2 forward the routes to AS 3.

We further simulate TBGP to study its performance in large scale networks. Similar to most of the previous BGP proposals (e.g., [20]), we use SSFNet [36], which is an event-driven simulator, and provides basic process model of BGP [36]. The experimental performance is seeded into simulations as the parameters. We use four different scales of AS-level topologies with 10, 29, 110, and 208 ASes, respectively (the later three topologies provided by BJ Premore [36] are generated from real BGP routing tables and used in most of BGP simulations [20], [37]). In our simulations, we compare TBGP with different variants of SBGP schemes, ordinary SBGP, SBGP with cryptographic operation speedup (S-A) [20], SBGP with sequential aggregate signature (SAS) [20], and Path Authentication (PATH) [22]. Among many proposed security-enhanced BGP proposals, we only evaluate and compare some classical ones, such as the SAS using aggregate signatures which is the main technique used by Zhao *et al.* [38]. The main overhead in S-BGP lies in verifying multiple signatures for path authentications, which is also one of the main goals in TBGP, and not addressed in origin authentication proposed by Aiello *et al.* [7]. Thus, we did not evaluate these schemes in this paper. The performance of cryptographic operations in these existing schemes is measured with standard Digital Signature Algorithm(DSA) [20].

A. Experimental Data

Firstly, we evaluate the overhead introduced by key unsealing during BGP bootstrapping. The result shows that TBGP has about 33% delay in bootstrapping. Since it is only one-time operation, the overhead is acceptable. Furthermore, we evaluate the performance of 512 bits IBS algorithms in TBGP. The execution time of signing and verifying operation with IBS is about 4ms and 50ms, respectively. The overall overhead is similar to that of the RSA and DSA algorithms [33].

The processing overhead in TBGP is introduced by route attestations including the cryptographic operations. We evaluate the processing overhead of TBGP with different number of announced prefixes. Figure 6 shows the processing overhead with different BGP sessions. All overheads increase with the increases of the number of announced prefixes. Averagely, the overall process time in ordinary BGP per route update is 0.16 *ms*, and the overheads in IN filter attestations, OUT filter attestations and both filter attestations per route update are 2.31 *ms*, 2.27 *ms*, and 2.32 *ms*, respectively. It is surprising that these different attestation operations (with different number of announced prefixes) introduce similar overheads. The possible reason is that route selections and IN and OUT filter

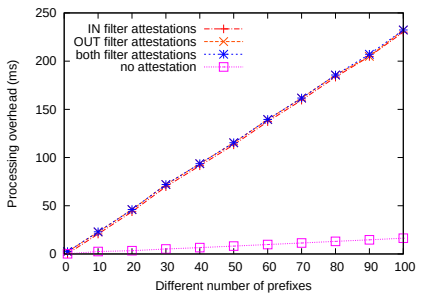

Fig. 6. The overhead of different sessions in ordinary BGP and TBGP: no attestation, IN filter attestations, OUT filter attestations, and both filter attestations.

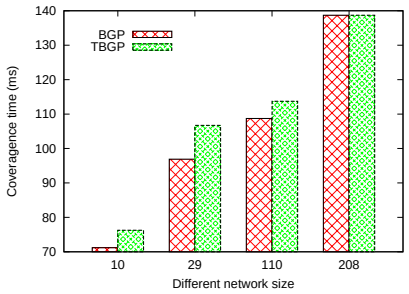

Fig. 7. TBGP introduces average 5% of extra convergence time over ordinary BGP. Compared to 200% extra convergence time of SBGP, it introduces very small convergence overhead.

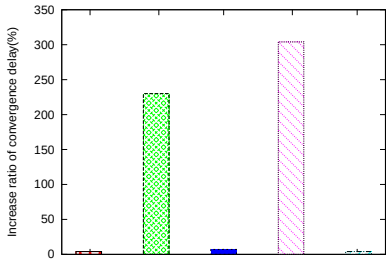

Fig. 8. TBGP only has 4% increase ratio in convergence time relative to ordinary BGP in the 100 ASes topology. TBGP and PATH have a similar convergence performance. Compared to SBGP, S-A, and SAS, TBGP has 56.5, 1.25, 75 times improvements, respectively.

attestations performed in parallel in both filter attestations if the number of announced prefixes is more than 1. In a later subsection, we will study whether the processing overhead impacts the performance of BGP routing (c.f., Figure 7).

B. Simulation Results

It is not surprising that TBGP introduces communication and processing overheads compared to ordinary BGP, as it consumes CPU resources to perform IBS signing and verifying operations, which are the major causes influencing the BGP convergence performance. To explore these aspects, we simulate with 512 bits IBS algorithms and model running times in Section V-A. For simplicity without loss of generality, the simulated networks have one BGP speaker for each AS and attestation overheads in each AS include both IN and OUT filter attestations. We evaluate the routing convergence time of our simulation, which considers all the overheads introduced in TBGP route computation and selection, and is frequently used to evaluate computation overheads in literature. Figure 7 shows the impact of TBGP on convergence time, compared with the ordinary BGP. In these four different topologies, TBGP has 7%, 10%, 4%, and 0% extra convergence time compared to ordinary BGP, respectively. Especially, TBGP does not introduce extra convergence delay in large-scale topologies, such as the 208 ASes topology, because the MRAI timer [1] of 30 seconds becomes the major cause of convergence delay. Compared with SBGP, whose convergence time is over 200% larger than that in ordinary BGP [20], TBGP achieves much better performance.

Figure 8 shows the impact of TBGP on the increase ratio of convergence time with the 110 ASes topology. TBGP only increases 4% convergence delay and achieves much better routing performance over SBGP and other variants of SBGP. For instance, the convergence performance in SBGP increases over 2 times of convergence delay, S-A introduces 9% extra convergence delay, and SAS increases over 3 times at the cost of increased memory consumption. Compared to SBGP, S-A, SAS, TBGP has 56.5, 1.25, and 75 times improvements in convergence time, respectively. The performance result is rational because only one signing and verifying operation is involved in a BGP speaker to attest a route in TBGP, while these secure BGP schemes need several times to verify a route. The overhead of message signature in TBGP is reduced from $\mathcal{O}(n)$ in SBGP to $\mathcal{O}(1)$ where n is the length of an AS_PATH. Note that to verify a received route update in these schemes, the time of signature verification is super-linear to the length of AS_PATH. PATH only requires one public key signature verification, therefore has similar convergence performance as TBGP.

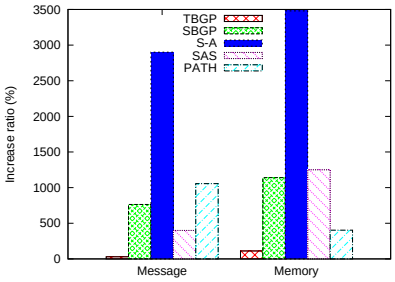

Fig. 9. Overheads introduced by TBGP are much lower than other schemes. TBGP only introduces 96% of increase in update message size and requires about 1.1 times more memory to cache routes. Compared to SBGP, S-A, SAS and PATH, TBGP has 24.38, 95.41, 12.28, and 34.09 times improvements in message size, and 9.26, 30.32, 10.25 and 2.63 times improvements in memory consumption, respectively.

Figure 9 shows the impact of TBGP on message size and memory costs with 110 ASes topology. The baseline of average announcement message and memory cost in our experiment is 36.09 bytes and 9 KB [20], respectively. On average, the message size increase in SBGP is more than 763% and that in TBGP is only about 96%. Compared to S-A, SAS, and PATH, TBGP still achieves much better performance. For example, the average message size of BGP updates in PATH is 34 times larger than that in TBGP since PATH needs to generate and piggyback tree-based authentication proofs in updates. Furthermore, TBGP has significant improvement in memory consumption. As illustrated, the SBGP scheme consumes additional 1140% of memory to cache routes and their signatures, but TBGP only requires about 1.1 times more memory to cache routes and has a 9.26 times improvement over sBGP. Similarly, memory consumption in S-A, SAS, and PATH is more than 130% larger than that in TBGP. The reason behind the low cost is that TBGP does not require caching received route signatures for further propagation thus eliminates the storage complexity of $\mathcal{O}(n^2)$ in SBGP.

VI. Discussion

Key Distribution: The prototype of TBGP adopts IBS and then relaxes the centralization requirement of authorities because different prefix/AS assignment organizations can generate private keys independently. It does not require additional infrastructure and mechanism to manage and distribute certificates. These authorities are only authorized to generate and bind private keys with prefixes/ASes which they are authorized to assign. Before that, PKG services provided by these authorities only need to negotiate to obtain IBS security parameters, such as same master keys, and then build a flat infrastructure in a secure way [16]. Actually, we can further relax the implication. Since TBGP builds transitive trust in the Internet by authenticating and attesting neighbor ASes, we can deploy local regional PKG services to generate different AS number keys. Different ASes can authenticate and attest each other and build local trust chains if their IBS parameters are assigned by the same regional services, and only some large ASes (or top-tier ASes) are required to achieve different parameters from different regional services to bridge the trust chains. Thus, we only require the global authorities, IANA and the regional Internet registries, such as AfriNIC, APNIC, ARIN, LACNIC, and RIPE NCC, to bind keys with prefixes. The approach is similar to what have been done in Resource Public Key Infrastructure (RPKI) for BGP security [39]. For sake of simplicity, we do not consider the prefix hierarchy in this paper, but assume the centralized PKGs distribute keys when a router goes online. To realize a decentralized key distribution, we can leverage the hierarchical IBS [40], where the public key (identity) is a hierarchical prefix, and then local/domain-level PKGs can be introduced.

Key Refreshment: It is well known that IBS algorithms have a difficult problem on key revocation. Although key-insulated systems can solve such a problem [41], they introduce more computation overhead on routers. We solve the problem from the view of BGP operations. In TBGP, private keys are under strong protection, which means a route can achieve correct signature only if the router platform is not compromised. If the router is misconfigured by its operator, the route also cannot obtain correct signatures because it cannot be attested by the trusted routing service. Moreover, in TBGP, we propose to use ephemeral public identities, where the public keys can be generated by including timestamp with identity depending on granularity. The private key is then updated periodically in a automatic way. This approach is suggested in original IBE algorithm [42], and is successfully implemented in commercial products [43]. In general, there are two cases for key revocation in TBGP: 1) The router role is changed, e.g., prefix owner is changed. This can be handled by key request and re-generation. 2) The keys are compromised. This case happens in TBGP when the TPM is compromised. If the router OS or BGP logic is compromised, private keys cannot be unsealed by the TPM. For attacks on TPM, we only require a TPM interact with some well known address authorities when the router firstly accesses to Internet. Thus, the attack interface of the Parno attack [44] is limited. Moreover, since the Tarnovsky attack [45] requires physical access to TPM, we do not consider this issue in this paper.

VII. Conclusion

In this paper, we propose TBGP, a lightweight secure BGP solution to prevent BGP routing attacks. In TBGP, a set of route attestation rules is strictly enforced in each router to simplify route attestations and build a trusted Internet routing infrastructure, and thus aggregated signatures are eliminated without sacrificing the security of BGP. Our prototype leverages the trusted computing (TC) technology to build transitive trust relationships between BGP speakers, and the identity-based signature (IBS) algorithm to sign/verify BGP routes and reduce the complexity of security operations in existing secure BGP solutions. Our security analysis and performance study shows that TBGP meets the security goals of BGP with significantly better convergence performance and lower resource cost than traditional solutions.

Acknowledgement

The work is supported by the National Natural Science Foundation of China under grant No. 61073166 and No. 61133015, the National Basic Research Program of China (973 Program) under grant No. 2009CB320502 and No. 2012CB315803.

References

[1] Y. Rekhter, T. Li, and S. Hares, "A border gateway protocol 4 (BGP-4)," *RFC 4271*, 2006.
[2] "Youtube hijacking: A RIPE NCC RIS case study," http://www.ripe.net/news/study-youtube-hijacking.html.
[3] J. Caballero, T. Kampouris, D. Song, and J. Wang, "Would diversity really increase the robustness of the routing infrastructure against software defects?" in *Proc. of the ISOC NDSS*, 2008.
[4] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol," *IEEE JSAC*, vol. 18, no. 4, pp. 582–592, 2000.
[5] R. White, "Through secure origin BGP," *The Internet Protocol Journal*, vol. 6, no. 3, pp. 15–22, 2003.
[6] P. van Oorschot, T. Wan, and E. Kranakis, "On inter-domain routing security and pretty secure BGP (psBGP)," *ACM TISSEC*, vol. 10, no. 3, pp. 1–41, 2007.
[7] P. McDaniel, W. Aiello, K. R. B. Butler, and J. Ioannidis, "Origin authentication in interdomain routing," *Computer Networks*, vol. 50, no. 16, pp. 2953–2980, 2006.
[8] Y. Hu, A. Perrig, and M. Sirbu, "SPV: Secure path vector routing for securing bgp," in *Proc. of the ACM SIGCOMM*, 2004, pp. 179–192.
[9] L. Subramanian, V. Roth, I. Stoica, S.Shenker, and R. Katz, "Listen and whisper: Security mechanisms for BGP," in *Proc. of NSDI*, 2004.
[10] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, and A. Rubin, "Working around BGP: An incremental approach to improving security and accuracy of interdomain routing," in *Proc. of the ISOC NDSS*, 2003, pp. 75–85.
[11] J. Karlin, S. Forrest, and J. Rexford, "Autonomous security for autonomous systems," *Computer Networks*, vol. 52, pp. 2908–2923, 2008.
[12] S. Goldberg, S. Halevi, A. D. Jaggard, V. Ramachandran, and R. N. Wright, "Rationality and traffic attraction: Incentives for honest path announcements in BGP," in *Proc. of the ACM SIGCOMM*, 2008, pp. 267–278.
[13] N. Aaraj, A. Raghunathan, and N. K. Jha, "Analysis and design of a hardware/software trusted platform module for embedded systems," *ACM Transactions on Embedded Computing Systems*, vol. 8, no. 1, 2008.
[14] R. Gummadi, H. Balakrishnan, P. Maniatis, and S. Ratnasamy, "Not-a-bot: Improving service availability in the face of botnet attacks," in *Proc. of NSDI*, 2009.
[15] E. Keller, M. Yu, M. Caesar, and J. Rexford, "Virtually eliminating router bugs," in *Proc. of the ACM CoNext*, 2009.
[16] A. Beimel and B. Chor, "Universally ideal secret sharing schemes," *IEEE Trans. on Info. Theory*, vol. 40, no. 3, 1994.

[17] Q. Li, M. Xu, J. Wu, X. Zhang, P. P. Lee, and K. Xu, "Enhancing the trust of internet routing with lightweight route attestation," in *Proc. of the ASIACCS*, 2011, pp. 92–101.

[18] Z. Zhang, Y. Zhang, Y. C. Hu, Z. M. Mao, and R. Bush, "ispy: Detecting IP prefix hijacking on my own," in *Proc. of the ACM SIGCOMM*, 2008.

[19] A. Haeberlen, I. Avramopoulos, J. Rexford, and P. Druschel, "Netreview: Detecting bgp configuration faults with static analysis," in *Proc. of NSDI*, 2009.

[20] M. Zhao, S. Smith, and D. Nicol, "The performance impact of BGP security," *IEEE Network*, vol. 19, no. 6, pp. 42–48, 2005.

[21] E. Shi, A. Perrig, and L. van Doorn, "BIND: A fine-grained attestation service for secure distributed systems," in *Proc. of the IEEE Symposium on Security and Privacy*, 2005, pp. 154–168.

[22] K. Butler, P. McDaniel, and W. Aiello, "Optimizing BGP security by exploiting path stability," in *CCS*, 2006, pp. 298–310.

[23] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: a prefix hijack alert system," in *Proc. of the USENIX Security Symposium*, 2006.

[24] X. Hu and Z. M. Mao, "Accurate real-time identification of IP prefix hijacking," in *Proc. of the IEEE Symposium on Security and Privacy*, 2007, pp. 3–17.

[25] P. Reynolds, O. Kennedy, E. G. Sirer, and F. B. Schneider, "Securing BGP using external security monitors," *Cornell University, Computing and Information Science, Technical Report TR2006-2065*, 2006.

[26] N. Feamster and H. Balakrishnan, "Detecting bgp configuration faults with static analysis," in *Proc. of NSDI*, 2005.

[27] T. G. Griffin, F. B. Shepherd, and G. Wilfong, "The stable paths problem and interdomain routing," *IEEE/ACM Transactions on Networking*, vol. 10, no. 2, pp. 232–243, 2002.

[28] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of Crypto*, 1984, pp. 47–53.

[29] "Trusted computing group," https://www.trustedcomputinggroup.org/.

[30] E. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *Proc. of CCS*, 2004, pp. 132–145.

[31] "TPM emulator," http://tpm-emulator.berlios.de.

[32] "GNU Zebra," http://http://www.zebra.org/.

[33] "Shamus software ltd, MIRACL," http://www.shamus.ie/.

[34] S. Goldberg, M. Schapira, P. Hummon, and J. Rexford, "How secure are secure interdomain routing protocols," in *Proc. of SIGCOMM*, 2010, pp. 87–98.

[35] L. Gao, "On inferring autonomous system relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, pp. 733–745, 2001.

[36] "SSF network models (SSFNet)," http://www.ssfnet.org/homePage.html.

[37] W. Sun, Z. Mao, and K. Shin, "Differentiated bgp update processing for improved routing convergence," in *Proc. of the ICNP*, 2006.

[38] M. Zhao, S. W. Smith, and D. M. Nicol, "Aggregated path authentication for efficient BGP security," in *CCS*, 2005, pp. 128–138.

[39] "ARIN RPKI," https://www.arin.net/resources/rpki.html.

[40] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Proceedings of ASIACRYPT*, 2002.

[41] Y. Dodis, S. Xu, and M. Yung, "Key-insulated public-key cryptosystems," in *Proc. of Eurocrypt*, 2002, pp. 65–82.

[42] D. Boneh, E. Goh, and X. Boyen, "Hierarchical identity based encryption with constant size ciphertext," in *Proc. of Eurocrypt, LNCS 3493*, 2005.

[43] "The true costs of e-mail encryption: Trend micro IBE (identity-based) vs. pki encryption,http://us.trendmicro.com/imperia/md/content/us/pdf/products/enterprise/emailencryption/the_true_cost_of_email_encryption_6-2010.pdf," Oct. 2010.

[44] B. Parno, "Bootstrapping trust in a "trusted" platform," in *Proc. of HotSec*, 2008.

[45] C. Tarnovsky, "Security Failures In Secure Devices," in *Black Hat DC*, 2008.