Security of the Border Gateway Protocol

LOUKAS DROSOS

Supervisor: Dr. Vasileios Stathopoulos

Department of Physics, National Kapodistrian University of Athens, Greece

Abstract. Technological advancements have made communication one of the most important achievements of today's world. The Border Gateway Protocol (BGP) is the standard interdomain routing protocol of the Internet, which means it has a crucial role in current communications. Despite its importance, the conception and development of BGP didn't include any internal security mechanism, which has proven to be a major limitation. Security analyses in the last years have shown that the Internet routing infrastructure is prone to many vulnerabilities and attacks which can cause large scale outages. Since the adoption of BGP, several security features have been proposed, but only some minor tweaks have actually been implemented. In this paper, we conduct a review of current BGP threats and explore security proposals and standardization efforts, as well as their advantages and limitations.

Introduction

The Internet is a large set of networks, each one consisting of routers and hosts under the control of a single entity. These networks, called autonomous systems (ASes), have their own unique AS numbers and connect with each other using external links. ASes also use routing protocols to exchange network reachability information between them and select the optimal path for data transmission. The process of routing between ASes uses external links and is called interdomain routing, while the interdomain routing protocol is the external Border Gateway Protocol (eBGP) and runs over TCP. Similarly, iBGP (internal Border Gateway Protocol) is the intradomain routing protocol that transmits information within an AS using internal links. Generally, when mentioning BGP, we refer to eBGP rather than iBGP [1], [2].

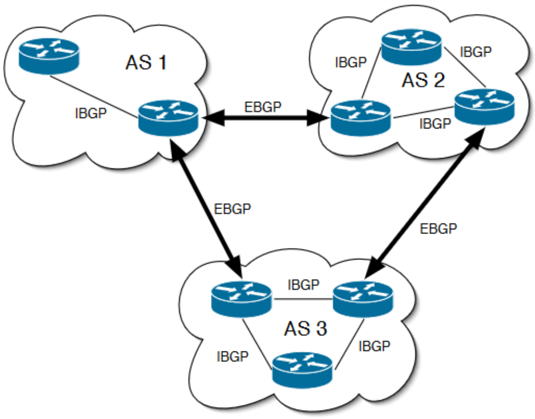


Figure 1. *Interdomain and intradomain routing of ASes* [3].

BGP has been widely used for over a decade and its deployment has allowed simplicity and resilience in the Internet's operation, even though it doesn't offer any performance enhancements or security guarantees. The limited guarantees provided by BGP leave it vulnerable to attacks and misconfigurations, while sometimes contributing to serious instabilities in the routing system and causing severe reachability problems. BGP vulnerabilities can also be exploited to monitor users of anonymization networks, cause damage to cryptocurrencies and even help spammers evade detection. These weaknesses could also lead to devastating communications failures in essential applications like online banking, stock trading, and telemedicine conducted over the Internet [2], [4].

As the dependency on the foundational network infrastructure to provide reliable and secure Internet services increases, there's been considerable interest in enhancing the security of BGP. Numerous research efforts have suggested various BGP security extensions over the past decades, with not one of them, however, being universally deployed on the Internet. This is primarily because they often address specific routing vulnerabilities or impose significant computational overhead [2], [4].

This paper explores the fundamental BGP vulnerabilities and possible attack threats, while also reviewing some security proposals. Section 1 provides a brief overview of interdomain routing, BGP and its implementation. Section 2 follows with the fundamental BGP threats and possible attacks. In Section 3 desired properties for BGP security solutions are examined, which will also be used to evaluate the existing security proposals that are introduced and analyzed in Section 4.

1. *Border Gateway Protocol*

The Border Gateway Protocol is used by a large number of ASes to discover routes that reach different ranges of IP addresses, called IP prefixes. BGP is an incremental protocol, routers send BGP announcement messages to other routers when new routes are available, and withdrawal messages when these routes no longer exist. BGP also functions as a path-vector protocol, where each AS adds its AS number at the start of the AS path before propagating the route to the next AS. Each router in the network selects a primary BGP route for every destination prefix and might implement complex policies to determine the route selection and whether to propagate it to a neighboring router in a different AS [2].

1.1 *IP Prefixes and AS Numbers*

An IP address is a 32-bit number, commonly represented in dotted-decimal format, with each of the four octets denoted by a separate integer. Institutions receive IP addresses in blocks of consecutive addresses, identified by the initial address and a mask length. The number following the IP address indicates the number of fixed bits in that prefix and is referred to as the prefix length. For example, the prefix 192.0.2.0/24 contains the 256 addresses, 192.0.2.0 to 192.0.2.255, that have 192, 0, and 2 as their first three octets, while the /24 means that the first 24 bits of the IP address remain constant, and the other 8 bits can vary. Assigning addresses in blocks reduces routing table sizes and minimizes route advertisements, as routers typically only need to route traffic to the address block instead of maintaining distinct routing information for each IP address [1], [2].

Initially, the Internet Assigned Numbers Authority (IANA) was responsible for the assignment of addresses to institutions, which is now overseen by the Internet Corporation for Assigned Names and Numbers (ICANN). Currently, IANA is responsible for the delegation of addresses in specific geographical regions. For instance, the assignment of addresses in North America is managed by the American Registry for Internet Numbers (ARIN), while the address space of Europe, the Middle East, and North Africa is managed by Reseaux IP Europeens (RIPE). Similarly, the Asia-Pacific Network Information Center (APNIC) handles IP address assignments in Asia and the Pacific Rim, while the Latin American and Caribbean Internet Address Registry (LACNIC) serves the Latin American and Caribbean regions, while the African Internet Numbers Registry (AfriNIC) caters to the African region. These regional registries have the authority to further assign IP addresses to organizations and other registries, including national registries and internet service providers (ISPs), that may also allocate smaller portions of the address block to different institutions. Fig. 2 illustrates the process of address delegation, where IANA delegates the address block 210.0.0.0/7 to APNIC. APNIC then delegates 211.120.0.0/12 to the Japan Network Information Center (JPNIC), which subsequently assigns 211.120.132.0/22 to Sony. Sony can further delegate addresses based on its organizational requirements [2].

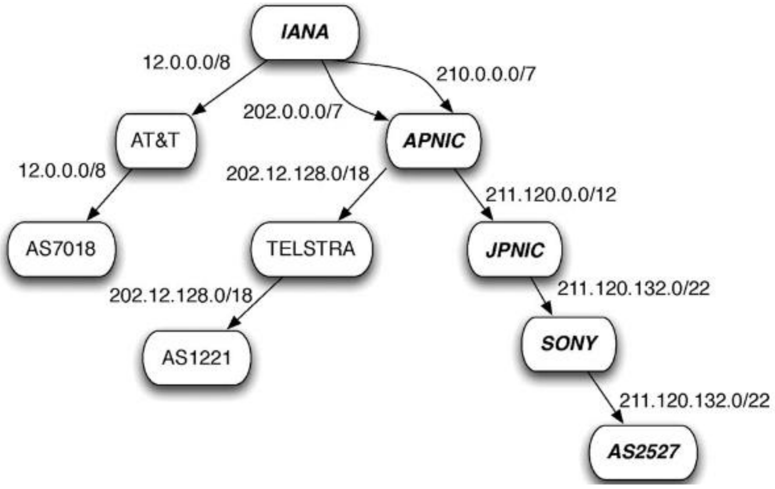


Figure 2. *Address delegation from IANA to regional and national registries* [2].

IANA similarly serves as the authority that handles the assignment of AS numbers (ASNs) to Autonomous Systems. AS numbers ranging from 1 to 64511 are considered public and have Internet-wide scope, with each number corresponding to a single AS. Some companies, however, can have multiple ASes. Public AS numbers can appear in the AS-path attribute of BGP advertisements. Despite this, many institutions may not require a unique AS number. For instance, an Autonomous System may connect to a single upstream network provider who is solely responsible for providing connectivity to the rest of the Internet. Private AS numbers within the range of 64512–65535 can also be assigned to customer ASes in order to communicate with its provider via BGP. Those BGP routes would then be advertised by the customer's provider without including the customer's private AS number in the path. This practice enables service providers to reuse the same private AS number for multiple customers [2].

1.2 *BGP Route Selection*

Autonomous Systems (ASes) exchange with other ASes information about the IP addresses they own and the routes they have to specific IP prefixes. When an AS announces its ownership of a prefix, it does so by declaring that it owns the prefix and creating a route towards the prefix consisting solely of its AS number. If the AS propagates a route, it prepends its AS number to the route towards that prefix. These exchanges of information occur through BGP messages that are transferred over the Internet's Transmission Control Protocol (TCP) from AS to AS. An illustration of this exchange is depicted in Fig. 3, where AS 6 owns prefix 12.34.0.0/16. This ownership is broadcasted by transmitting the prefix along with AS number 6 to all ASes connected to AS 6. In this scenario, it is only sent to AS 5, which then prepends its number to the route and forwards it to neighboring ASes, indicating that the route to 12.34.0.0/16 is along AS 5 to AS 6 [1].

When routers are presented with two routes to the same prefix, they typically retain the shorter one and discard the longer one. Typically, the shorter path is the one with the fewest number of hops. Also, in case routers receive a route leading to a prefix that is a more specific version of a prefix they already possess, they store and forward both routes. When the destination IP address for data packets matches both prefixes, it will be forwarded along the path to the more specific prefix [1].

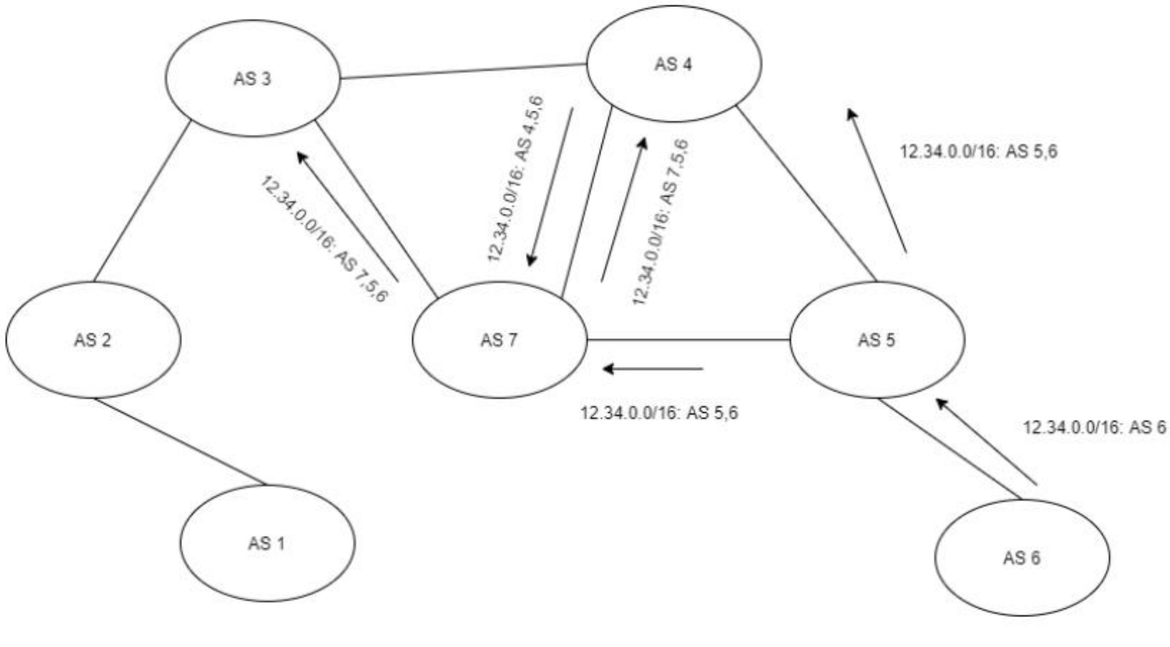


Figure 3. *Regular advertisement of prefix 12.34.0.0/16 originating from AS 6* [2].

1.3 *BGP Export Policies*

Nowadays, the interconnectivity of ASes is based on confidential business agreements that dictate the policies that will be implemented on each AS connection. These business relationships are classified as either customer-provider or peer-peer relations. BGP peers are BGP routers that connect to one another in order to exchange routing information. In a customer-provider relationship, a customer AS pays another AS, which is either a provider or another customer, to gain access to the rest of the Internet. In a peer-to-peer relationship, on the other hand, two ASes negotiate a link between themselves and exchange traffic free of charge. An AS can propagate incoming routes to other ASes based on the type of relationship it has with the AS it received the information from. Routes learned from customer ASes can be further advertised to other customers, peers and providers, while routes learned from peer or provider ASes can be advertised to customers only. From the business revenue perspective, a customer route is preferred over a peer or a provider route, and a peer route is preferred over a provider route [4], [5].

In case two neighboring ASes connect to each other at multiple geographic locations, an AS may include a Multi-Exit Discriminator (MED) which is the last decision maker in case all other route selection factors are the same. A MED is used to specify the best link to its neighbors and direct the traffic to chosen peering location. The use of a MED is typically a part of the contract between the two ASes. Otherwise, an AS prioritizes its own local policies and based on them can select any of the available routes to its neighboring AS [2].

1.4 *BGP Message Format*

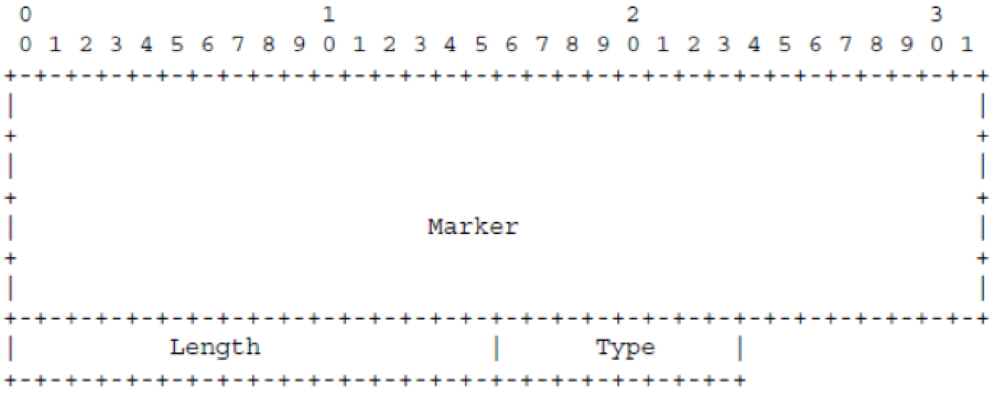
BGP is used to share routing information between ASes. BGP peers connect to one another to exchange routing information via BGP messages. Similar to IP, BGP messages feature a fixed-size header designed to convey information about the subsequent data that may or may not follow the header. Fig. 4 illustrates a schematic representation of this header. The header comprises of a 128-bit marker, which serves as a value for detecting synchronization loss between BGP routers and authenticating incoming messages. Additionally, there is a 16-bit long length field that specifies the total message length, including the header, in octets. Finally, an 8-bit long type field indicates the message type: 1 for OPEN, 2 for UPDATE, 3 for NOTIFICATION, and 4 for KEEPALIVE, each one with its own purpose [1], [6].

- OPEN messages are used to set up a BGP connection between two peering routers. An OPEN message is the first message sent by each router of a connection once the connection is established [1].

- UPDATE is a message type that transfers routing information between BGP routers, including path availability and new path attributes, which can be used to create a relationship graph of different ASes. Each UPDATE message contains a Classless Inter-Domain Routing (CIDR) network address or IP prefix, an AS originating this prefix, the Autonomous System path (AS_PATH), which is the sequence of ASes that the message has traversed through, and the IP address of the next in the path router to the destination [1], [4].

• NOTIFICATION messages are used for error detection. When a NOTIFICATION message is transmitted, the active BGP connection closes [1].

• KEEPALIVE are messages that are exchanged between peers to verify that certain peers are still reachable and that the session is still active [1].



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                                                               +
|                           Marker                              |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Length               |      Type     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4. *A schematic representation of the header of a BGP message* [1].

1.5 *BGP Connection Setup*

ASes use BGP to announce routes to a number of prefixes based on their routing policies and negotiated interconnections. The establishment of a BGP connection is illustrated in Fig. 5. Initially, BGP routers are in an idle state until they connect to another BGP router, transitioning to the "connect" state. The router remains in this state until the three-way handshake of TCP is complete and a TCP connection is established. When a connection is established, the router sends an OPEN message to start a BGP session and is either an the "active" state or an "opensent" state. If the OPEN message was transmitted successfully to another router, then the transmitter is in the "opensent" state, otherwise it is in the "active" state. In the latter state, the router will transmit another OPEN message and if successful the router transitions to the "opensent" state, if not its state changes back to "connect". During the "opensent" state, if the OPEN message is confirmed to be received by another router, the transmitter goes into the "openconfirm" state. In this state, a KEEPALIVE message is transmitted and both routers transition to the established state, which is the final state and allows two routers to exchange routing information with one another [1].

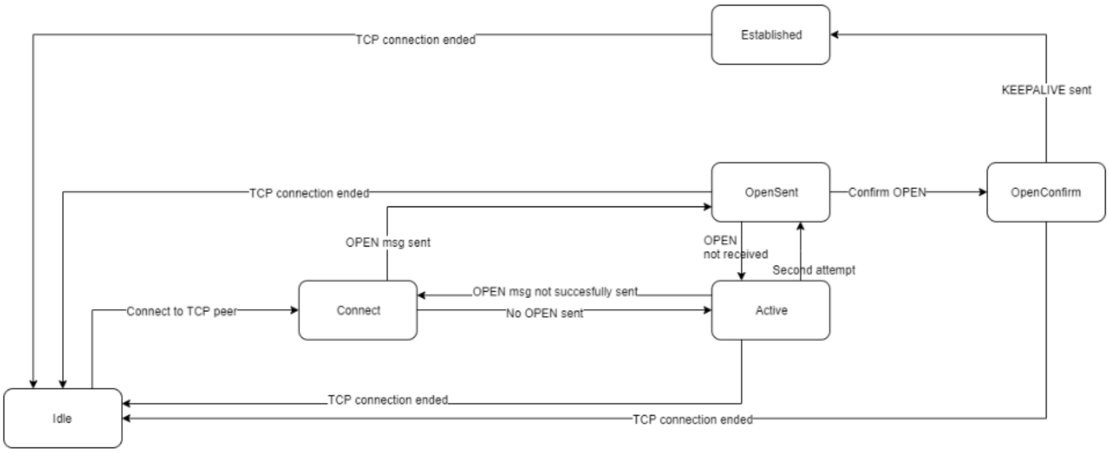


Figure 5. *BGP connection establishment* [1].

If no routing updates are exchanged, then KEEPALIVE messages are periodically sent to keep the peering connection open. When a routing table, called Routing Information Base (RIB), changes, UPDATE messages are exchanged between routers to announce new routes, route updates and route withdrawals. When a router receives an UPDATE message, it stores the new routing information in its RIB. The RIB of every router consists of the Adj-RIBs-In, the Loc-RIB, and the Adj-RIBs-Out. The Adj-RIBs-In store information about routes learned from other BGP routers. These routes can be filtered in order to make easier the selection of routes that will be forwarded to the Loc-RIB for usage in the selection procedure. The Loc-RIB stores these routes that the BGP selected and writes them to the local routing table. The Adj-RIBs-Out contains a set of routes that the BGP router has chosen for advertisement neighboring BGP routers. The selected routing information will be carried by the UPDATE messages coming from this BGP router. This process is illustrated in Fig. 6 [1], [4].

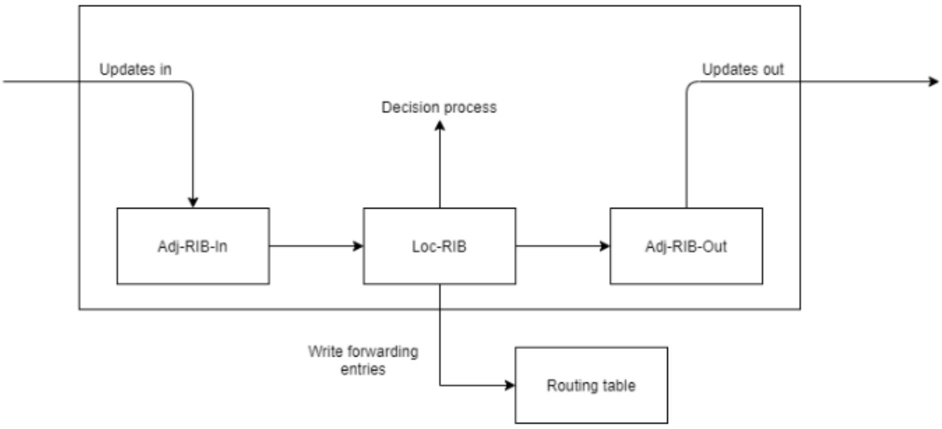


Figure 6. *Selection of routes to be carried by the UPDATE messages* [1].

Routers may also use Routing Flap Damping (RFD) and Minimum Route Advertisement Interval (MRAI) timers. The RFD timer tracks how often a route is withdrawn and re-announced. If this frequency surpasses a certain threshold, the route is labeled as damped, indicating instability, and is ineligible to be chosen as the best route. On the other hand, the MRAI timer determines the duration of time that must elapse before a route can be re-advertised to neighboring routers. The primary objective of both timers is to diminish the occurrence of routing changes and message overhead, thereby reducing the routers' load and restrict overall routing instability [4].

2. *Attacks against BGP*

BGP was developed in the 1990s with the sole purpose of linking subnetworks in order to create a global network. Because BGP was developed in a time when the Internet was not a critical infrastructure, the risk of redirecting traffic was not considered as a serious threat to prevent it from happening. Due to the lack of validation for propagated routes or ownership claims of certain prefixes, BGP can be exploited either maliciously or by accident (such as misconfigurations). BGP messages are transported using TCP/IP, which is a protocol with vulnerabilities to attacks such as SYN flooding and IP spoofing, meaning that the disruption TCP will also affect the correct functioning of BGP. We will assume, however, that we have secure TCP connections so we can examine the attacks that make use of BGP's vulnerabilities [1].

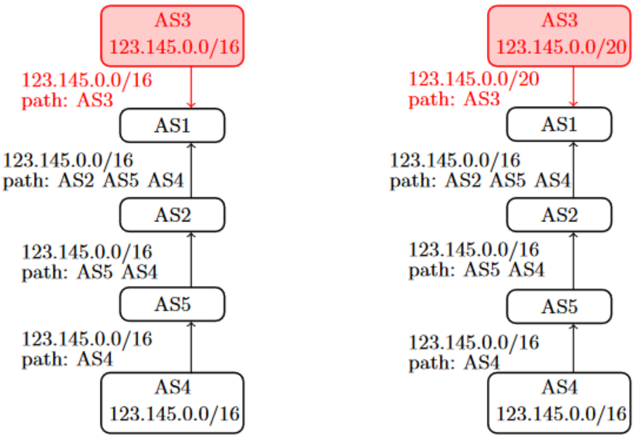
2.1 *Prefix Hijack*

A prefix hijack happens when one AS advertises falsely advertises ownership of a prefix that it does not actually own, with the intention of diverting traffic intended for that prefix to itself. This exploit takes advantage of BGP's lack of verification for prefix ownership claims made by ASes. If no financial motivations influence the decision-making process, then ASes typically select routes to prefixes based on the shortest number of hops. In this case, ASes will select the invalid route if the hijacking AS is closer in terms of hops. For instance, in a network depicted in Fig. 7(a), AS 1 will select an incorrect route towards prefix 123.145.0.0/16, while the other ASes will choose the correct one. Despite the legitimate AS 2 that propagates the legitimate route to AS 1, the number of hops in the that route exceed that of the already selected incorrect route. As BGP lacks mechanisms for route authentication or validation of prefix ownership, some ASes might select a false route towards a prefix while others choose the correct one [1].

When financial motivations are taken into account, particularly in scenarios involving customer-provider relationships between ASes, route selection in the case of a prefix hijack becomes more complicated. A prefix hijack attack has the highest success rate when the original route leads to a provider, since the use of that route would cost money. On the other hand, the least successful attack is the one with a route towards a customer, because using that route would generate revenue [1].

A variation of the prefix hijack known as the subprefix hijack can be even more impactful, especially when a sequence of subprefixes is announced that combined makes up the original prefix. Subprefix hijacking takes advantage of the fact that traffic destined for a particular prefix is directed along the route with the most specific prefix that matches the destination IP address. In a subprefix hijack, an AS falsely claims ownership of a prefix that is more specific than another prefix. For example, in Fig.

7(b), AS 4 has declared ownership of the prefix 123.145.0.0/16, then AS 3 executes a successful subprefix hijack by advertising ownership of the prefix 123.145.0.0/20 [1].



(a) Prefix hijack

(b) Subprefix hijack

Figure 7. *AS 3 falsely claims the (sub)prefix of AS 4 and transmits to AS 1 fake routes to this (sub)prefix with a (a) prefix and (b) subprefix hijack attack* [4].

One of the most notable instances of a prefix hijack in real-world networking is the Pakistan Telecom incident of 2008. In February 2008, in response to a government order to block access to YouTube within Pakistan, Pakistan Telecom began advertising its ownership of the prefix 208.65.153.0/24 to its provider, PCCW. Notably, YouTube was using the prefix 208.65.152.0/22 at the time, although it no longer utilizes this prefix. The objective was to intercept a portion of the traffic destined for YouTube from Pakistan, that's why it can be classified as a subprefix hijack attack. However, PCCW distributed the announcement not just within Pakistan but globally. The result was that Internet traffic intended for YouTube from around the world was redirected to Pakistan, resulting in a widespread impact. The hijack, however, was relatively brief, with YouTube responding after approximately 80 minutes and the false routes being withdrawn just over two hours later [1].

2.2 *Path Altering*

Path altering is the act of altering the AS path in UPDATE messages. Since BGP lacks any integrity checks for altered paths, ASes can modify paths without any intervention. This can cause traffic to be dropped due to routing along a path with a missing a link, but it can also allow malicious ASes to intercept traffic by routing it through their routers, compromising confidentiality. Path altering can also prevent the selection of a legitimate path by adding ASes to the path, making the pathway too long for most routers to consider taking and selecting a different, illegitimate path. This is easily achievable if an AS prepends its own AS number many times over to make the path excessively long. An illustration of a path altering attack is depicted in Fig. 8, where AS 3 receives updates for the prefix 12.34.0.0/16 with paths (7,5,6) and (4,5,6). According to BGP propagation rules, it should transmit the message to its neighbors with its AS number prepended, resulting in AS 3 selecting either (3,7,5,6) or (3,4,5,6) as chosen route. In this case, however, AS 3 opts to alter the path and relays path (3,6) to its neighbors. All the neighbors of AS 3 receive and store the false path, as it is shorter or the only path available. AS 3 can take one of two actions: establish a virtual connection between itself and AS 6 to route traffic through itself, gathering information in the process, or discard all traffic intended for AS 6 [1].

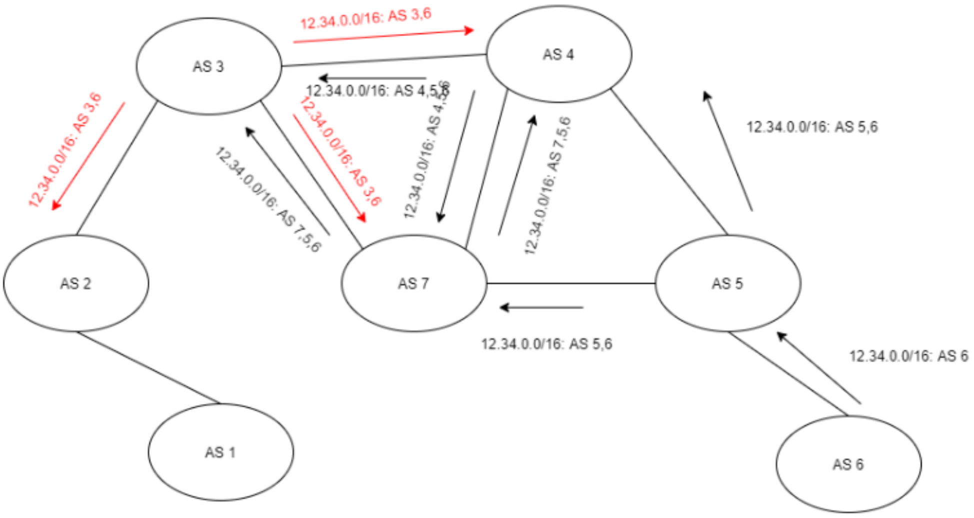


Figure 8. *A path altering attack where AS4 propagates a different path than intended* [2].

There is not a lot of media coverage about path altering and traffic rerouting attacks, due to the lower frequency of reports about their occurrence. An example of a path altering attacks is an incident that happened in June 2019, where a large part of European telecommunications was rerouted along China Telecom. The Swiss company Safe Host is a company that hosts data centers and accidentally leaked routes to China Telecom. Then China Telecom then announced these routes onto the Internet, redirecting a lot of traffic through the AS of China Telecom. The routes stayed in circulation for approximately two hours and, although it was not exactly an attack, as it happened by accident, it still resulted in significant disruption and unintended rerouting of traffic through routers not designated to receive such traffic [1].

2.3 *Speaker Impersonation*

Speaker impersonation is the act of a router falsely claiming to speak BGP, or the router being configured to speak BGP, but with incorrect AS information. This can lead to the injection of false AS numbers into paths, resulting in deceptive routing paths. In the former case, BGP traffic may pass through potentially wiretapped routers, while in the latter, traffic may be redirected to a different AS than originally intended. Both scenarios, nonetheless, compromise network traffic confidentiality, posing serious risks [1].

Although early studies highlighted speaker impersonation as a potential BGP security concern, there have been no significant reports of this flaw affecting global Internet routing. Early security proposals, like S-BGP, addressed this vulnerability by requiring routers to be authorized to speak BGP via a public key infrastructure (PKI). However, later BGP security solutions have largely overlooked this issue, likely due to its rarity in real-world incidents and the ease of achieving similar goals through path alteration. Consequently, modern solutions lack specific defenses against speaker impersonation attacks [1].

2.4 *Protocol Manipulation Attacks*

Protocol manipulation attacks are attacks where a malicious AS aims to manipulate properties of the routing protocol itself. Specifically, the MED and the RFD/MRAI can be exploited to carry out such an attack. Since the MED is not protected, the malicious AS may affect another ASes' decisions by tampering with the MED values of routes, resulting in some paths being propagated to the wrong ASes and causing a route leak. Exploiting the RFD/MRAI timer, in contrast, involves a malicious AS to continuously withdraw and re-announce a route. ASes configured with the RFD timer perceive the route as unstable due to the frequent withdrawals and bans it. On the other hand, ASes utilizing the MRAI timer delay the distribution of the corresponding UPDATE messages, making some ASes perceive the route as unreachable due to the delayed updates [1], [4].

Similar to speaker impersonation, this issue is recognized in the realm of BGP security, and even though there are concerns associated with this attack, there haven't been any reports of such attacks causing significant impact. This doesn't imply, however, that no such attacks have actually occurred. Compared to speaker impersonation, there are even fewer security measures in place to prevent this type of attack. This might be because this specific threat to BGP was identified after much research on secure BGP solutions had already been conducted [1].

2.5 *Denial of Service Attacks*

An AS can use correct routing data in a malicious way, causing attacks such DoS and route leaks against BGP routers. Denial of Service (DoS) attacks are executed by flooding the BGP routers with lots of data, causing heavy congestion on routers or links carrying BGP messages and resulting in the failure of the BGP session. When the BGP session recovers, the routers need to exchange full routing tables. DoS is not a weakness exclusive to BGP, and there are countermeasures against such attacks [1], [4].

Indeed, while there are countermeasures aimed at enhancing BGP security, they generally do not address DoS attacks caused by flooding BGP routers with a large volume of BGP messages. Currently, there are no dedicated security solutions that mitigate DoS attacks targeting BGP routers directly [1].

3. *Desired properties for BGP Security*

In order to evaluate the effectiveness and limitations of existing BGP security proposals, it is essential to analyze the desired properties that must be integrated into a secure routing protocol. Our classification encompasses four primary dimensions: security, privacy, performance, and deployability [4].

3.1 *Security and Privacy Properties*

BGP security proposals must address all known vulnerabilities of the legacy protocol that were previously described and offer countermeasures to mitigate these threats. Additionally, they must ensure that they do not introduce any new attack vectors that were not present in the plain BGP protocol. At the same time, BGP security proposals should also acknowledge that ASes often desire to maintain the confidentiality of their routing policies, business relationships, and other commercial data. Regarding routing privacy, it's crucial to evaluate how much additional sensitive information the new secure protocol may reveal compared to the legacy protocol [4].

3.2 *Performance Properties*

BGP security solutions must deliver specific performance properties to be effectively deployed and utilized on the Internet. One of these properties is convergence delay, which measures how quickly routers settle on the best route. It's essential to establish a baseline convergence time using the legacy protocol. In addition to avoiding prolonged convergence times, it essential to ensure stability in our protocol by verifying if convergence is ever achieved. In case it is not, the quality of connections to some prefixes may degrade or even be lost during the transient period. Scalability is also important in such a protocol in order to assess whether the protocol can scale effectively when fully deployed on the Internet as the number of ASes adopting it grows [4].

Another important performance property is the computational overhead of the protocol. This considers the number of BGP control messages processed per unit of time and the additional CPU-intensive operations required compared to ordinary BGP. It also examines whether auxiliary, more powerful hardware is needed for these computations. The bandwidth overhead refers to the rate of BGP control messages sent and how additional security attributes in the messages impact the required bandwidth. Finally, storage overhead assesses the additional memory required on each BGP router for a new BGP security solution compared to plain BGP implementation. It also considers the need for auxiliary hardware to fulfill these new storage requirements [4].

3.3 *Deployability Properties*

The successful integration of a new BGP security solution depends not only on its security and performance properties but also on how easy its deployment and adoption across the Internet is. Deployability evaluates whether the new BGP security proposal can be deployed incrementally over time. This property examines whether information can be seamlessly forwarded between routers supporting the secure protocol and those running the legacy protocol within the same AS. Due to the vast number of ASes composing the Internet, the ASes that have upgraded to the new protocol must also maintain backward compatibility to enable routing with non-adopters, so coexistence between plain and a secure BGP implementations can be achieved. Simultaneously, once the incremental adoption of a new BGP security solution is initiated, adoptability measures the quantity of volunteer ASes willing to adopt the new protocol and reflects how extensively the adoption will spread. The initial set of adopters and their routing policies significantly influence the level of protocol adoptability [4].

4. *BGP Security Solutions*

There have been many proposed solutions trying to solve BGP's many security vulnerabilities in order to protect it from the previously mentioned attacks. The spectrum of BGP security solutions consists of basic solutions that focus on specific attacks, such as prefix hijacking, to comprehensive solutions engineered to address multiple security vulnerabilities within BGP simultaneously [1].

The proposed BGP solutions in this paper are control plane methods, with their primary goal being the authenticity of the data payload of the BGP protocol. In essence, a router must ensure that incoming data hasn't been removed, modified or replayed during transmission. When receiving an UPDATE message, the router must authenticate the advertised prefix, verify the origin AS, and validate the correctness of the AS path and any additional attributes if they exist. To achieve this verification process, some proposals rely on overlay networks, such as IRV, while other proposals rely on cryptographic methods. Proposals such as S-BGP, soBGP, psBGP and BGPsec rely on asymmetric cryptography, while SPV relies on symmetric cryptography [4].

BGP solutions based on data plane methods also exist and primarily depend on inspecting individual packets by verifying cryptographic primitives, which makes them impractical for widespread deployment. For this reason, most, if not all, of the data plane methods serve as supplementary countermeasures and should be employed alongside a control plane proposal [4].

4.1 *Real-world Security Practices*

Before focusing on research proposing BGP security enhancements, it's important to understand the current protection practices used by network operators. Today, several ASes extend their routing policies by filtering out potentially problematic prefix announcements, such as announcements containing private ASNs or too long AS paths. Additionally, route filtering can be combined with peer locking to further restrict faulty routes that were mistakenly announced between provider ASes and peer ASes. Although incomplete, route filtering and peer locking are widely adopted solutions due to their simplicity and effectiveness. However, their deployment requires significant computational and storage overhead, while also violating privacy requirements due to the exchange of commercial data. This, and the fact that peer locking fails to prevent intentional attacks as it relies on trust between ASes, make neither protection practice as a comprehensive, long-term solution for secure interdomain routing [4].

Route filters can also be created with the use of public repositories with routing data, such as the Internet Routing Registry (IRR). The IRR's objective is to offer a shared global perspective of accurate routing information by allowing ASes to voluntarily upload routing data, which can be then used by other ASes. In order for the IRR to be effective, it must be secure, accurate, and kept up-to-date. However, the upload and extraction of data from the IRR is error-prone, making ASes hesitant to upload confidential routing information [4].

4.2 *Interdomain Route Validation*

The Interdomain Route Validation (IRV) protocol is a new protocol that does not intend to replace BGP, rather, it operates independently from it. Every AS has its own IRV server, where AS-specific policy data is stored. When receiving an UPDATE message, a BGP router contacts its local IRV server. The IRV protocol then performs origin validation by querying the IRV server of the AS where the data came from. In cases where validation of multiple ASes forming a path is required, collections of IRV servers are queried. An illustration of how IRV works is shown in Fig. 9. When AS3 receives a route from AS 2, the IRV server in AS 3 queries AS 2’s server. One observation from this diagram is that AS 1 doesn't require IRV in order for AS 3 to authenticate that specific UPDATE messages originate from AS 2 [1], [4].

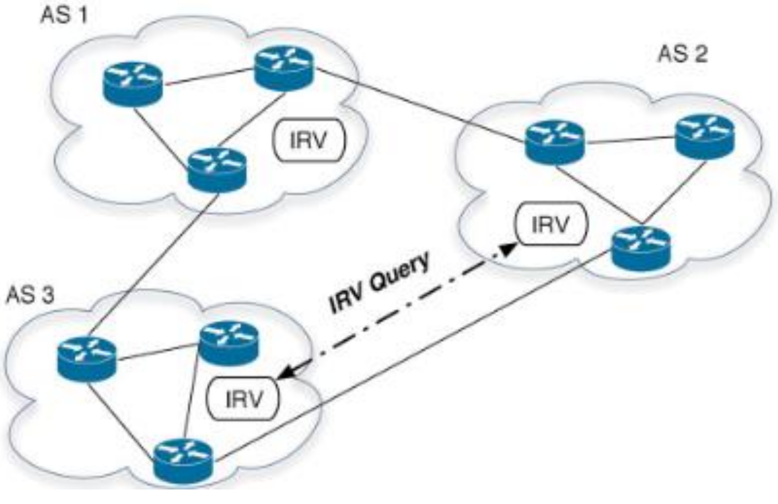


Figure 9. *Operation of the IRV protocol* [2].

By managing access control, IRV servers help maintain privacy while ensuring that only authorized entities can view sensitive routing data. BGP routers can upload routing reports to IRV servers, allowing for the detection of misconfigurations and monitoring the overall health of the network. Combined with the origin verification of UPDATE messages, IRV can provide some form of defense against protocol manipulation attacks. Nevertheless, IRV introduces a lot of overhead because it requires nearconstant querying of previous ASes, however, performance can be somewhat improved by caching previous queries and storing previous routing information to allow for debugging and failure detection. At the same time, IRV has limitations when it comes to its scalability and its adoption, since path verification requires both ASes of a pair to have implemented IRV, while a functioning network must exist for IRV to be widely deployed [2], [4].

4.3 *Secure-BGP*

Secure BGP (S-BGP) is the earliest comprehensive routing security solution specifically developed for BGP. The way S-BGP implements security is by using two public key infrastructures combined with IPsec and a new path attribute that contains "attestations". Public key infrastructure (PKI) is a framework that assigns and delegates public keys to ASes, enabling the authentication of the users sending digital communications. These keys are distributed through a hierarchy, starting from individual organizations and extending to providers and regional registries, with ICANN at the top. One PKI manages address allocation, verifying that an AS owns the prefix it claims, while the other PKI assigns AS numbers to BGP routers, ensuring that a BGP router belongs to the AS it claims to belong to [1], [2].

An AS that claims ownership of a certain prefix is called an attestation and is given a digitally-signed statement called address attestation (AA). An AA consists of a single AS and a set of IP prefixes and is signed by the resource holder. These AAs are distributed out-of-band and verified through a certificate chain from the origin AS to IANA. While AAs prevent (sub)prefix hijack attacks, they do not address AS path modifications. To counter this, route attestations (RAs) are included in UPDATE messages. Each router along the path signs the RA, which includes signatures from all previous routers on the path. RAs primarily protect the AS path attribute but can also secure other BGP attributes, such as the MED. S-BGP also uses IPsec, specifically the Encapsulating Security Payload (ESP) protocol, to ensure authentication, data integrity, and anti-replay for all BGP traffic between neighboring routers. The Internet Key Exchange (IKE) protocol is used for key management supporting ESP. The S-BGP PKI includes separate certificates for IKE, distinct from those used for RA processing [4], [7].

Although S-BGP addresses many BGP threats, it introduces significant computational costs and performance issues that hinder its adoption. Attack strategies that manipulate an AS's export policies could still reroute traffic effectively, demonstrating that S-BGP does not protect against protocol manipulation attacks. The fact that effective attack strategies were already devised before the solution saw widespread adoption undermines the benefits of implementing S-BGP. Additionally, the hierarchical structure of PKIs introduces a single point of failure for the Internet, making its proper functioning dependent on the availability of PKIs. An attacker who successfully targets this single point could cause severe disruptions to Internet accessibility. These factors combined make the protocol impractical, preventing its widespread adoption [1].

4.4 *Secure Origin BGP*

Secure Origin BGP (soBGP) was developed to address BGP vulnerabilities by allowing administrators to balance security and protocol overhead according to their configuration preferences, without requiring full centralization. Similar to S-BGP, soBGP employs a PKI with three types of certificates. The first certificate type binds a public key to each soBGP-speaking router. The second certificate type links an ASN to a set of prefixes that the AS is authorized to advertise. The third certificate type provides details on routing policy, including configured protocol parameters and the local network topology. This information enables a soBGP router to build a topology database that reflects the router's network view, which is essential for validating incoming UPDATE messages. If the AS path in the UPDATE message contradicts the router's topology, the route is dropped [2], [4].

Compared to S-BGP, where AAs are distributed out-of-band, soBGP distributes the certificates for origin authentication in-band between peers using a new BGP message type called SECURITY. On the other hand, the other two certificate types are distributed out-of-band. The key difference between soBGP and S-BGP in terms of path authentication is that S-BGP's route attestations are dynamic—they accompany every BGP UPDATE message, providing recipients with a real-time view of the message path. In contrast, soBGP's approach involves a fundamentally static topology graph and database, which only update when a new policy certificate is issued. Consequently, when an UPDATE is received, the path it took might not be accurately reflected in the peer's topology database [2], [4].

The amount of security provided by soBGP is directly related to the number of ASes that deploy it. By using the topology created from policy certificates, ASes that deploy so-BGP can consistently verify the next hop in the AS path. Additionally, ASes running soBGP can exchange their certificates with each other, even without direct connections, enhancing their understanding of the topology and the ownership of prefixes. Consequently, the security of routing improves as more ASes adopt soBGP. Even though soBGP allows for benefits through incremental deployment and security without a central authority, the correlation between deployment benefits and the number of adopting ASes means that the security benefits of a single AS deploying soBGP are minimal. This is likely a key reason why soBGP has not achieved widespread deployment [1].

4.5 *Pretty Secure BGP*

The Pretty Secure BGP (psBGP) system introduces an address origin authentication service based on a decentralized trust model between ASes, while a centralized trust model is used for AS number authentication. For authenticating AS numbers and public keys, psBGP uses PKIs. Unlike S-BGP, where the PKI is centralized under ICANN, psBGP places the Internet Regional Registries (IRRs) at the top of the certificate hierarchy. This approach mitigates the risk of a single point of failure for the entire Internet, reducing it to a single point of failure per continent. Additionally, each AS generates a prefix assertions list (PAL), which is used to validate whether an AS is authorized to originate a particular prefix. A PAL contains the prefixes delegated to the AS and a list of IP prefix ownership assertions for its neighbors. To verify the authenticity of an origin AS, a BGP router checks the consistency between the PALs of the origin AS's neighboring ASes [1], [4].

Even though psBGP is more secure than soBGP as it performs integrity-based path verification, and it is less centralized than S-BGP and uses fewer certificates, especially for BGP router authentication, it needs to be widely adopted to provide any security benefits, especially due to the requirement of peers to have PALs to verify prefix ownership of a participating AS. Only ASes that deploy psBGP have these PALs. As such, for psBGP only those ASes are actually trustworthy when it comes to prefix authentication. The lack of PALs is problematic for the protocol's deployment since it requires a substantial amount of ASes to already have deployed the solution in order for it to have any real security benefits [1].

4.6 *BGPsec*

In addition to the substantial protocol overhead caused by S-BGP, soBGP, and psBGP, a major challenge to their implementation is the absence of a global Public Key Infrastructure (PKI). The Resource Public Key Infrastructure (RPKI) offers a global PKI for origin authorization, similar to S-BGP, by providing a trusted mapping from prefix sets to ASes. Consequently, RPKI can only protect against prefix hijacking. Unlike a standard PKI, RPKI certificates are designed to verify ownership of specific resources and not identities. This means RPKI provides authorization but not authentication. Due to the lack of authentication, other entities can assume the role of the certification authority (CA) [1], [4].

While RPKI helps limit (sub)prefix hijack attacks, it does not prevent AS path modifications. BGPsec is a security proposal that leverages RPKI to offer route authentication. It enables ASes to use their certificates to sign the routing information received from the previous router, including the AS number it belongs to and the AS number of the next router on the path, and includes this information in the message. To validate a received message, ASes can consult the RPKI to verify that an AS owns the prefix it claims. BGPsec also periodically refreshes routers' certificates and re-sends UPDATE messages using the newly generated certificates to maintain routing stability and mitigate replay attacks by authorized routers [1], [4].

The main vulnerability of BGPsec, and the reason it is not actually deployed, is that in order to do origin authentication and path authentication it requires a comprehensive update to BGP, since data is transmitted between all ASes in UPDATE messages. Additionally, research has indicated that even with full implementation of both RPKI and BGPsec, BGP would still be vulnerable to attacks such as path alterations. Similar to S-BGP, the existence of known attacks against a non-deployed solution undermines the potential benefits of implementing the solution [1].

4.7 *Secure Path Vector*

To maintain low protocol overhead while securing BGP, symmetric cryptography can be employed. One effective method for path validation is the use of nested message authentication codes (MACs). A message authentication code (MAC) is an unforgeable tag attached to a message that ensures the integrity (proof that the message has not been tampered with) and authenticity (proof that only a party with access to a specific secret key could have created the MAC). It is generated by computing a function that takes a secret key and the message as inputs, producing a tag. The recipient, who also knows the secret key, can compute the same function to verify if the MAC matches the one sent with the message. A common method for generating a MAC is the HMAC variant, which utilizes a cryptographic hash function. In practice, an origin AS generates a MAC by combining an initial authenticator value with its prefix and adds the MAC to an UPDATE message. Each subsequent AS then creates a new MAC using the MAC from the incoming announcement. Each new MAC includes the data received and the authenticator value of the previous router. When an UPDATE message is received, the validator uses all known secret keys to recursively verify the announced AS path [2], [4].

The Secure Path Vector (SPV) protocol is an improvement over the previous method that uses a sequence of one-time off-line signatures. In SPV, the signer performs computationally intensive cryptographic operations beforehand, allowing the actual signing process to be faster. SPV operates alongside BGP with the primary objective of verifying path integrity using only symmetric cryptographic primitives. It is important to note that path authentication inherently includes origin authentication since every path has an origin that must also be authenticated, although this aspect does not rely on symmetric cryptographic functions. Despite its advantages, SPV introduces significant computational overhead due to the intensive cryptographic operations required, as well as network overhead because a substantial amount of state information must be transmitted and processed. Finally, SPV does not provide protection against AS path forgery and collusion attacks [1], [4].

Conclusion

Even though the BGP protocol is fundamental piece for internet routing, it has significant security vulnerabilities that threaten the reliability and the correct operation of the Internet as a whole. Its trust-based design makes it vulnerable to attacks like prefix hijacking, protocol manipulation, Denial of Service and AS path forgery. These weaknesses can result in serious consequences, including traffic interception, data breaches, and widespread network disruptions.

Efforts to enhance BGP security have been proposed, including overlay network solutions such as IRV, asymmetric cryptographic methods such as S-BGP, soBGP, psBGP and BGPsec, and symmetric cryptographic methods such as SPV. These methods, however, either eliminate most of the BGP threats at the cost of additional computational and network overhead, or sacrifice security goals to achieve performance. For example, they often fall short in addressing potential threats, such as AS path forgery and collusion attacks.

Despite the development of various BGP security solutions, none have been widely deployed to protect the entire internet. This is partly because BGP security solutions have evolved to eliminate protection against threats deemed less important, focusing instead on reducing overhead for critical threats. Another reason, however, is the large adoption of these solutions required by ASes, since some of these security solutions have to be implemented in multiple ASes in order to be effective, which makes them impractical to use.

Ultimately, the ongoing challenge lies in balancing enhanced security measures with the need for efficient and scalable network performance, without the need for required mass adoption beforehand in order to be effective. Future research must continue to explore innovative solutions that can provide robust security for BGP without compromises. With the threat landscape evolving over time, collaboration among network operators, researchers, and policymakers is essential to develop and implement comprehensive security frameworks that can protect the global internet infrastructure from evolving threats. The security of BGP is necessary to ensure the reliable and flawless operation of private and public communication.

References

[1] T.R. van Rossum, "BGP security and the future: A meta-analysis of BGP threats and security to provide a new direction for practical BGP security," 2021.

[2] T. R. P. M. J. R. Kevin Butler, "A Survey of BGP Security Issues and Solutions," 2010.

[3] T. F. P. M. J. R. Kevin Butler, "A Survey of BGP Security," 2005.

[4] A. P. T. E. Asya Mitseva, "The state of affairs in BGP security: A survey of attacks and defenses," 2018.

[5] D. M. ,. R. S.-G. ,. X. M.-B. M. Y. M.S. Siddiqui, "A survey on the recent efforts of the Internet Standardization Body for securing inter-domain routing," 2015.

[6] B. M. Martin O. Nicholes, "A Survey of Security Techniques for the Border Gateway Protocol (BGP)," 2009.

[7] Stephen T. Kent, "Securing the Border Gateway Protocol," 2003.