Interdomain Routing Security (BGP-4)

A Comparison between S-BGP and soBGP

Rostom Zouaghi

Technical Report

RHUL-MA-2009-01

16th February 2009

Department of Mathematics

Royal Holloway, University of London

Egham, Surrey TW20 0EX, England

http://www.rhul.ac.uk/mathematics/techreports

ROYAL HOLLOWAY, UNIVERISTY OF LONDON

Interdomain Routing Security (BGP-4)

A Comparison between S-BGP and soBGP

Rostom ZOUAGHI

Supervisor: Dr. Stephen Wolthusen

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature:

Date: **5th September 2008**

Abstract

The Border Gateway Protocol (BGP) is the most important protocol for the interconnectivity of the Internet. Although it has shown acceptable performance, there are many issues about its capability to meet the scale of the growth of the Internet, mainly because of the security issues that surround interdomain routing. The Internet is important to many organisations in various contexts. Thus, it is required to provide a highly secure protocol to keep the normal operation of the Internet. BGP suffers from many security issues. In this dissertation, we cover those issues and provide the security requirements for this protocol. We enumerate the numerous attacks that can be conducted against BGP. The aim of this study is to examine two considerably discussed protocols. Secure-BGP (S-BGP) and secure origin BGP (soBGP) have shown a revolutionary view on interdomain routing since they endeavour to providing security mechanisms at the protocol level. The objective is extended to comparing these two solutions by examining their contribution to the Border Gateway Protocol in terms of security. Moreover, we study their interoperability, efficiency, performance, and the residual vulnerabilities that each solution failed to resolve. Our findings have revealed that ultimately, the solution chosen will be dependent on the desired level of security and deployability. As is often the case with security, a compromise between security and feasibility is of a major concern and cost-effectiveness is the main driver behind deployment.

Acknowledgements

I would like to take this opportunity to thank the following persons for their input, help and support:

- My project supervisor at Royal Holloway: Dr. Stephen Wolthusen.
- Dr. Chez Ciechanowic and Dr. Peter Wild for their support throughout this MSc.
- Fellow ISG students in the MSc programme at Royal Holloway, University of London.
- Last, but not least, my parents and family for their kindness, support and encouragement.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

The Internet has become a fundamental resource in academic institutions, government agencies and small to large businesses, as well as a vibrant part of our daily lives. At the present, the Internet connects millions of users across the globe. It has become the underpinning for commercial enterprises and a strong scientific tool. This large network of networks requires the interconnection and collaboration of a significant number of autonomously controlled networks. Paying for the service, users expect to reliably communicate with other clients or servers active on the Internet whenever desired. Electronic-commerce (e-commerce) based companies rely totally on the Internet such as eBay, Amazon, etc. According to a Shop.org / Forrester Research study conducted in 2008, online retail sales raised this year by approximately 17% reaching $204 billion. This is an instance of the criticality of the Internet to many companies.

The good functioning of communication in the Internet relies on routing, which is the component that determines feasible paths (or routes) for data to flow from a source to a destination. Computers in the Internet depend on routing data in order to be able to discover and communicate with each other. Currently, the Internet routing infrastructure is intolerably frail due to many shortcomings. It is commonly misconfigured [1]. Moreover, it has considerably weak security properties [2]. In addition, it is hard to manage [3]. As a consequence, communication becomes unreliable and unpredictable.

In this chapter, we cover the basics of Internet routing. Moreover, we describe the hierarchical structure and addressing of the Internet. Then, we identify the configuration issues that occur to interdomain routing and their impact on the Internet. Finally, the security issues that surround the routing infrastructure and the Internet itself are broadly covered. Then the aims of this dissertation are defined in the conclusion.

1. INTERNET ROUTING OVERVIEW

Although it is generally thought that the Internet is a single network that people connect to; it is however composed of a large number of interconnected networks that are independently operated, called **Autonomous Systems** (ASes). For instance, when a user makes an HTTP request to a server in a different network, data travels across multiple ASes before reaching its destination, as shown in Figure 1.1. Technically, an AS represents an internetwork or a collection of networks and routers, controlled by one entity. Sometimes, these ASes have competitive objectives but they must collaborate with each other, by exchanging routing information, in order to realise large-scale and universal connectivity.

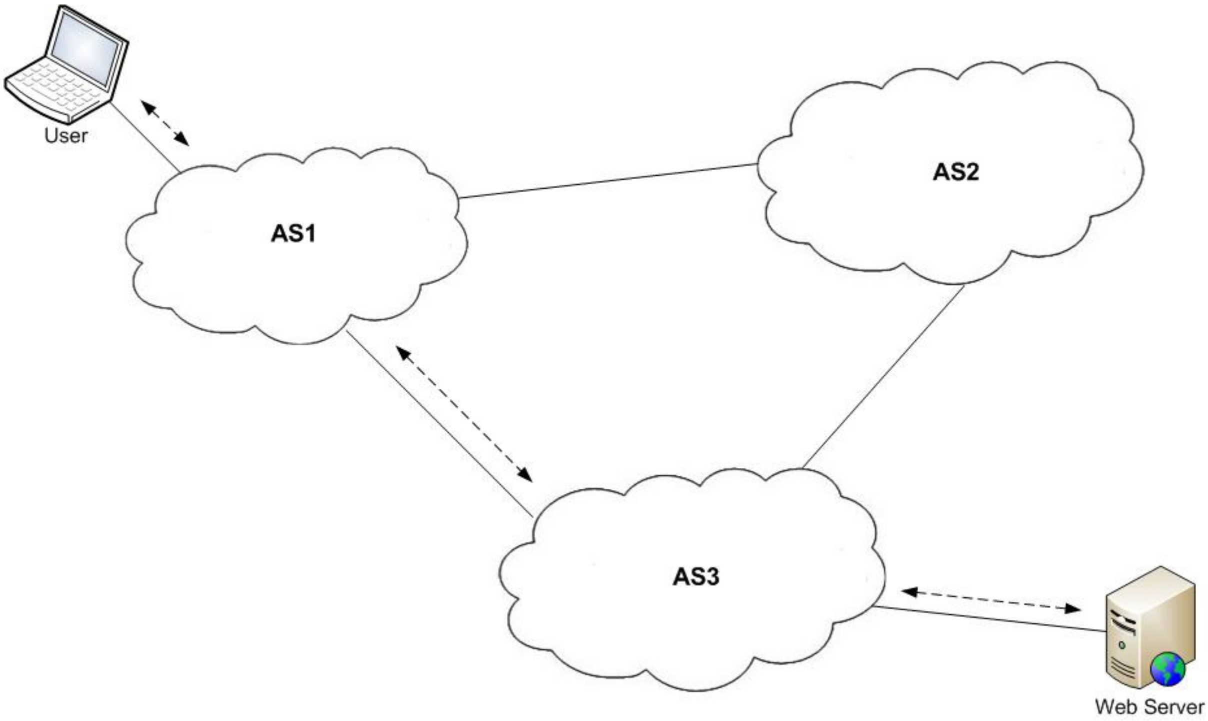


Figure1.1: An Internet path traversing multiple ASes

Within an AS, routing is applied and controlled internally by the owner through internal routing protocols. It ensures correct connectivity and reachability of nodes across the AS for internal communication. After correct configuration, **Interior Gateway Protocols** (IGPs) are used for automated routing information update. They ensure that routing information present at each router is most reliable and cost-efficient with respect to the metrics used to quantify the cost. A few examples of such protocols are: RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), and EIGRP (Enhanced version of IGRP). While interior routing handles packets travelling from an internal source to an internal destination, data flowing outside an AS or sourcing from an external AS cannot be routed via IGPs. The information required for such scale is out of internal routing's reach. For such traffic, more information and flexibility is required because of the restrictions that can be met in other ASes. Furthermore, IGPs' design cannot scale within internetworks as large as the Internet. Thus, more data needs to be used for routes that travel along different autonomous systems.

The solution is External Gateway Protocols (EGPs). This type of protocols uses higher level abstract data to define routes between different ASes. An analogy for this can be identified when someone travels to another country by route; and they know through routing information provided that they have to travel across different countries to get to the destination. Then, in each country more data is provided on routes to get to the border to pass to the next country and so on. Moreover, every country has its own policies concerning its border and the type of nationalities or persons allowed in the country. The countries represent autonomous systems and people travelling are packets flowing. Every AS has a number of routers used for routing information within the AS and some are defined to be the border routers that send traffic to, and receive it from neighbouring ASes. These domains (i.e. ASes) have different policies set by the owners via filters created accordingly using different parameters present in the routed traffic. Every router that is a speaker of the interdomain routing language can communicate with its peers in the neighbouring ASes. They exchange routing information on the reachability of different autonomous systems.

The current interdomain routing protocol on the Internet is the Border Gateway Protocol (BGP) [4]. Global reachability between ASes is established by setting up BGP sessions between their border routers. Then, they exchange reachability information to different ASes in the Internet. Every AS may have between a single to hundreds of routers. Every router selects the best route to each destination. Routing in the Internet is destination based, where every router selects the next hop (i.e. router) to forward traffic to, based on the packet's destination IP address [5]. More details on BGP are addressed in Chapter 2. Routers within an AS must use an IGP to discover the path to the router which one of its interfaces is pointing to the next hop AS. Internal routing protocols are not discussed in this dissertation. Other work provides more detailed treatment [6, 7, 8].

2. INTERNET ADDRESSING AND AUTHORITIES

Communication on the Internet is based on IP addresses and AS numbers. IP addresses are 32-bit numbers; usually each byte is separated by a dot and represented in a decimal integer. For example, the 32-bit binary 01111101 10100011 00101101 00100010 would be represented by 125.163.45.34. Since an IP address is 32-bit long, one may think that there is a limit of about 4.2 billion (2^{32}) on the number of hosts that can be supported. In practice and due to address reservations and assignments which are part of the addressing system, the maximum size is lower but using a few technologies such as NAT (Network Address Translation), provides support for larger Internet [9].

Institutions in the Internet are assigned these IP addresses in a contiguous manner (i.e. blocks of neighbouring addresses). They are represented by the first address and a mask length. This is a method identified by the Internet Engineering Task Force to eliminate classful addressing and start the new **Classless Inter-Domain Routing** (CIDR) approach [10, 11]. It is a method used for assigning IP addresses without relying on the standard IP address classes (e.g. Class A, Class B, etc). It introduces a flexible mask that reflects the size of the network and network ID. In classful, the network ID element could only obtain a predefined number of bits: 8, 16 or 24. In classless, the number of bits is flexible and varies depending on the mask. For example, the prefix 164.0.2.0/24 with a mask 255.255.255.0 contains all the addresses where the first 24 bits represent the network ID and remain static, and the last 8 bits represent the different addresses that can be allocated to different hosts in the network (i.e. from 164.0.2.0 to 164.0.2.255). For this example, 254 hosts can be allocated in this network because the first address represents the network address (i.e. following our example, the network address would be 164.0.2.0) and the last one is the broadcast address (i.e. 164.0.2.255 from our initial example). Instead of storing routes for every address, this type of allocation (i.e. CIDR) results in smaller routing tables. This leads to a smaller number of route advertisements, since the routers need only to identify the network segment of the address and forward it accordingly.

Public IP Addresses were originally assigned to different regions in the world by the Internet Assigned Numbers Authority (IANA), and then by the Internet Corporation for Assigned Names and Numbers (ICANN). IANA is responsible for global management of the IP addressing systems used for routing Internet traffic. IP addresses are usually assigned in a hierarchical way. Internet Service Providers (ISPs) assign IP Addresses to users. They obtain allocations of IP addresses from a Local Internet Registry (LIR) or National Internet Registry (NIR) or from their Regional Internet Registry (RIR). As shown in Figure1.2, there are five RIRs maintained by IANA in different regions of the world: North America Region (ARIN), Latin America and some Caribbean Islands (LACNIC), Africa region (AfriNIC), Europe, The Middle East and Central Asia (RIPE NCC), and Asia and Pacific Region (APNIC). IANA only provides additional allocations of IP Addresses to RIRs when required. It does not deal directly with ISPs or end users only in exceptional circumstances such as allocation of multicast addresses or other protocol specific needs. Lately, ICANN started to delegate this responsibility to these regional registries. Thus, allocation of IP addresses and AS numbers is done regionally.

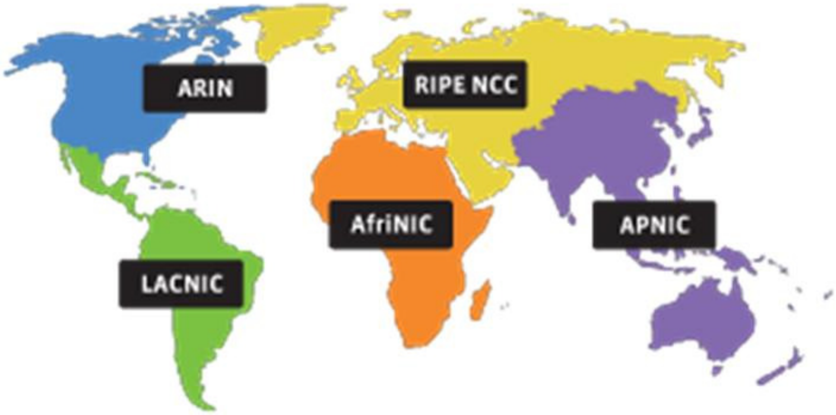


Figure1.2: IANA's Regional Internet Registries (RIRs)

More information is required for interdomain routing to scale with the Internet's growth. Autonomous Systems are entities, part of the routing information in the Internet. They group together a number of IP prefixes, which are under the same administrative control and conform to the same routing policy. Therefore, they are assigned numbers named **Autonomous System Numbers** (ASNs). ASNs are 16-bit numbers and similar to IP addresses, they are assigned by ICANN as the highest authority or its delegates, the different RIRs. Multiple organisations can use private ASNs to route its packets to the ISP using inter-AS routing. These private ASNs can vary from 64512 through 65534. However, the ISP must officially register its AS number. Public ASNs are allocated from 1 to 64511. The AS numbers 0, 54272 to 64511, and 65535 are reserved [12]. Therefore, customer ASes are provided with private AS numbers for interdomain communication with their provider. Then, the latter would advertise the routes for the customers not including their private ASNs but its public AS number(s).

3. Configuration Issues

Interdomain routing involves a large population of interconnected entities, mainly communicating with messages through a set of rules and "etiquette" forming a protocol. Because of the large scale of the internet, interdomain routing protocols and mainly the Border Gateway Protocol (BGP) become rather complex. This makes the configuration of these protocols vastly a critical part. Moreover, any small error can lead to devastating consequences. Through configuration, these protocols become rather flexible and allow organisations to meet further requirements around accepting, rejecting, forwarding traffic and more. With configuration, an AS is able to choose the ASes to carry traffic for [61], the way traffic enters and leaves the AS [62], the way its routers learn routes to external destinations.

Business demands and changes that occur at a higher frequency in the Internet may also change routing information and traffic patterns. Coupling the latter with the complexity of configuration, administrators become frustrated when they have such responsibility. Human error is highly predictable in these situations. Thus, configuration issues have happened and caused, as envisaged, problems to the Internet community. In 1997, a minor ISP in the USA, and more precisely in Florida, caused all Internet traffic to be routed through it due to a misconfiguration [63]. This led to the entire Internet going down for a while. This is one of the major damaging misconfiguration in the history of the Internet. Another one happened in 2002, where US telecom giant WorldCom brought down 20% of the nation’s Internet backbone in USA as reason of a misconfiguration problem [64]. Although configuration issues are not the main concern of this dissertation, they prove the fragility of interdomain routing. More information on misconfiguration issues can be found in this PhD thesis [65].

4. Security Issues

The Internet was designed for communication purposes and the security concerns were not part of the requirements and the design process. Thus all interdomain routing was not secure; but fulfilled to some extent the communication between Autonomous Systems. Although some exterior routing protocols have proven to be stable, there are still some serious thoughts on whether they will still be able to handle the rapidly growing Internet. Well known exterior routing protocols could be the target of attacks that could disorder Internet Services, such as the de-facto standard BGP.

After glimpsing on misconfiguration issues, it was realised that interdomain routing, at its state, is highly fragile and vulnerable. If it is as such to human error, these issues can be used maliciously by an attacker. This means that the adversary is able to conduct an attack that might aim at projecting a similar behaviour to a misconfiguration. Thus, interdomain routing suffers from serious security issues. As covered before, these protocols rely on message exchange. These messages are not protected from many violations. The first is Integrity. Interdomain routing does not provide integrity services in its messages making it vulnerable to undetected altering of data. Furthermore, source authentication of data is not supplied. ASes do not have a security mechanism to prove their identity and the address space they use. Furthermore, routers within those ASes cannot verify and validate other ASes. Last but not least, the authenticity of the routing information is not protected. This means that it can be altered or created by a malicious individual. These security problems prove that interdomain routing is miles away from reaching concrete stability.

5. Conclusion

The Internet has become a crucial part, if not the spine, for most companies and businesses. Thus, internetworking is the backbone for the operation of both corporate and non-corporate networks. The raison d'être of internetworking is Interdomain routing; the latter is ubiquitous and underpins all internetworks including the Internet. Thus, efficiency, performance, reliability, and stability of the protocols used for routing are tight requirements that should be considered at all times. The issue that arose was that security in routing was not considered from design to implementation and deployment, consequently making these protocols exceptionally vulnerable to attacks. Due to their complexity, current research is more focused on optimising them for the expanding Internet rather than securing them. Moreover, routing security failures happen despite good order and functioning of protocols. The problems are generally caused by malicious participants and also due to misconfigurations. The issue of routing security is typically outside the scope of traditional communication security. Also, adding security needs to be less resource consuming, which means that performance and efficiency are always prerequisites.

In this dissertation, we aim at providing a comprehensive approach at defining the security issues that concern interdomain routing. Then, by providing a few solutions, this will give us the ability to analyse and compare them. The solutions chosen are Secure-BGP (S-BGP) and secure origin BGP (soBGP). This choice was made because of the high focus of the research community on these two protocols. They both aim at providing a certain level of security to the de-facto standard of interdomain routing: BGP.

At first, an overview of BGP-4 is covered. This provides the reader with the required background knowledge to understand the interdomain routing in more depth. Then, a threat analysis of BGP is conducted. This covers its vulnerabilities and potential attacks and attack scenarios against it. Followed by the latter is a chapter dedicated to BGP security. It supplies the reader with some current practices to secure BGP and the security requirements for the protocol. After that, we examine two solutions that aim at securing interdomain routing. Then, we provide an analysis of their level of security and performance in a large scale. Furthermore, deployments and backward compatibility issues concerning both solutions will be covered. Finally, we end the dissertation by providing a conclusion and future work that should be focused on, in the next few years.

Chapter 2

OVERVIEW OF BGP-4

AS illustrated before, the Internet is composed of **Autonomous Systems** (ASes). Internally, the latter use interior routing protocols such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol), EIGRP (Enhanced version). ASes are connected together through exterior routing protocols in order to form larger internetworks and especially the Internet. Border Gateway Protocol (BGP) is the most important protocol that is holding the interconnection and communication between different ASes in the Internet. In this chapter we provide an overview of BGP. Firstly, we cover its topology and main entities that are required for its functioning. Then, we cover the different traffic types that are found in interdomain routing. After that, storage and advertisement of routing information is illustrated. Then, we explain the algorithm behind BGP. Finally and in the last section, we examine the different operations included in the protocol and messages used for exchange of routing information.

In the early Internet, routers communicated differently than today. There were some centralised routers functioning as a core AS, using the Gateway-to-Gateway Protocol (GGP) for internal communication and Exterior Gateway Protocol (EGP) for inter-core AS communication. When the Internet expanded into an AS oriented architecture, EGP had still the ability to function and handle the communication. Thus, EGP (Exterior Gateway Protocol) was still operational as an exterior routing protocol for ASes and the Internet. However, it had some weaknesses that affected its routing ability while the Internet was rapidly expanding. When the number of ASes grew, the importance of the data flow similarly grew. Thus, the necessity of developing a new protocol that could scale well within the fast growing Internet was critical. In June 1989, the first version of the Border Gateway Protocol (BGP) was developed and published in RFC 1105 [13]. The current standard for BGP is BGP-4 RFC 1771 [14] which came after BGB-2, BGP-3 and a first version of BGP-4. BGP-4 has additional defining standards, RFC 1772 [15], 1773 [16], 1774 [17]. Then, a few modifications were updated to BGP-4 and published in January 2006 in RFC 4271 [18], making RFC 1771 obsolete.

BGP, in one sentence, is used to first exchange reachability information between ASes. Then, that information is used to determine routes to different networks. In each AS, one or multiple routers are assigned to perform interdomain routing by running BGP software in them. BGP routers are internally (i.e. inside the AS) linked between each other and externally with different BGP routers in other ASes. Every router stores routing information in a set of **Routing Information Bases** (RIBs). This information is propagated across the whole internetwork. This will allow reachability information to be available everywhere, which ensures that every node in the internetwork knows how to reach any other node.

Moreover, BGP is able to handle non-uniform AS topology. This means that ASes can be randomly connected and not affecting the running of the protocol. Moreover, ASes must have at least one BGP router but may have as much as required. BGP is required and does scale with random topologies of autonomous systems. Because of this flexibility, route determination and selection structure is rather more complex. The protocol uses more than what is required for other routing protocols which is only the next hop, such as RIP. Instead of using a distance-vector approach, BGP applies a **path-vector** protocol. The routers use more information about the entire path which is represented by a chain of interconnected ASes. The scale of interdomain routing is so large that it requires cautious route decisions. Hence, the algorithm that will define the best route will need to direct its attention to reliability rather than the cost and efficiency. It will focus on the avoidance of router loops and other error conditions. Furthermore, route selection relies on the BGP policies applied at each AS and if traffic can flow without being filtered out. The update of tables and other operations are based on the exchange of messages achieving different tasks. These different BGP messages will be explicated in detail later in this chapter.

BGP is a very important protocol and the de facto standard for interdomain routing. Before being able to analyse the security issues of this protocol, it needs to be defined and analysed accordingly to find the different holes that make this protocol extremely vulnerable to different attacks. First, BGP topology will be illustrated with the different entities that are required for the protocol to function. Then, the data storage and processing by the routers will be examined. Furthermore, an algorithm overview and the data required will be covered. Last but not least, BGP detailed messaging and operations will be analysed, since they remain the weakest link in terms of security for interdomain routing.

1. BGP Topology

One of the most important features of BGP is its flexibility. It can handle a full mesh topology (i.e. every AS is connected to all other ASes), a series of simultaneously connected ASes or any other type of arrangement. A more interesting observation is that it is also able to handle changes in topologies that can take place over time. A pertinent remark to note, BGP has a prerequisite assumption which reflects the fact that it is not responsible for the traffic when it flows inside ASes. For BGP, an AS is autonomous and applies to the fullest the fact that it is controlled by an independent owner of that AS. So, BGP does not rely on the internal topology of the AS; and only uses the information transmitted to it from the AS and distributes it to other ASes.

BGP Speakers

In interdomain routing, routers, in ASes, connected with other routers in other ASes are called **speakers**. This is because they speak the same language which is exterior routing, following the same protocol which is BGP. They are in a way the representatives of ASes in the borders. There are two types of routers in every AS. **Boundary routers** are those which use interior routing such as OSPF. Those that use exterior routing (e.g. BGP) are **border routers**. Interconnected BGP routers from bordering Autonomous Systems are **neighbours**. They are two border routers representing their ASes allowing flow of packets between the two entities. An AS can have more than one BGP router. These routers are **Internal Peers** using what is known as **Internal BGP** (IBGP). The other type occurs when the routers are neighbours in different ASes. They are called **External Peers** and use **External BGP** (EBGP). They are both similar but differ slightly, and the difference will be explained further in this chapter. As shown in Figure2.1, router R1 shares an external link with R2. The link is a physical medium link and does not relate to the BGP session established, which is an EBGP session for this case because it is between neighbouring ASes. However, R1 shares an internal link with R2 which will be used to establish an IBGP session. R3 and R4 do not share a link but they will be able to set up an IBGP session to propagate routing information coming from external peers. The link here is a physical medium from the physical layer in the OSI model or the TCP/IP architecture.

Traffic Flow and Traffic Types

In general, there is always a high-speed, high-capacity AS that serves and accepts carrying other ASes' traffics. This can happen only if arrangements have been made prior to allowing traffic flow through an AS. There are different types of traffic flowing in interdomain routing. The traffic flowing within an AS which either originated in the same AS or delivered by another AS is the **Local Traffic**. **Transit Traffic** is the traffic flowing within an AS that originated from another AS and intended to be delivered to another AS.

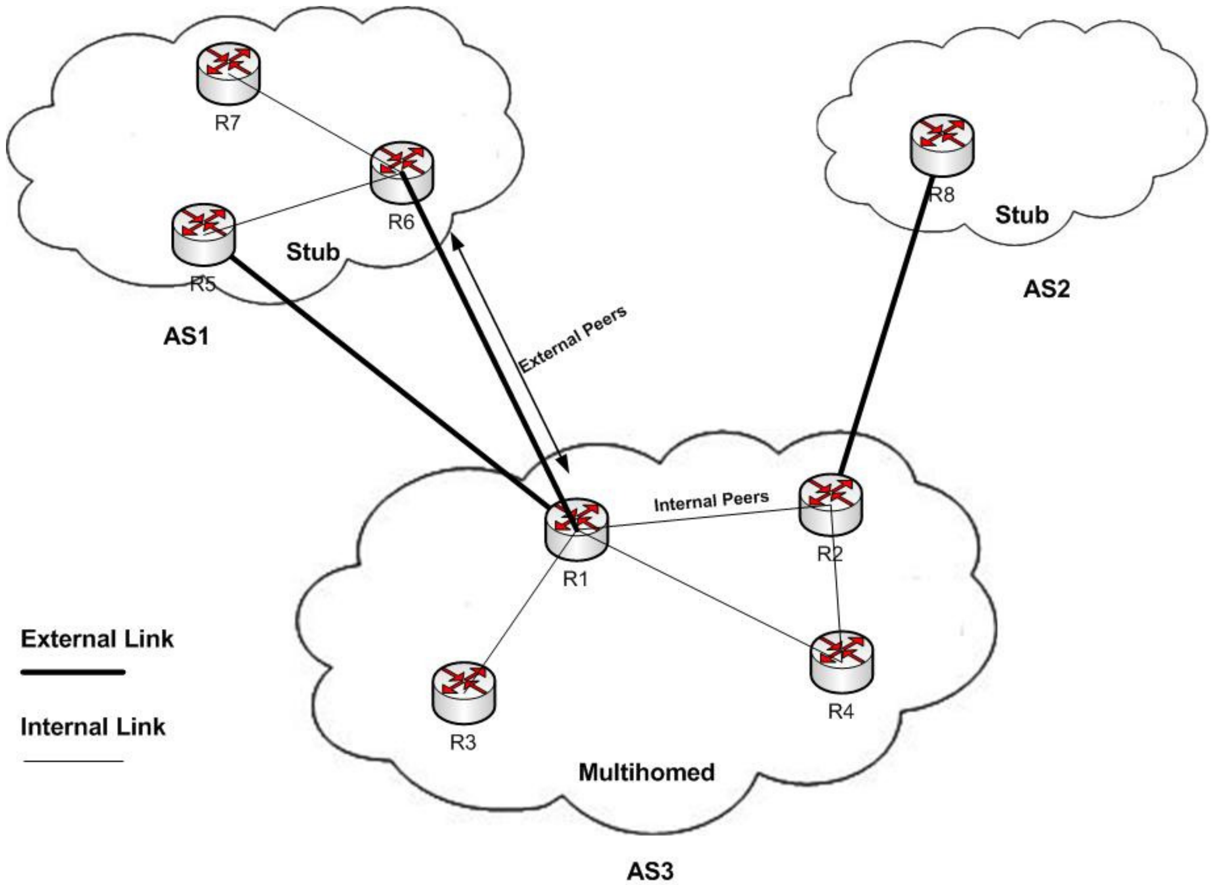


Figure2.1: An Example of a BGP Topology

An ISP, in general, has many ASes connected to it that use its services to reach the Internet. Some ASes in an ISP allow transit traffic to flow inside them. These are **Multihomed** ASes. A Multihomed AS is an AS that is connected to more than one AS and traffic can be transit or local. Due to some policies in certain domains, some ASes may not allow transit traffic. These are **Stub** ASes. A Stub AS is an AS that is connected to only one AS and the inbound traffic is always intended for the AS itself (i.e. only allows local traffic). As shown in Figure2.1, AS3 is a multihomed AS and allows traffic to transit. If AS1 sends some data to AS2, traffic will flow from R6 or R5 to R1 via EBGP. Then, traffic will be forwarded internally, within the multihomed AS3, from R1 to R2 through IBGP. Following that, traffic will be forwarded from R2 to R8 using EBGP.

AS Routing Policies

In order for an AS to communicate with another distant AS, its traffic must at least transit through another AS before arriving and the end point. The issue behind that is that many ASes are forced to be used for transit traffic. This will certainly consume resources such as bandwidth, processing and memory, and also can be a threat to the AS. That is why there are routing policies to be configured for each AS in order to control traffic. These policies are non-technical definitions. Moreover, they can be of a political nature, organisational, business context, competitiveness or security measures. This allows the implementation of these policies without relying on central authority. These policies are not part of the BGP protocol. Furthermore, they are configured by the owner of the AS and depending on the organisational policies.

One of the policies that can be implemented is the **No Transit Policy**. This policy would be used when no transit traffic is allowed to flow within the autonomous system. This means that the AS is defined as a stub. To allow more flexibility for a multihomed AS but still restrict some packets flowing from certain ASes, **Restricted AS Transit Policy** can be forced. It will also expose itself only to ASes that are accepted in the policy. Another type of data used to restrict a certain type of traffic is for example time. The latter can be used as a parameter to restrict or allow transit traffic only at certain times. This type of policy is named **Criteria-Based Transit Policy**. The different parameters that can be used allow greater flexibility to the corporate needs of the AS owners.

All these types of policies do not allow greater flexibility. Even if they do, effectiveness and complexity will decrease dramatically if restriction policies increase in each multihomed AS. The issue that can occur from such policies is the decreasing number of Transit ASes. For instance, most ASes prefer, for security measures, to accept only local traffic. That will cause a very slow and inefficient interdomain routing. However, the latter are designed in a way that there will be certain ASes intended to carry large amounts of transit traffic. Some high-speed, high-capacity ASes will play the role of multihomed ones. Moreover, carrying traffic between ASes happens only after certain arrangements have been made.

Storage and Advertisement

The way routing information is processed and stored is crucial to the routing infrastructure. The aim of BGP is to facilitate the exchange of this routing information between external and internal peers. This will allow speakers to determine efficient routes to each network. The main activities of route information management in each BGP router comprise of different tasks. The first task is **Route Storage**. Each router stores routing information about the reachability of other networks. This information is received from other internal or external peers. The information will be stored in a database for later or immediate processing. When a router receives a **Route Update**, it must make a decision on how to use the information. Depending on many parameters, choice of updating the routes is taken. However and before that, the decision process also takes in consideration when and how the information should be used to update the routing information. In addition to this task, there is **Route Selection**. This deals with the selection of best routes using some parameters in the database stored about different routes. The fourth task is **Route Advertisement**. This process is used to propagate the reachability of other network throughout new or updated routes. This is accomplished with the route update process through an UPDATE message, as shown in Figure2.2.

Every BGP router, routinely, stores, updates, selects and advertises routing information to other peers. Routing information is stored in every router in a routing information database named **Routing Information Base** (RIB). When an UPDATE message is received, it is stored in a database named **Adj-RIBs-In**, as illustrated in Figure2.2. The latter holds information received from BGP peers. When such a message is approved, it is stored in the main core database that holds selected routes considered to be valid and best routes to reach a speaker. It is called **Loc-RIB**. When data is received, approved and stored, it needs to be advertised to neighbours. The router takes the relevant information and stores in an **Adj-RIBs-Out** database. This process is based on what is known as **BGP Decision Process**. It is part of the system of Route Update, Selection, and Advertisement. The previous three databases can be implemented within one entity and used differently. Those were a way to define different sections of a database, while they can be physically three separate databases or put together.

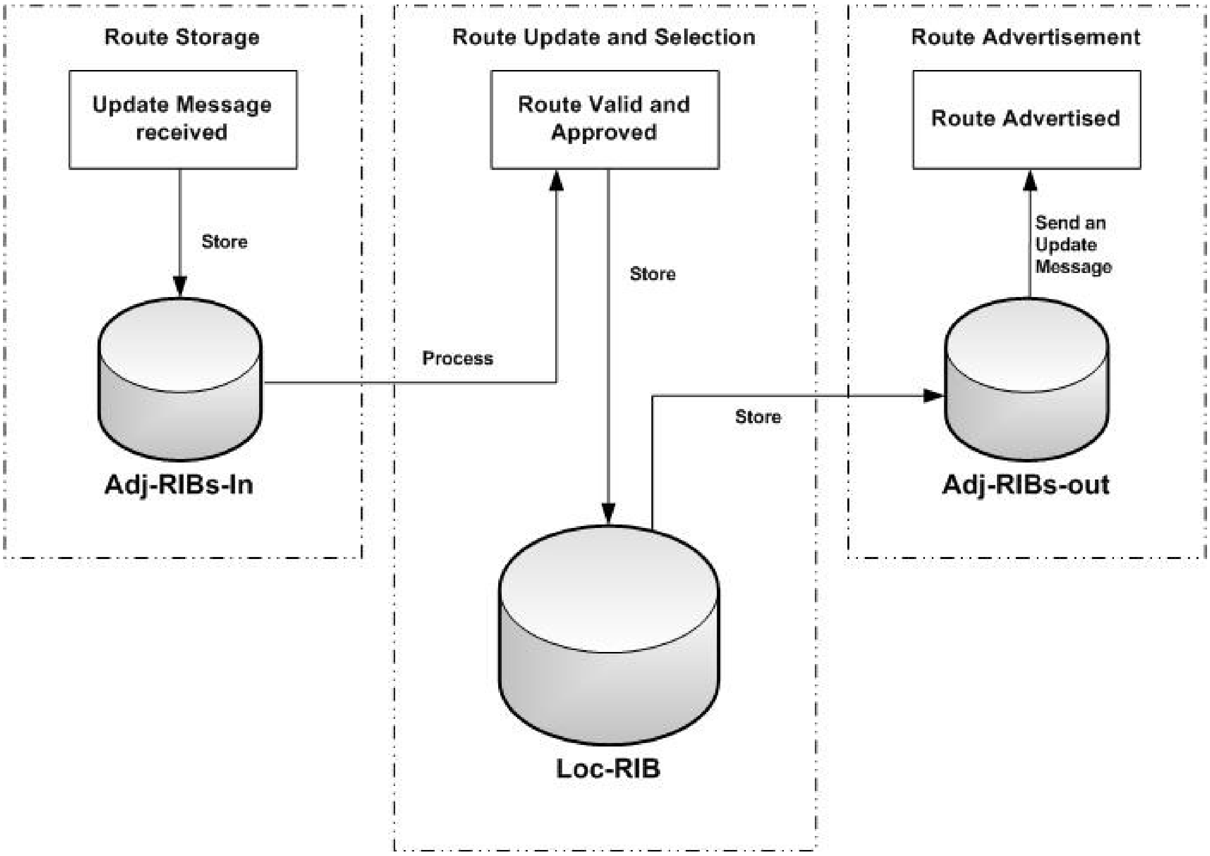


Figure2.2: Route Information Management and Storage in the Route Decision Process

2. Algorithm Overview

As stated before, using simple Distance-Vector or Link-State attributes is not sufficient and can conclude in looping routes or what is called deadlocks (i.e. Infinite loops), since the topology of interdomain routing is in some way random or arbitrary. It is, therefore, necessary to know more than the next hop. By storing the characteristics of the entire path, there is a possibility to know how to compute and change routes. So, BGP advertises networks as destinations and the path description for reaching those destinations. Such algorithm is known as a **path-vector algorithm** [19]. All this data is stored in the RIB of each speaker. These attributes are categorised depending on their importance.

The first type is **Well-Known Mandatory**. These attributes must be recognised and known by every speaker. They, also, must be included in all messages sent, be it route description or UPDATE message. The second is **Well-Known Discretionary**. These are attributes that must be known but may or may not be included in UPDATE messages; meaning they are optionally for the sender but mandatory for the receiver. The third type is **Optional Transitive**. These attributes are optional to be known and sent by a speaker. However, if received, they must be passed on even if not understood or recognised by the speaker. The last one is **Optional Non-Transitive**. These are similar to the previous ones (i.e. Optional Transitive); however, when received and not recognised or known, they must be dropped by the receiver.

Standard Path Attributes

Clearly, path attributes are one of the most important features of BGP as they provide the protocol with the flexibility required for such routing scale. These attributes will be defined not in the greatest detail since they will be analysed concerning the security issues that arise regarding them. Table2.1 represents a summary of BGP path attributes found in TCP/IP Guide book [20], page 659.

Attribute	**Classification**	**Type Value**	**Description**
Origin	Well-Known Mandatory	1	Specifies the origin of the path. Whether the path came from an interior protocol, older exterior protocol, or another source.
AS_PATH	Well-Known Mandatory	2	A list of AS numbers that indicates the path to the destination network. It is used to collect

			routes and to detect routing loops.
Next_Hop	Well-Known Mandatory	3	It represents the next hop router to be used to reach the destination.
MULTI_EXIT_DISC (MED)	Optional Non-Transitive	4	When an entry to or exit from an AS includes multiple Entry/Exit points (i.e. More than one BGP router), this attribute is used to discriminate between them (i.e. Choose one exit or entry point over the others).
LOCAL_PREF	Well-Known Discretionary	5	Used in communication between BGP speakers in the same AS to indicate the preference of a particular route.
Atomic_Aggregate	Well-Known Discretionary	6	If a BGP speaker receives a set of overlapping routes, while one is more specific to the other (e.g. One is a subnet of another one), it sets the path attribute to 1 when it uses the less specific one.
Aggregator	Optional Transitive	7	It contains the AS number and BGP ID of the router that performs route aggregation. It is used for troubleshooting.

Table2.1: BGP Path Attributes

BGP Decision Process

A BGP speaker can initiate new routes. It may obtain information on a new route from an interior protocol on an AS. It will then create an entry in its RIB and decides whether to advertise it or not. Moreover, when a router cannot reach a destination, it advertises an unfeasible or withdrawn route to its peers. However, when receiving an UPDATE message containing a new or an updated one, before it is approved, it goes through a decision process. Most of the path attributes are used to decide which route is more adequate to store in the Loc-RIB, then advertise it from Adj-RIBs-Out. This process is part of the route update, selection, and advertisement functions. The process of deciding on which route is best to use is tightly dependent on evaluating the data relating to the path attributes. As shown and described previously in Figure2.2, upon arrival of an UPDATE message, the route information may travel across different logical locations. This data is analysed throughout the decision process. The latter encompasses three phases.

The first phase deals with the analysis of the received data. Whenever new routing information destined from a peer BGP speaker arrives, it is analysed at the Adj-RIBs-In. Then, a preference level is allocated to the route. The preference level is assigned based on various criteria. Since BGP uses path-vector algorithm, the number of ASes between the router and the network is one of them. Evidently, it will have a higher preference level for a route containing fewer ASes in the AS_PATH parameter. Another very important criterion is concerned with policies. Data may reach an AS where its BGP speaker filters the packet out, because it does not allow that traffic based on some policy criteria. Thus, even if the number of ASes is lower does not denote that it is the best path. This is because it cannot guarantee that the end node is reachable through that path. In addition to that, the origin of where the path came from is also a decision factor.

When the level of preference is attached to the route, the best route is selected amongst all similar destination routes in the second phase. The route with the highest preference level is selected. If a set of similar routes (i.e. similar destination prefix and identical prefix length) share the same highest preference level, a tie-breaking rule needs to be applied to retrieve only one best route through other parameters. It first starts by checking that route with the highest LOCAL_PREF value is selected. This degree of preference could have been either selected locally or learnt from another external speaker via an UPDATE message. If this step ends with only one route selected, the tie-breaking decision process terminates. Else, it uses the next parameter which is the AS_PATH. The route with the shortest AS_PATH is selected. Then, if the speaker takes in consideration the MULTI_EXIT_DISC, the route with the lowest value is selected, ensuring that the multiple routes were learnt from the same bordering AS. If this filtering keeps more than one route, the NEXT_HOP is checked for the best cost. This involves comparing the cost of each NEXT_HOP in the IGP's database. Then, if all the routes were leant by IBGP peers, the route learned from an EBGP speaker with the lowest identifier is selected. If the route was learnt only via IBGP peers, the route with the lowest BGP identifier is selected. This way of selection proves that there is no guarantee on the efficiency and reliability of the route. Moreover, it shows that the decision process can be tricked very easily by inputting false routes but with the best preference level.

After the first and second phase, the best route calculated by the speaker needs to be advertised to neighbouring peers. In the third phase, the best route is selected from Loc-RIB and stored in Adj-RIBs-Out for advertisement. This function is part of the route advertisement process. The route is sent to BGP peers via an UPDATE message. The rather key limitation of BGP is that it does not deal with individual routers but with ASes. Anything that is happening within an AS is hidden to the outside world. Thus, selecting the fastest and lower cost route is not that efficient, since not all ASes are the same. Some ASes are larger. This means that there can be longer looking routes but a quicker one, while faster looking routes are sometimes the longer ones (i.e. with a higher cost). This limitation is an important vulnerability because any BGP lookalike speaker can fool a real one into selecting for example a false route as a best route. The security issues of BGP will be dealt with in the next chapter.

3. BGP Operations and Messaging

After looking at how BGP-4 is used to store the routes and select the best ones, higher level communication is important and crucial to realise and keep the routing information up to date. BGP's operations mainly deal with messaging. These messages are crucial to the routing infrastructure because they are means by which route information is exchanged between BGP speakers. In every AS, BGP routers need to be allocated to perform their task. However, this part is not included in the protocol description. Hence, it is the responsibility of the AS' administrators to define the BGP speakers. Then, the bordering routers need to be linked physically in order to communicate.

When, for instance, two routers are configured to talk BGP with each other, the first move they do is establishing a Transport Control Protocol (TCP) session [21] at port number 179. This is the layer four OSI model TCP transport session. It is a three way handshake starting from the initiator of the session with a SYN packet. Then, the receiver responds with a SYN ACK packet. Finally, the session initiator sends an acknowledgement ACK to start the transmission of packets. As we can observe, BGP requires certain reliability in exchanging data. Rather than creating a new protocol for reliable communication, TCP already exists and is a connection-oriented reliable protocol. The use of TCP is not accidental. It is a protocol that accomplishes the orderly delivery of messages, detects duplicates, recognises when information has been lost and retransmits it, etc. Moreover, it can control the rate of sending packets so that the receiving end will not be overloaded.

Before an attempt of a TCP connection to be established between peers, the BGP session is in the **Idle** state as shown in Figure2.3. Then, when a speaker initiates a connection with a peer, the BGP session is in a **Connect** state. If the TCP connection cannot be established after a while, the initiator periodically keeps trying to establish a connection. The BGP sessions changes to an **Active** state. When a TCP connection is established, external or internal peers are assured of the reliability of the delivery, as long as the connection is up and running.

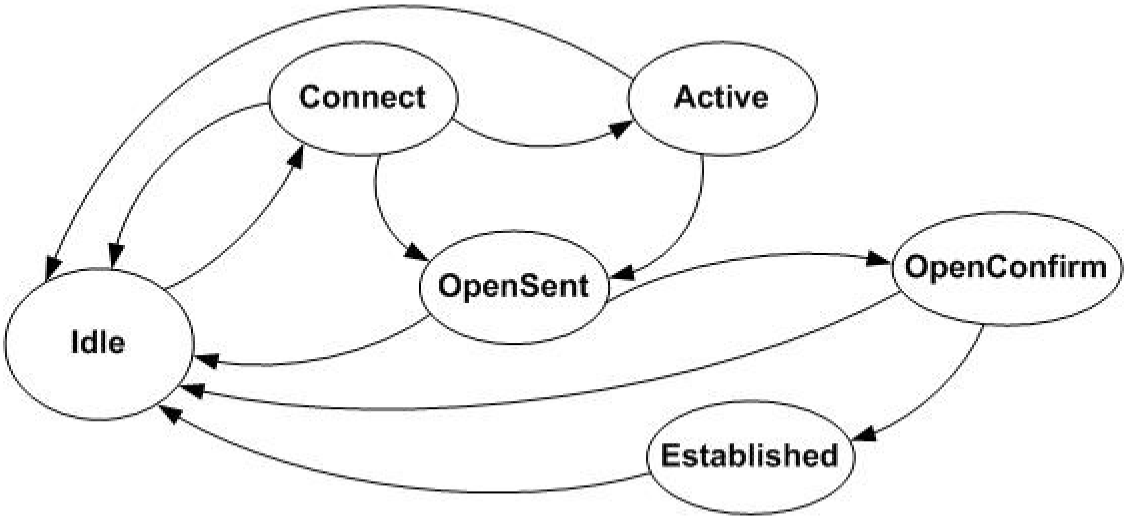


Figure2.3: BGP Session Finite State Machine

After a TCP connection is established between peers, they do not know anything about each other in terms of BGP's level data, since it is only a TCP connection. Therefore, the first thing peers do is to identify each other in many ways. This will allow them to establish a BGP session. To do so, they will need to exchange an **OPEN** message. The router that initiates the first OPEN message transitions in an **OpenSent** state. When a node receives a similar message, it transitions to an **OpenConfirm** state. When the parameters sent in the OPEN message are accepted, each side sends a **KEEPALIVE** message and transitions to an **Established** state. Details of these messages will be defined later in this chapter. At this time, the BGP session is considered to be live and routes can be exchanged. When a session is established at first, it is required by the protocol that all routes with different prefixes need to be exchanged. For this task, it uses **UPDATE** messages. For instance, if a speaker has 30,000 diverse prefixes and configured to send them all, a large number of UPDATE messages will be sent advertising all these prefixes. Then, only changes in routes are advertised between routers. The important feature of BGP is that considering policies, it does not always accept the learnt route. The receiving speaker can whether accept or reject the route update. These BGP sessions remain in the Established state. If a serious error occurs, the neighbour noticing the error sends a **NOTIFICATION** message to its neighbour and ends the TCP connection. This will lead to the denial of all routes received from that peer and going back to the Idle state.

IBGP ISSUES AND ROUTE REFLECTION

These BGP sessions are established with all speakers in neighbouring ASes. Every speaker shares a session with its external neighbour through EBGP. Similarly for IBGP, every speaker within the same AS share sessions with all the speakers creating a full mesh of IBGP connections. This does not imply that it has to share a physical medium with all speakers within the AS. On the contrary for EBGP, external peers are physically linked. The difference between IBGP and EBGP is on the retransmission of a valid best route from an UPDATE message. When a speaker receives an UPDATE message from an IBGP peer, it cannot retransmit to other IBGP peers in the AS. However, when it receives a valid UPDATE message with a valid new best route from an EBGP peer, it retransmits the route to all its IBGP peers and other EBGP neighbours.

The issue that rises regarding IBGP full mesh sessions is that it is computationally consuming. Moreover, this enforces peers receiving updates within the same AS not to advertise that route to a neighbour. By having, for example, 50 IBGP routers in an AS, it leads to 1225 IBGP sessions; and by adding only one router, the number of sessions will become 1275 (the calculation is done through the equation: (n.(n-1))/2 where n = number of routers). Thus, the solution for this issue is **Route Reflection** [22]. The concept of route reflection is to add a level of hierarchy to IBGP. This will lead to the ability of some routers to readvertise the learned routes to other IBGP peers. This eliminates the need for a full mesh. The routers that are able to readvertise are **Route Reflectors**. Those that get the reflection of routes are **Reflector Clients**. This makes route reflectors advertise the new routes only to reflector clients. Similar hierarchy speakers (i.e. route reflectors or reflector clients) do not readvertise routes between them. This is accomplished by adding a new attribute ORIGINATOR_ID with an attribute type 9. It is optional and non-transitive with a four bytes length. It is used to keep track of router Identities. Thus, a route reflector does never advertise a route to an IBGP speaker with an ID listed in the ORIGINATOR_ID attribute. This will also prevent loops of UPDATE messages. The second attribute added is also an optional non-transitive that groups a route reflector and its clients in a cluster. The attribute is CLUSTER_LIST and its type code is 10. When a reflector advertises a route to a non-client peer, it adds the current cluster ID to the related attribute. When a reflector receives a route, it checks if it matches a similar route with similar cluster ID to accept or refuse it. Another approach to solving the issue of scaling with IBGP full mesh approach is Autonomous System Confederations [23]. This will not be covered but details are found in RFC 5065.

Route Flap Dampening

One of the main issues that occur in interdomain routing is called **Route Flapping**. This happens when a link oscillates between connection and disconnection. As stated before, when a link goes down, the TCP session goes down and this will make all the learnt routes in that session withdrawn from both peers. Then, the link goes up and a new session is established and all the withdrawn routes are exchanged. The issue is when this happens frequently in the Internet’s scale.

A solution to this is to hold back the advertisement of routes somewhere near the route until it turns into a stable state. It is called **Route Flap Dampening** (RFD) [24]. It allows the speaker to consider the stability of a route and the peer in choosing whether to utilize or readvertise the route. RFD uses a value penalty that defines the criticality of the route flapping frequency in a link. Whenever the route flaps, the value is incremented. Penalty is decremented when the route stops flapping for a while. If penalty reaches a certain value, the route is suppressed and avoided for later forwarding. It stays dormant until the value decreases below the threshold. RFD is only used for EBGP and not IBGP. If it did, there will be a lot of inconsistencies within ASes because of the route suppression.

TCP MD5 Authentication

This is not part of the BGP protocol; but one of the sole security mechanism used by ISPs is generally TCP MD5 Authentication. The TCP connection can be attacked, for example by sending an RST (reset) messages causing an unsynchronised state of segment numbers. This will cause the TCP connection to stop and hence the BGP session to halt as well. Consequently, adding some practical security was required. To protect BGP sessions against the introduction of spoofed TCP segments into the connection stream, the proposed solution is an option added to the TCP connection, being able to hold an MD5 digest [26]. MD5 is a hash function; and the one used outputs a 128-bit digest. For more information on the hash function, chapter 9 in the Handbook of Applied Cryptography [25] provides further details on the cryptographic primitive.

To apply this protection mechanism, both parties (i.e. BGP peers) need to share a key or a password prior to any connection. The MD5 digest will be included in all TCP segments. To calculate it, it will require the following inputs as presented in RFC 2385 [27]:

1. The TCP pseudo-header (i.e. source IP address, destination IP address, zero-padded protocol number, and segment length)
2. The TCP header, excluding options and assuming a checksum of zero
3. The TCP segment data
4. An independently specified key or password, known to both TCPs and presumably connection-specific

After calculation of the digest, it is sent to the BGP peer. The latter will compute the same inputs and compare the calculated and received digests for similarity. If they are similar, then the segment is accepted. If they do not mach, the receiver drops the segment. Now, for a successful attack, it is required to guess the TCP segment number and the shared password. The standard does not include the way to generate the shared password or key and leaves the matter independent to the implementers or administrators. This does not sanitise the sessions from attacks. MD5 has its weaknesses as a hash function and vulnerabilities still remain. Moreover, the password generation is not defined, and this leaves an open issue on key space or password strength. The security issues will be included in detail in the next chapter.

4. BGP MESSAGES

BGP, as a protocol, runs its functions through the exchange of messages. It uses four types of messages to keep sessions up, update new routes, notify of errors and open BGP sessions. AS described before, these messages are exchanged between speakers subsequently after a TCP three-way handshake is established. A common header is shared between all four messages as shown in Figure2.4. The **Marker** field is used for authentication or synchronisation between a pair of peers. This value of marker will depend on the message being sent. For instance, when the first OPEN message is sent, this field contains all 1s. When the security option (i.e. applying TCP MD5 authentication) is decided between peers and se, this field will carry the 128-bit calculated MD5 digest when the security option is used. If it is not used by the peers, the Marker field will be filled with 1s. The **Length** field indicates the total length of the entire BGP message in octets, including the header. The length must vary from 19 to 4096. The **Type** field indicates the type of the message sent: 1 for OPEN message, 2 for UPDATE, 3 for NOTIFICATION and 4 for KEEPALIVE.

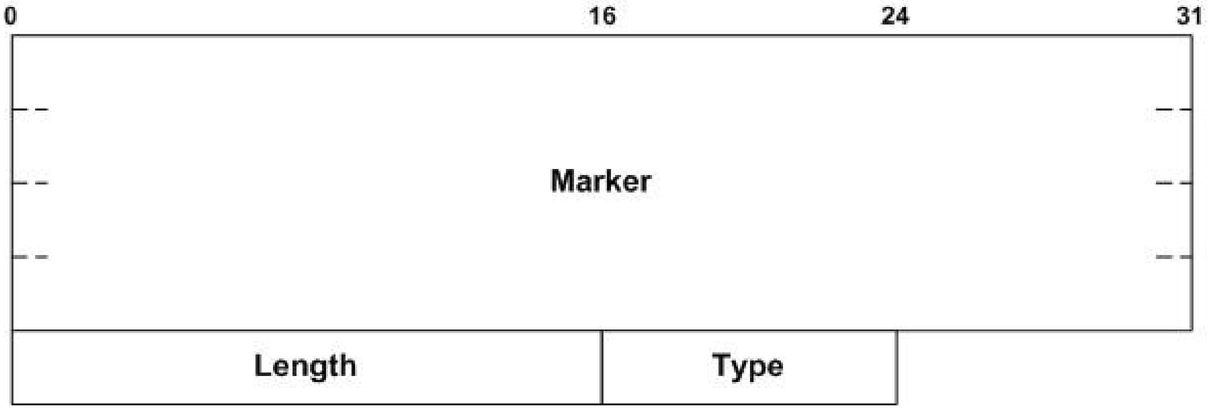


Figure2.4: BGP Common Header Format

OPEN MESSAGE

This is the first message sent by a BGP speaker to its peer subsequently after a TCP connection has been established. As shown in Figure2.5, the first three fields are common and are present in each message. The **Version** field specifies the version of the BGP protocol the sender is using. **My Autonomous System** field reveals the AS number of the sending speaker. **Hold Time** is used by the sender to suggest a time interval by seconds between successive transmissions of **KEEPALIVE** messages. **BGP Identifier** field represents the IP local interface address of the BGP router. The **Optional Parameters Length** field indicates the length of total length of the **Optional Parameters** (i.e. encoded in TLV: Type, Length, Value, used for authentication and optional added modules).

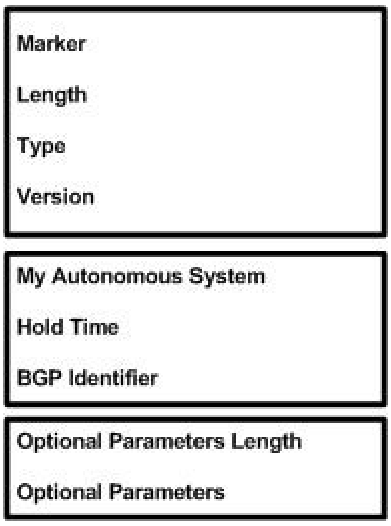


Figure2.5: BGP OPEN message format

KEEPALIVE MESSAGE

This message is the factor that keeps the connection established between peers. KEEPALIVE is used by speakers to constantly monitor the reachability of their peers. These messages are exchanged periodically by peers. They must be exchanged before the hold timer expires. If it does, the connection is dropped by the peer not receiving KEEPALIVE messages. The recommended time between two successive KEEPALIVE messages is a third of the hold time interval. This message contains the basic data in a common header format, as shown in Firgure2.6.

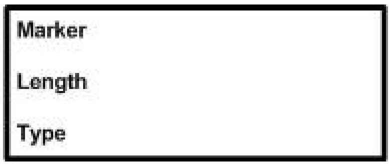
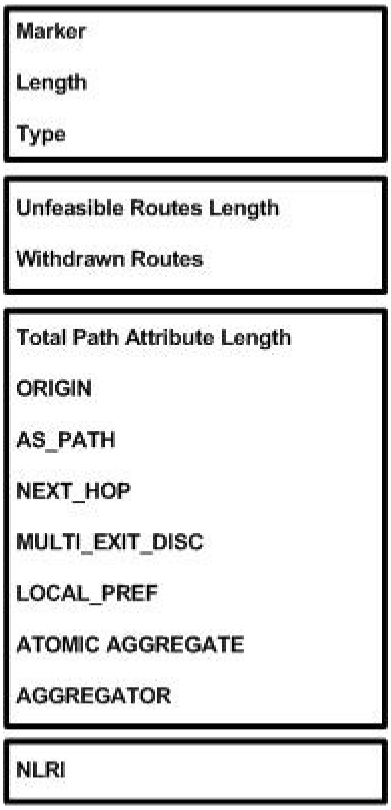


Figure2.6: BGP KEEPALIVE message format

UPDATE MESSAGE

When a link is established, peers begin an ongoing process of message updates of the reachability of Networks. Each router encodes the new information from its RIB into a BGP UPDATE message. The latter contains information about network address and path to various networks (AS_PATH). The route updates are incremental, meaning they only send the information about routes that have been changed. This will save bandwidth. Apart from the first three common format fields, an UPDATE message exposes the withdraw routes in its **Withdraw Routes** field. This comes after the length of those withdrawn routes in **Unfeasible Routes Length** field. In **Total Path Attribute Length**, the advertising speaker exposes the length of the path attributes field which contains the list that comes after it in

Figure5.7. Finally, **Network Layer Reachability Information** (NLRI) is used to advertise the IP address prefixes for the route being advertised.



Marker
Length
Type

Unfeasible Routes Length
Withdrawn Routes

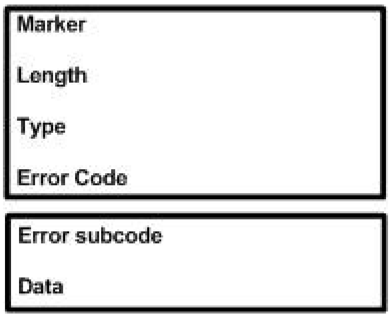
Total Path Attribute Length
ORIGIN
AS_PATH
NEXT_HOP
MULTI_EXIT_DISC
LOCAL_PREF
ATOMIC AGGREGATE
AGGREGATOR

NLRI

Figure5.7: BGP UPDATE message Format

NOTIFICATION MESSAGE

When a BGP speaker notices an error or catches an exception, it sends a NOTIFICATION message. After doing so, the speaker imminently closes the TCP connection. The **Error Code** field indicates the type of error that occurred. **Error subcode** provides more specific information concerning the error condition and the nature of the error. The field **Data** explains the cause for the notification.



Marker
Length
Type
Error Code

Error subcode
Data

Figure2.8: BGP NOTIFICATION message format

5. Conclusion

After viewing details about the protocol, it is majorly relied on the exchange of different messages. Moreover, one of the major issues with BGP is its complexity compared to other routing protocols. This can be understood because of the scale of the Internet. Coming back to our major concern which is security, BGP as a protocol does not have any mechanisms that provide protection to the messages exchanged, as viewed over this chapter. The use of MD5 authentication is not part of the protocol and not mandatory. Moreover, it has its weaknesses. In the next chapter, we cover the vulnerabilities of BGP and the attacks that can be conducted against it, followed by possible attack scenarios.

Chapter 3

BGP THREAT ANALYSIS

As covered before, BGP was designed in order to overcome the communication issues that were encountered in the previous protocol (i.e. EGP). BGP has shown great stability over almost the last two decades. However, there are still some serious thoughts on whether they will still be able to handle the immensely growing Internet. One of the major issues in BGP is Security. It was considerably well designed for communication purposes, but the security concerns were left behind and were not part of the design process. Thus, BGP is fragile as a protocol and can lead to serious damages to the Internet community. In this chapter, we illustrate the vulnerabilities that exist in the protocol. Then, we provide the reader with the attacks and attack scenarios able to disrupt the functioning of interdomain routing and the Internet in general.

1. BGP VULNERABILITIES

In the last chapter, the overview of the protocol BGP was covered. No single security is part of the protocol except some mechanisms were added to make it harder for a malicious behaviour to succeed, such as the TCP MD5 authentication. Any entity that connects to the Internet pays its ISP for that service. When it connects, it becomes part of the ISP's administrative Autonomous System. An entity is eligible to route its own traffic to other entities through its ISP. The latter routes its own traffic through its upstream ISP and receives routes from it. It can be deducted that systems are grouped together and can be targeted as such by a malicious individual [41]. As a consequence, vulnerabilities found in BGP are very serious.

As stated in the first chapter, interdomain routing suffers from misconfiguration issues. BGP suffers from the same problems. This means that misconfiguration which can be a human error can lead to serious damages. Hence, an attacker can provoke similar or worse damages to the interdomain routing or the Internet as a whole. BGP suffers from vulnerabilities that can be exploited in many attacks.

BGP MESSAGE VULNERABILITIES

When two peers establish a session, whether EBGP or IBGP, the protocol does not protect the exchange of those messages from different violations. The absence of security measures prior to the session establishment or after leads to the nonexistence of protecting the **integrity** of those messages. If the integrity can be violated, this means that a malicious individual can exploit this vulnerability by intercepting and changing the transmitted messages as they will.

Another issue considering update messages is that they can be replayed by an attacker. Apart from the TCP sequence number as a weak mechanism, BGP messages can be replayed since they do not provide any **freshness** service. An old message can be replayed with the right TCP sequence number after a new session is established. This means that if a route has been added and a malicious individual intercepts that UPDATE message, they can replay the update after the route has been withdrawn. This might cause an invalid route to be present in the forwarding table (i.e. BGP routing table Loc-RIB and Adj-RIBs-Out).

In addition, there is no mechanism that provides **source authentication** of messages to BGP speakers. The TCP MD5 authentication was added to overcome the problem of a potential message sent from other than the legitimate BGP peer. However, as will be illustrated in the next session, MD5 authentication has its weaknesses; and in today's standards it is not classified amongst highly secure mechanisms for integrity or source authentication security services. Moreover, this so called solution is not part of the BGP protocol. Although now majorly used, it has many weaknesses considering many aspects from MD5 hashing collisions, key management issues, weak passwords, etc. This is not a long term secure solution for a protocol as important as BGP.

Although it is not part of the major aim in securing BGP, confidentiality can lead to better protection of messages exchanged between peers. Message interception is one of the easiest and cheapest attacks that can be used to extract data required for further attacks against BGP. This protocol does not provide any confidentiality service. However, this is not part of the key concerns in securing interdomain routing.

Routing Information Announcement Vulnerabilities

One of the major issues in BGP is to deal with the quality of routing information transmitter. In other words, the reachability information needs to be qualitatively trusted since this is the aim of routing in general. It is inherently intrinsic to routing. Hence, the importance of this information is trivial for the routing infrastructure to keep the packets arriving at the intended destinations. Following the previous analogy in chapter 1 about routing in roads, if the information provided is wrong, someone who wants to go to Germany from England can end up in Algeria for instance if routing information were wrong. Thus, there has to be an authority that decides and advertises the routing information from a country to another. This means that someone travelling generally buys a guide approved by an authority which can be the Interior Ministry in some countries or any other trusted party. Coming back to interdomain routing, the announcements of reachability information needs to be validated by an authoritative AS. Not any AS can provide new routing information. For example, an ISP, as the upstream AS for its clients, is the one which provides routing information. However, BGP does not validate this authority for UPDATE messages. Thus, any AS that might be malicious or apprehended by an attacker, is able to announce new routes to its peers.

Since BGP does not provide data origin authentication and does not provide authorities for route announcements, the authenticity of the path attributes announced by each BGP speaker is not validated by the protocol. This denotes that all the attributes described in the previous chapter can be played around with by an attacker and cause damages to a stub AS, multihomed AS or even a portion of the Internet. There is no mechanism in the protocol that checks for the validity of the data used for UPDATE and OPEN messages.

Consequently, the absence of security controls and safeguards, introduced previously in vulnerabilities, can be exploited to craft attacks, using the weaknesses of the exterior routing protocol to conduct larger attacks goals or against it directly. There are several generic attacks that can be conducted against interdomain routing. The first one is **Eavesdropping**; which is the interception and reading of BGP messages, as the data is in clear text. BGP does not protect against **Replay** attacks. These are, simply, the recording and resending of messages. Moreover, it does not protect against **Message Insertion** attacks. Having the knowledge of sequences of packets can eliminate part of this issue but still remains if the attack is well crafted. Then, an attacker would have the ability to insert bogus messages into a BGP session for example. In addition, there is no protection against **Message Deletion** attacks. An attacker can intercept and delete messages between **Speakers** (i.e. inter AS routers communicating with each other) or totally remove routes from the forwarding table. An attacker is also able to remove messages between two speakers, modifies and resends them back to the receiver. Interdomain routing is vulnerable to **Message Modification** attacks. Moreover, it is weak against **Man-in-the-Middle** attacks. A malicious individual is able to corrupt the communication streams between speakers and becomes an unnoticed and unknown intermediary. Furthermore, it is largely vulnerable against Denial of Service (DoS) attacks. These generic attacks will be covered in following section in more detail and in different attacks against different parts of the BGP protocol.

2. BGP Attacks and Attack Scenarios

BGP has been receiving quite a lot of attention considering its fragility towards malicious attacks. As a protocol, BGP can be categorised amongst the weakest and most dangerous protocols. This is due to the serious economic damages that would emerge if the Internet as a whole, or more precisely the core registries and routers were to be attacked and compromised. This section will demonstrate some attacks that if well conducted can succeed and violate the well functioning of BGP and inter-AS communication [33]. Then, it will demonstrate the usability of those attacks against BGP to aim at larger goals of adversaries.

ATTACKS

As previously illustrated in Chapter 2 Figure2.3, different attacks in those different states in the BGP session finite state machine can be conducted by malicious individuals. These can be found at different stages in the BGP session establishment process. Referring back to the finite state machine, the attacks can be conducted at the Idle state where there is no session established between speakers. Attacks also can happen at the Connect and Active state where malicious data is injected and can cause a denial of service. The first three states refer exclusively related to the Transport layer TCP session flaws. BGP inherits all the attacks and security flaws from the TCP session, in addition to other attacks concerning the BGP session itself. The latter can be accomplished in the OpenSent, Open Confirm and Established states [33].

EAVESDROPPING

This attack is required in most of the coming attacks. Although it is not a major concern in securing BGP, this attack if eliminated will make further attacks much harder to craft because of the lack of knowledge that can be gathered. Thus, this attack is generally more passive. It is used to listen to messages exchanged between peers. Generally, it can be achieved by physically tapping the physical medium between BGP speakers. Another way of realising it is by gaining local access to a network segment, compromising a server and installing sniffing software. The adversary can then use this gained information from this attack to craft more dangerous ones [33].

COMPROMISE MD5 AUTHENTICATION

MD5 authentication was added to the BGP session in order to protect the session establishment and all the messages exchanged when the session is up [27]. After the exposure of MD5 vulnerabilities in the previous chapter, there are more flaws and attacks that can be conducted in many ways and not necessarily relating too closely to the protocol.

Social engineering [28, 29] is a technique used to deceive people into giving in secret information or changing parameters into their system that would make it more vulnerable or open for remote access by attackers. If the AS owner has weak security policies related to passwords, it would be an security issue knowing that BGP MD5 authentication is based on sharing passwords. Any type of social engineering can be conducted to deceive one of the administrators in both ends (i.e. both speakers in each AS) into giving the password for the MD5 calculation. Moreover, the attacker as a social engineer has two chances for each password, since there are two peers in different ASes sharing the same session but having different security policies. For instance, one of the ASes has weak security measures when an employee is dismissed. Supposing that the employee is an administrator who knows the password, and he is not happy of what happened. An attacker who observes what is happening in the company can track the fired administrator and deceive him into giving up the password for vengeance. The administrator has nothing to lose and gives away the password to the attacker. The latter can then use that password to initiate an unauthorised session with a BGP speaker, inject packets for poisoning the routing table or causing a denial of service against the session or the routers' memory capacity [33].

Another way into compromising the password is to capture it using a key logger for example. Key loggers are applications used to record users' key strokes. The aim of key loggers is spying on users by monitoring their passwords and their daily routine, performing political, commercial or industrial espionage, etc. For this situation, the victim is the administrator responsible for interdomain routing or networking and the aim is monitoring and retrieving the MD5 password for later abuse. The general goal of attacks varies according to the motivation and the gain. If the attacker can gain or compromise access to an administrative machine, they will be able to install a hostile application that monitors and logs keystrokes typed by administrators. These applications also provide a clear monitor view of the activity in the machine. In this way, the attacker can retrieve the MD5 password from the logs or see it in the screen while it is being typed [33]. Another way into promiscuously retrieving the password is to sniff traffic while it is being sent within the management traffic. This can be achieved by tapping the physical medium, or installing sniffing software after compromising a server's operating system, locally in the AS. In a different way, router configuration is a major issue and many things are left unnoticed; and one of these things is passwords. The latter can be captured from configuration by compromising the network management server or the router itself [30]. The router can be physically or logically compromised. If the attacker can access the data centre where the router is placed, they can recover the password using many methods, especially rainbow cracking [31] for time and efficiency. However if the attacker cannot physically access the router, there are many remote logical attacks able to succeed. The malicious individual can sniff the password, recover the password as they might do in a physical attack, or just guess it. They can also exploit the security flaws present in different applications used as a medium for configuration such as Telnet and SSH (Secure Shell). This will provide them with the MD5 password required to establish a session and inject poisonous packets.

In addition to these attacks, another one is to actively brute-force the MD5 password by sending to a peer a segment with the MD5 authentication option. Then, the attacker can watch the response from the peer to determine the validity of the key used for the hash. If a valid password was found, the attacker can gain access to the router with the password and also use it to poison the routing table and more. These attacks will be illustrated later in this chapter. Such attack can be easily conducted if the attacker can obtain an MD5 authenticated packet. This will allow the attacker to conduct an offline attack. For example, the attacker can use a rainbow table attack which is implemented in many cracking tools.

MD5 as a hash function is not very robust to collision attacks [32]. Collision avoidance or limitation is one of the most important security properties of hash functions. Collisions happen when given two different messages; the digests calculated from those messages are similar. In August 2004, MD5 collisions were found. V. Klima used a method that found a collision in around half a minute with a notebook computer [32]. If the attacker can exploit these weaknesses of MD5 in finding collisions, they can use those collisions and craft poisonous packets for instance.

Setting up an unauthorised BGP session with a peer

As viewed in Chapter 2, a TCP session is required for peers to establish a BGP session. The requirement for an attacker to establish an unauthorised session with a peer is to pass the MD5 authentication, if required. The latter was examined in the previous session. As covered before, BGP inherits all the vulnerabilities of the TCP protocol. Thus, it inherits all the attacks against the TCP protocols and sessions. Not all the attacks are useful, and only the useful attacks will be exposed.

An attacker can use some foot printing and reconnaissance techniques to gather information about an AS. If an attacker can know the IP address of a BGP speaker, its peer, and the ports used for a session, they can spoof the TCP packets with the source IP address and port number of the peer. Then, they can establish an unauthorised TCP session with the speaker, using the usual three way handshake (SYN, SYN ACK, and ACK). This attack can be done on a remote EBGP speaker or a local IBGP speaker. In both cases, it can lead to easier table poisoning for example. Another way to achieve such attack is to gain unauthorised access to the router and reconfigure it. The configuration should allow a peering session with the attacker’s router. Then, a session can be established between the attacker’s router and the BGP speaker, since it is allowed after compromising the router configuration [33]. After this, the attacker will end up in a connected and/or authenticated TCP session, in an OpenSent state where they can start sending BGP OPEN messages to start an unauthorised BGP session. Once this is established, the attacker can more easily launch attacks that can affect both the peer and the network itself.

BGP Spoofing Attack

In order to communicate with a speaker in an existing BGP session formed by the speaker itself and its legitimate peer, the attacker needs to acquire more information about the session. This attack is thought to be easy; however it is not. They will have to acquire the following information to be able to conduct this attack:

Source IP address of the peer: To do this, they can use ICMP traceroutes from various places on the Internet through the BGP peer. J. Rexford and her research team found an accurate way of making an AS-Level traceroute [34].

Source port number: This field must be additionally spoofed. The initiator of the BGP session always has a port number greater than 1024 and sequentially or randomly selected; while the peer will receive the packets in port 179. Since the attacker does not know which BGP router initiated the session, they might have to sniff the traffic between the peers and get the information required.

TCP Sequence Number: The TCP protocol has a sequence number field that is used by the receiving end through a windowing technique. If any packet received is in a range below the window range, the packet will be dropped. This feature weakly prevents replay attacks. However, since BGP sessions are designed and meant to stay connected for longer, the window size is quite large. This gives the attacker a better chance in falling within the window size and getting the right sequence number. The attacker would have to send a number of packets at once with incremental sequence numbers, until one is accepted.

TTL (Time To Live): TTL is a safety mechanism used to drop a packet if it gets lost in the Internet. The TTL is a number that represents the maximum number of hops a packet can take. Generally, ISP peering sessions use EBGP; and since they are directly connected, the TTL is set to 1. If the received packet's TTL is greater than 1, it is dropped. The attacker will have to traceroute the packet and not the number of hops the packet takes before it reaches the target. Then, the attacker can set the TTL accordingly so that when it is received, its value will be 1.

In one hand, the attack can be TCP based spoofing, where the attacker targets the BGP port of the router which is not always 179, depending on which side the communication was initiated. On the other hand, the attack can target the peer with a spoofed BGP packet. For both types, the attack is not that easy to craft and the attacker will require the knowledge of the previous fields. These fields must all be similar and synchronised with the legitimate session. In addition, the attacker might need a layer 1 (physical) or Layer 2 (Data Link) medium. After successful completion of this attack, the victim speaker will think that the message is legitimate and processes it as if it has been sent from its peer.

BGP Hijacking

This attack will require the above attack (i.e. BGP spoofing) to be successful. The attacker will need to masquerade BGP status packets as if they were coming from the neighbour. The packet would look legitimate to the peer receiver. However, it would carry malicious BGP updates. These updates could be causing a denial of service to the BGP session, introducing false routing information, or withdrawing valid routing information. Effective BGP hijacking will require further knowledge to the attacker about the BGP session. They would require knowing what was set up in the OPEN message. This can be done through different eavesdropping attacks, as mentioned in the first attack through sniffing and physical wire tapping. The attacker can reroute traffic towards his station causing a serious violation of privacy and confidentiality.

Route Injection

In the last sections, attacks in setting up an unauthorised session were covered. If an unauthorised session is set up, other attacks are easier to achieve. The latter include adding nonexistent routes, changing route preference level to a faulty route, etc. However, if the attacker cannot set up a new session or wants to attack an existing BGP peering session, they would have to craft their attack differently and will need more information on the session, as pointed up earlier in spoofing and hijacking attacks. The attacker can use one of the previous attacks to inject or advertise routes where the network does not have allocation authority. It is an **unauthorised route injection attack**. This will draw away traffic from the authorised network causing a Denial of Service (DoS) on the network that allocated the address. Since it is a layer 3 spoofing (i.e. IP spoofing), it is easy and there is no protection in the protocol against it.

Another type of route injection is the **unallocated route injection attack**. The attacker would advertise IP addresses that have not yet been allocated by IANA. They can overload a router's BGP and forwarding tables with these types of IP addresses. This can create some issues to the routing infrastructure in the Internet. Routing tables will grow in size, which may lead to BGP table explosion and therefore resource exhaustion. This occurs because most ISPs do not filter out unauthorised routes. The reserved IP address space set by IANA is publicly listed but a number of ISPs ignore them in their filtering.

De-Aggregation Attack

This attack can cause a lot of damage to the internet community and generally to ISPs. It can also happen when misconfigurations occur. This attack uses a feature of BGP in choosing the more specific routes for their routing tables. If an attacker can break into a multihomed customer AS, they can launch an attack from it. They would have to announce more specific prefixes (e.g. /24s). Since the most specific route is always selected, this will consume more router memory and disrupt global Internet routing operation and can crash routers as well. The attacker will send unauthorised UPDATE messages to peers with specific prefixes. Generally, saturated links cause more damages and can disrupt the routing infrastructure. If the ISP does not perform strict ingress route filtering on customer ASes, the attack would not only have an impact on the ISP itself, but these routes will propagate across the Internet or its peers.

TCP BASED ATTACKS

RST Attack

This attack will require the ability to spoof messages within an existing TCP connection established between peers. The attacker can send a spoofed message with the RST bit set to 1, to one of the peers. The latter will terminate immediately the connection with its peer causing a denial of service. The peers then will have to establish another connection and send routing all routing data to each other. If this attack is conducted after many connections, route flapping will occur as discussed in Chapter 2. This will cause the routers to suffer from Route Flap Dampening (RFD). The attacker uses this feature of BGP to increase the penalty value in RFD. This will cause a temporary and possibly long inactive BGP speaker, which will affect with a significant impact a large number of users [36, 39].

SYN RST Attack

This attack can be performed indirectly through another attack. The latter is called **SYN attack**. The attacker here will cause an indirect reset by sending a TCP packet within the window frame with the SYN bit set to one of the speakers in the peering session. The receiver will send a RST set packet and immediately stop the connection. This attack is an indirect way of using the RST field to stop the connection. This attack is rather more dangerous since it can cause the generation of more packets resulting in flooding the connection. This can happen if the attacker targets one BGP peer that is connected with multiple peers. Because this is a reflection attack, all the peers will send the same RST packet at the same time causing resource saturation [38].

SYN ACK Attack

When a legitimate TCP SYN is sent from a speaker to a peer, an attacker can learn that information and send a TCP SYN ACK packet before the peer does. The peer will receive an empty ACK reply. Then, the legitimate peer will send a RST to close the connection. The attacker needs spoof the SYN ACK message with the right sequence number.

ICMP Attack against TCP

This attack has a particularity of being able to be achieved blindly. The attacker will not need all the information required for the RST attack. ICMP messages are used to handle errors and fault recovery on the network. If the ICMP message reports a hard problem, TCP will close the established connection. If it reports a soft problem, TCP will record the information and retransmit data until it is acknowledged or the session is closed [35]. Because ICMP messages do not require the TCP specific fields such as sequence number, the attacker can blindly send and ICMP error message indicating a hard error. This will cause a TCP RST attack to both peers. This will end the connection between the BGP peers causing a denial of service. This attack can exploit RFD to cause a complete halt for the EBGP session.

TCP SYN Attack

If an attacker is able to send a SYN TCP session opening packet to a speaker during the connection establishment of the speaker with its neighbour, they can cause the legitimate peer's SYN connection to be ignored by the speaker since it would appear to be a second connection. The attacker can then go on with the sequence of required messages to get to the Established state for the BGP session. If a similar session has been established with the legitimate peer, the speaker will detect the collision and chooses the session to be ended. This will depend on a BGP identifier. If the attacker chooses the fields carefully, the legitimate peer's session can be terminated.

SYN Flooding Attack

Using previous attacks, the attacker can impersonate, prior to session establishment, a BGP neighbour. The attacker can send a large number of TCP uncompleted connections (i.e. only the first message in the three-way handshake SYN) to the BGP router at port 179. This will cause the exhaustion of TCP connections memory and can crash the router. This is a denial of service attack. This can also be used in a distributed way, where the attacker sends multiple TCP SYN messages to the target from different nodes. This is a distributed denial of service attack. These attacks are hard to deal with since there is nothing BGP mechanism that can defeat them [37].

BGP Messages Attacks

BGP messages are used to exchange routing information and connectivity between BGP peers. Knowing the non-existance of security in those messages, they can all be used to cause different types of attacks that cause a denial of service. These messages can be used in a malformed way or at states where the normal running of the protocol's process does not expect it.

OPEN message Attack

As stated before, these attacks, generally, target a denial of service of the BGP session. An attacker can send an OPEN message to a speaker at the Active or Connect state. This will cause the speaker to terminate the connection and drop the connection and turn to the Idle state. These attacks require careful timing. The attacker may use sniffing techniques or be a man-in-the-middle in this establishing session. Moreover, the attacker can send an OPEN message at the Established or OpenConfirm states. This can cause a connection drop when a detection of a collision occurred in the BGP speaker's process. Another similar attack is to send a carefully spoofed OPEN message at the OpenSent state. This will cause the speaker to transition to an OpenConfirm state. When its peer sends an OPEN message, the speaker will detect a collision and drop the BGP session. RFD can be exploited in this attack.

KEEPALIVE message Attack

The attacker needs to synchronise well the KEEPALIVE message when it is sent. If they are able to do so, they can send a KEEPALIVE message before the BGP session is established. This means that they send it at the Active, Connect or OpenSent state. When a peer receives such message at these states, it detects a synchronisation problem and terminates the session returning to the Idle state. RFD can be exploited in this attack too.

UPDATE message Attack

If an attacker can spoof an UPDATE message, they can send one with more than the maximum number of prefixes allowed, at the Established state. This will cause the session to be aborted and alter to the Idle state. Therefore, all the information learned will be deleted in the tables and a new session needs to be established to exchange the routing information. However, the attacker can make this denial of service more efficient by exploiting RFD, causing the speaker to be put in a halt state or totally ignored.

An attacker can exploit UPDATE messages by sending malformed packets. They can set in the UPDATE wrong attributes, such as Total Attribute Length, syntactic errors in fields, or missing attributes. In any case, the attacker can play with all the attributes present in those messages creating errors in parsing. This will cause the receiving peer to drop the session and the same previous scenarios of DoS may occur.

Moreover, the attacker can send an UPDATE message at any other state than the Established one. This will cause the BGP process to return to the Idle state by dropping the connection. This is a similar DoS attack that can exploit the RFD option.

NOTIFICATION message Attack

If an attacker can spoof a NOTIFICATION message at any state, they can stop the process and turn it to the Idle state. If the peers are already connected, such message can cause the connection to be dropped. In such attack, exploiting RFD is possible. Oscillation of connections will continue; and the attacker needs to keep sending NOTIFICATION messages. This will cause the penalty value in RFD to increase, until the peer is stopped for a while. This is one of the types of DoS that can be caused by an attacker.

ATTACK SCENARIOS

The previous attacks covered are atomic as described in [33]. However, an attacker would want more when attacking the routing infrastructure. These larger goals are described in this section as attack scenarios. So, an adversary would use BGP vulnerabilities to execute larger attacks that have bigger impact on the Internet itself and its community. S. Convery et. al. in [33] split up the attack scenarios into five different goals. This section will describe those attack scenarios in a more BGP protocol focused way.

DISABLE A STUB AS

There are many ways an attacker can disable a stub AS. All of the attacks studied that relate to a denial of service can be used to disable a stub AS from receiving routing information from its ISP multi-homed AS, and routing its packets outside its border. The attacker can use SYN flooding to crash the BGP speaker of the target AS. They can use one of the BGP messages attack by sending wrong fields in messages or messages at the wrong state of the speaker. Moreover, they can use TCP RST attack against the BGP session established between the target and the service provider for instance. In addition, they can use SYN, SYN ACK and ICMP attacks to achieve a similar goal. Obviously, these attacks need to be continuous until they exploit the Route Flap Dampening option to provide the speaker with a large penalty value. Therefore, there are many attacks that can be used to cause such goal but generally attackers want more than disabling a stub AS. However, depending on the targeted AS, the level of impact increases.

Disable Critical Portions in the Internet

Many routing attacks can have the objective to disable critical portions in the Internet. The criticality depends obviously on the representation of the portion and need of that portion in the Internet by the dependent organisation, or even country. This objective can be achieved by altering a global internet routing table. This can be done by realising an unauthorised route injection attack. This attack will insert unauthorised prefixes into the routing table. Then, the attacker must be certain of the propagation of these injected unauthorised routes despite the fact that route filtering is applied in many ASes. Then, they can repeat this in multiple ASes in different providers. An attacker can establish an unauthorised BGP session with a peer instead of conduction the route injection attack. Another way to achieve such goal is to disable core critical routers. This attack will have a larger impact because of the importance of the target. Majorly, the attacks are of DoS type. The adversary can use TCP Reset or message attacks against the BGP process. These will cause a denial of service to the session. Otherwise, they can attack the router with SYN flooding at port 179 until the memory resources are saturated. Another way is to flood the routing table by sending the most specific routes that should be accepted by the upstream AS. This will cause the routing tables to flood because of the more specific routes. Since all these types of routes are sent, they will be propagated causing a chaos similar to the AS7007 incident in 1997 [40]. This attack exploits the routing table memory limitations. All these attack scenarios cause a denial of service to a portion of the Internet.

Disable a Multihomed AS

To achieve such an objective, the attacker can use any of the previous two attack scenarios at a higher scale. This means that the attack will be conducted against many BGP speakers. The attacker can disable many stub ASes that are connected to the multihomed AS. This way, all the links that are connected with the multihomed AS will be down. The attacker can isolate the target from all other peers causing a denial of service to targeted multihomed AS and the stub ASes that rely on it. Another technique is to disable the critical portions of the multihomed AS’s network. This attack uses the same approach as disabling portions of the Internet. It will focus on causing a denial of service on the BGP processes relied on by the target.

Blackhole Traffic

This type of goal requires a few attacks to be achieved successfully. Blackholing traffic means that traffic routed or forwarded will be dropped and will not reach its destination. This attack can target a stub AS or an ISP from the outside if the latter relies on a single upstream ISP. The attacker can use different techniques in persuading the peer to route all the traffic to their router. They can establish an unauthorised BGP session with the target. Then, send UPDATE messages that route all traffic through the attacker's machine. This way, the adversary will receive all the packets through their machine and drop all of them, while keeping the BGP session live. The targeted AS will forward its traffic to the malicious router using the information learnt from it. Another way to achieve this attack is to send spoofed BGP UPDATE messages that poison the routing table with more specific unauthorised prefixes. This way the decision process of the targeted BGP router will use those new routes that lead to nowhere. This creates a sort of blackhole for the traffic originating from the targeted AS.

DNS Attacks

This goal is the one that is targeted by many attackers. Routing based attacks can be used to conduct other ones through the Domain Name System. The first aim would be for the adversary to collect personal data of users for instance. After a successful routing attack, a malicious individual can attack the DNS and lure traffic towards a compromised web server for example. This way, any user, for instance, can use a service where credentials are required. The attacker can get hold of them through this scenario [61]. Other more damaging attacks can be conducted using interdomain routing as a proxy. For instance, the attack can a BGP based attack to masquerade as root DNS servers. This provides the attacker with such large flexibility and immense damage they can cause to the internet community.

3. Conclusion

Most of these attacks and attack scenarios are able to be conducted to disturb the functioning of BGP processes. However, they require deep knowledge of BGP routing and routing architecture of the target. Most implementers and manufacturers generally declare that such attacks have never occurred and are unlikely. However, they did and they can happen since there are many cases concerning misconfiguration that have caused almost chaos. Nevertheless, the presence of these vulnerabilities in the protocol itself is disturbing. The state of BGP security cannot be left as it is and the countermeasures should be included in the protocol and not added as extra options for the users. Hence, security requirements need to be defined before analysing the solutions that have been put in place to avoid such possible attacks that can harm the Internet as a whole. In the next chapter, we examine the security mechanisms used nowadays to endeavour to secure some portions of interdomain routing. Moreover, we study the different security requirement needed for better functioning of BGP and the security problems required to be solved.

Chapter 4

BGP SECURITY

After reviewing the different threats and attacks that can be achieved by exploiting BGP vulnerabilities, this chapter presents the current methodologies used by ISPs to secure their BGP routing infrastructure. Then, it covers the security requirements needed to minimise the issues discussed previously. Moreover, we illustrate the main security problems that should be emphasised to provide a protection at the protocol level.

1. CURRENT PROTECTION MECHANISMS FOR BGP

Since BGP is the main protocol used in interdomain routing, securing it by any means while research is in progress is a must for all ISPs. Generally, the protection mechanisms used nowadays is to protect the TCP session from attacks. Actually, it is not for protection but only making it harder for attackers to affect ISPs and their upstream providers and downstream customers. Moreover, traffic filtering is used extensively in border routers.

TCP MD5 AUTHENTICATION

TCP MD5 authentication was analysed in the previous chapter. It is not part of the BGP protocol and is implemented by most ISPs. As stated in chapter 2, it is used to protect BGP sessions against the introduction of spoofed TCP segments into the connection stream. The proposed solution is a keyed Hash function or known as Hashed Message Authentication Code (HMAC) [42]. It is used for each message exchanged between peers. However, a password or key is chosen manually and inputted as such in both ends of the session. Considering thousands of routers used concurrently, maintaining shared secrets between them is extremely complicated. Furthermore, these shared secrets need to be changed regularly or they will be subject to different attacks against the cryptographic function. In addition, it will add more complexity to key management, since it is manual.

IPSEC

Although much more effective than the previous solution, it is not widely used by ISPs to protect their BGP sessions. This is a protection mechanism for the layer three IP datagram. IPsec is widely used for tunnelling VPNs over Internet between endpoints when transmitting confidential or important data [43, 44]. This security mechanism can be used to protect BGP sessions from Integrity violation, Replay and DoS attacks through its

Authentication Header protocol (AH). It can also be extended to an additional confidentiality security service via its Encapsulating Security Payload (ESP). In addition, it can dynamically negotiate secret keys and has an implemented key management mechanism. The latter uses the IPsec Internet Security and Key Management Protocol (ISAKMP) [45] and the Internet Key Exchange (IKE) [46]. IPsec is used to protect the BGP peering sessions by implementing Virtual Private Networks [47]. The implementation of this safeguard is efficient to tackle BGP session local vulnerabilities. However, it does not address widespread attacks and cannot scale with them.

Generalised TTL Security Mechanism (GTSM)

This is a security mechanism that prevents attackers from remotely sending BGP spoofed messages to targets. This mechanism uses the TTL attribute in the IP packet. The TTL is a value that is decremented at every hop and if reaches zero (0), the packet is dropped. Originally, between BGP peers TTL is set to 1 by the sending router. As illustrated in the last chapter in spoofing attacks, an attacker can set the TTL by counting the number of hops so that it arrives to the target with the value 1. This mechanism uses a different value to be set between peers. Peers that require multi hops to reach each other are rare. Thus, GTSM uses a TTL with a value 255 for the sending speaker. The receiving peer needs to check that the value of TTL is not less than 254. If it is not the case, the packet is dropped or flagged according to the implementation. This will assure that no remote attack can be conducted.

The following is a table that shows the efficiency of those three techniques to protect peering sessions [49].

	Integrity	**DoS prevention**	**Replay Prevention**	**Confidentiality**
MD5 Integrity	Yes	No	Yes	No
AH (IPsec)	Yes	Yes	Yes	No
ESP (IPsec)	Yes	Yes	Yes	Yes
GTSM	No	No	No	No

Table4.1: BGP Peer Session Security Mechanisms

Suspicious Traffic Filtering

This technique is conducted using defensive routing policies. The latter are used to filter out malicious or suspicious announcements. This includes checking for hazardous and risky attributes of UPDATE messages. Most ISPs, for example, implement ingress and egress filters derived from routing policies. They use lists of loopback addresses and addresses with no match, in a document called Documented Special Use Addresses (DUSA), provided by IANA. These filters can parse all BGP messages and especially UPDATE messages to retrieve and drop malicious looking packets. This method is a good defence method but this depends on the policies and filters which become very messy and hard to control after a while.

2. Security Requirements

The previous solutions used by ISPs to temporarily protect their interdomain routing are weak against other attacks. Some of them are quite strong but rely on good management and do not protect large scale attacks. Furthermore, in order to protect interdomain routing, the solution has to consider many parameters that relate to the protocol itself. Thus, there needs to be a few requirements set that define correct operation of BGP as a protocol and speakers. This means that any attack against BGP ought to determine a non-correct operation. The security services that should be provided for proper BGP operation are the authenticity, freshness and integrity of the routing information exchanged. In addition, a BGP speaker's decision process, storing and distribution of routing information must be in accordance with the BGP specification and routing policies established by ASes [50].

Initially, high level requirements should be put in place before setting the more detailed ones. Firstly, any security architecture must not rely on mutual trust amongst subscribers and ISPs. There must be no trust between entities because there are some parties that can never be trusted, and those that can be, are prone to error, misconfigurations or can be apprehended by a malicious adversary. Secondly, the elements of security solutions must exhibit similar dynamics as the parts of BGP they protect. This means that the solution must scale within the BGP architecture and protocol. Moreover, it must be backward compatible, which means that the deployment of the solution can be incremental. Thirdly, the resources required for the solution ought to be in the same range of requirements of memory and processing power for BGP. Thus, the solution should demonstrate similar reliability, efficiency and performance. Fourthly, the security services described before (i.e. integrity, freshness and data origin authentication) must be assured at the traffic itself. For the fifth point, BGP routers should be capable of verifying not only the owner of each prefix that authorised the origin AS, but also that each succeeding AS in the path has been authorised by its predecessor [41].

Following the high level needs, more specific requirements can clarify the objectives for securing BGP. These requirements are well illustrated in [50] by S. Kent et.al. The main concern in BGP is the security of UPDATE messages, since they define the healthiness of routing tables. If UPDATE messages are malicious, then the whole routing infrastructure functions wrongly leading to disastrous communication on the Internet. Thus, to ensure security, the following requirements need to be realised. Firstly, the UPDATE message should be kept integral and authentic. The BGP speaker receiving the UPDATE message must be able to validate that it was sent by the intended peer. Moreover, it can verify that the message was not modified while in transfer and the routing information is fresh and not replayed. Secondly, there must be a mechanism implemented that ensures that the receiver of the UPDATE message is the intended one. Thirdly, the receiving speaker must be able to verify that the sending peer is authorised to advertise routing information on behalf of its AS. As a fourth requirement, there must be a method to verify any prefix advertised in an UPDATE that it was authorised by its parent organisation to own that address space. Fifthly, a BGP speaker receiving an UPDATE message must be able to verify that the first AS in the route was authorised to advertise the prefixes by the owners of their address spaces. Another requirement is the ability of a receiving speaker to verify withdrawals. The verification encompasses the ability to confirm that the peer before withdrawing the route was a legitimate advertiser of that route. Seventhly, a security mechanism needs to be applied to make ensure the well functioning or the BGP decision process and operations. This covers speaker's BGP rules, its AS's routing policies for storage, modification and distribution, decision process, and deriving the forwarding table. Finally, the receiving BGP speaker must apply correctly its decision process and routing policies to decide whether to accept the UPDATE message or reject it. Because the routing policies are not defined in BGP and left to the AS's administration, the last two security requirements are not reliable to securing BGP and should be done separately. If they have to be included, the semantics of BGP itself need to be changed since the protocol does not address this issue.

3. BGP Security Problems

After specifying the security requirements for BGP, security problems can be derived from it. These are the current main efforts that are focused on to provide higher security for the protocol. From the previously derived requirements, the main focus on securing BGP deals with UPDATE messages and the environment that they depend on. As described in [41], T. Vardar has provided three main security problems for BGP: Hop Integrity, Origin Authentication, and Path Validation.

Hop Integrity

Gouda et.al. define in [51] the state of a computer network providing hop integrity. If a router A receives a message M from a router B, the A can check that M was not altered during transmission and is not a replay of an old message [51]. However, BGP does not provide this service. To do so, it needs to provide Data Integrity and Source Authentication.

Messages ought to be verified at each hop to ensure that they have not been altered, replayed, destroyed in both an unauthorised and accidental way. As defined previously, source authentication represents the validation that the sender of the messages is a legitimate one and not an imposter. These are the two services that need to be addressed properly to provide hop integrity.

ORIGIN AUTHENTICATION

This represents the evidence that the data received is the one that should be received. It represents the validation of claims of address ownership from ASes. This will allow a speaker for example to authenticate a BGP peer. Then, it needs to be able to verify that it is authorised to advertise routes. Since the Internet is somehow hierarchical in the provision of AS numbers and IP addresses and prefixes (Chapter 1), this hierarchy should be kept to validate the AS chains of address ownership. This can be used in a PKI (Public Key Infrastructure) format or any means that can provide this service.

PATH VALIDATION

As covered in Chapter 2, a BGP UPDATE message contains a prefix and its associated AS path to reach it. Path validation should allow that the path of ASes is valid and should reach the intended prefix. This means that each BGP speaker in the path must be reachable by the previous one. Moreover, each AS present in the path must be authenticated. This ensures that a malicious UPDATE that contains false routes will not be used.

4. CONCLUSION

To sum up, although BGP was provided with a few security mechanisms, it has not shown that it is safe and secure. Moreover, these mechanisms are independent from the protocol and they represent measures applied only by those who want to. Thus, mechanisms inclusive to the protocol should be designed and implemented. Thus, the security requirements for BGP were defined with the security problems that raise the white flag. However, research has brought us a few still debatable solutions to this issue. In the next chapter, we examine two major solutions (S-BGP and soBGP). We provide an overview of their security mechanisms and how they endeavour to secure interdomain routing and the Internet.

Chapter 5

Solutions for Securing Interdomain Routing

After viewing the different issues surrounding current interdomain routing security in chapter 3, the appropriate security requirements of a better functioning border gateway protocol was covered in the last chapter. Then, the major security problems were defined. Following this, solutions for securing interdomain routing have been researched for many years. Some solutions cover many aspects of the protocol and some cover only a few. In this chapter, two solutions are defined and explained. Then, we compare them in the next chapter providing the advantages and disadvantages of each solution.

The mechanisms built to secure BGP are numerous. However, we cover the two most important and emphasised ones. The first is Secure-BGP (S-BGP) [50]. The concept was developed by S. Kent, C. Lynn and K. Seo and published in April 2000. The second one is secure origin BGP (soBGP) [57]. It was designed mainly by CISCO engineers and published in 2003 as a draft for discussion.

1. Secure-BGP

BGP, as a protocol, has shown many issues concerning messages. The main concern of S. Kent et. al. focuses on the different aspects surrounding UPDATE messages. This is due to their importance over the healthiness of routing tables. The first subsection describes the design overview of the solution. Then, the security mechanisms are covered followed by the proposed deployment of S-BGP.

Design Overview

Secure-BGP is based on three different security mechanisms that endeavour to satisfy the BGP security requirements. The S-BGP architecture uses Public Key Infrastructures (PKIs), Attestations, and IPsec.

The first is **Public Key Infrastructure** (PKI) [52]. Key management in a large scale such as the Internet necessitates the existence of public key cryptography where every AS is provided with a pair of public and private key. This will need a public key infrastructure for key management. The hierarchy required will follow the same scheme as the Internet's. Thus, the root **Certificate Authority** (CA) is IANA/ICANN. The latter provides keys for RIRs (i.e. Regional Internet Registries – Chapter 1) which in turn supply keys for major ISPs and so on [53]. These asymmetric key pairs are used extensively in many security solutions. This can provide confidentiality but the major concern is integrity and origin authentication. The cryptographic mechanism that provides these security services is digital signatures [25]. When a speaker sends a message, it signs it with its private key (i.e. signature key). When the peer receives it, it can verify it with the public key (i.e. verification key) of the sending speaker. S-BGP considers the use of **Digital Signatures with appendix**. The latter includes hashing the message and signing the digest itself. This will decrease processing power and memory usage. PKI and digital signatures will help provide secure identification of BGP speakers, ASes and address blocks. Moreover, it will support AS number ownership and BGP router authorisation to represent an AS.

The second entity S-BGP relies on is the use of **Attestations**. The latter form a trivial part of S-BGP since they are used to encapsulate authorisation information within UPDATE messages. This will use digital signatures ensuring authenticity and integrity of data provided in those messages. Moreover, they will be utilised to check that each AS along the path had been authorised to advertise the route by the previous AS. In addition, attestations will be used to verify that the advertising AS was authorised by the owners of the IP prefixes contained in UPDATE message to advertise them. For backward compatibility, attestations ought to be carried in an optional transitive attribute. It will contain digital signatures covering the whole route. Since there are two objectives, two types of attestations will be required. The first type is **Route Attestations** and issued by ASes. The second type is **Address Attestations** and issued by the organisation that owns the prefix. Further explanation is provided in the next section.

The third component is **IPsec**. It is used to secure point-to-point communication between BGP speakers. As stated in the last chapter, it provides different services: integrity, anti-replay and anti-DoS attacks. These are the security services required for update messages. Confidentiality can be provided by IPsec but it is not a fundamental requirement for interdomain routing itself. It is applied at the IP layer and can detect quickly DoS and replay attacks. It has proven great stability when implemented and used in VPNs (Virtual Private Networks).

Proposed Security Mechanisms

As stated in the last section, the approach adopted encompasses PKIs, Attestations and IPsec. It involves two Public Key Infrastructures and a new attribute enclosing attestations. Moreover, it includes the use of IPsec. These modules are used by every BGP speaker to fulfil the security requirements. This section covers in more detail these security mechanisms implemented in S-BGP.

S-BGP relies on the use of PKIs, based on X.509 (version 3) certificates [54, 55]. They use the hierarchy and delegation present in the Internet, starting at the top of the pyramid IANA/ICANN and then the regional registries followed by major ISPs and so on. Having the PKIs matching the same infrastructure as the Internet authoritative system saves a lot of time and a large cost. Moreover, it keeps the solution away from trust issues which is a major concern in PKIs. As shown in Figure5.1, ICANN/IANA delegates its authority to its regional registries RIRs. The latter do the same to Large ISPs, then to DSPs or organisations. IANA/ICANN or RIRs can directly assign public key pairs to organisations depending on the circumstances.

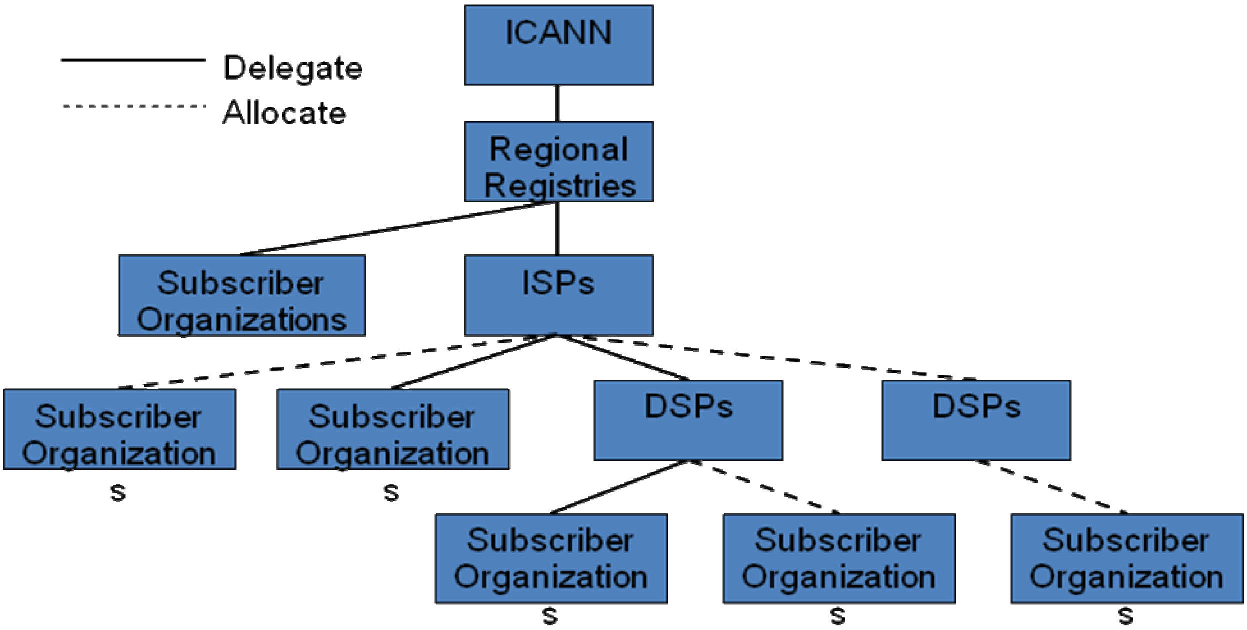


Figure5.1: PKI Delegation Hierarchy and Allocation Structure

There are two different PKIs used in S-BGP. The first one is a PKI for Address Allocation which is used to issue certificates relating to address assignments. The second is a PKI for Assignment of ASes and Router Association. This is responsible to provide the authority level of speakers and ASes through certificates.

Address Allocation PKI

This PKI is used to issue certificates to each organisation that is given rights of a portion of the IP address space. It mirrors the same hierarchy as the Internet. This means that the root CA is IANA/ICANN followed by RIRs. The RIRs delegate authority to corresponding ISPs

(Internet Service Providers), DSPs (Data Service Providers) and end users. This architecture does not require that an address assignment has to be signed and certified by all the upper hierarchy since it is a delegated authority. If an ISP provides and certifies an address space for its customer, the latter does not require certification from registries or the root CA (i.e. ICANN). Moreover, any subscriber or DSP that does not contribute in BGP routing information exchanges is not issued with a certificate.

As address blocks are assigned to organisations, certificates are done in a similar manner. Every address block is bound to a public key that belongs to its organisation. These certificates provide proof of ownership of the address blocks. Every certificate encloses an extension specifying the set of address blocks allocated to the ISP, DSP or subscribers. Hence, ICANN, as the root CA, issues itself a certificate asserting ownership of all the IP address space on the Internet, as shown in Table5.1. Then, it issues certificates for RIRs and hands over IP address blocks to them, as illustrated in Figure5.2 [56]. RIRs are consequently given authority to certify ISPs, DSPs or subscribers that are directly linked to them (i.e. they directly assigned address blocks to them). A RIR assigns address blocks and certifies for example an ISP with address blocks. In turn, the ISP is delegated and has the authority to assign IP address blocks to its customers and those that use BGP are provided with a suitable certificate.

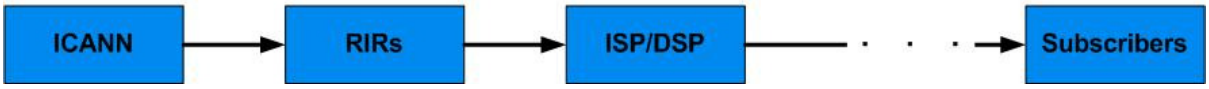


Figure5.2: Certification path in Address Allocation PKI

Type	Subject	Signer
Root	ICANN	ICANN
Registry	RIRs	ICANN
ISP/DSP	ISP/DSP	RIRs/ICANN
DSP/Subscriber	DSP/Subscriber	ISP/RIRs/ICANN

Table5.1: Address Allocation PKI Certificates

AS Assignments and Router Association PKI

For this PKI, three certificates will be required. The first two are used to authenticate ASes and BGP speakers; and the third is used for the authentication of the relationship between those two entities (i.e. ASes and speakers). For this PKI, the hierarchy of authority is a bit different. The root CA stays ICANN and the RIRs come after it. Nevertheless, the third tier contains organisations that own ASes. Then, it is followed by a tier containing AS numbers and routers, as illustrated in Table5.2.

Type	Subject	Issuer/Signer	Extensions
Root	ICANN	ICANN	All AS numbers
Registry	RIRs	ICANN	Allocated AS numbers
AS Owner	ISP/DSP/Subscriber	RIRs/ICANN	Allocated AS numbers
AS	AS DNS number	ISP/RIRs/Subscriber	AS number
BGP Speaker	BGP Speaker DNS name	ISP/RIRs/Subscriber	AS number and Router ID

Table5.2: AS and Speaker PKI Certificates

The assignment process is similar to the one used for the previous PKI. At the top of the hierarchy and root of trust is ICANN, as shown in Figure5.3 [56]. It assigns AS numbers to RIRs, which in turn assign ASes to the third tier which is composed of ISPs, DSPs and also Subscribers, also called AS owners. They in turn provide certificates for authenticated ASes. Moreover, they issue certificates for BGP speakers that encompass the AS number, router name and router ID. This proves that the BGP speaker belongs to the AS it is originating from.

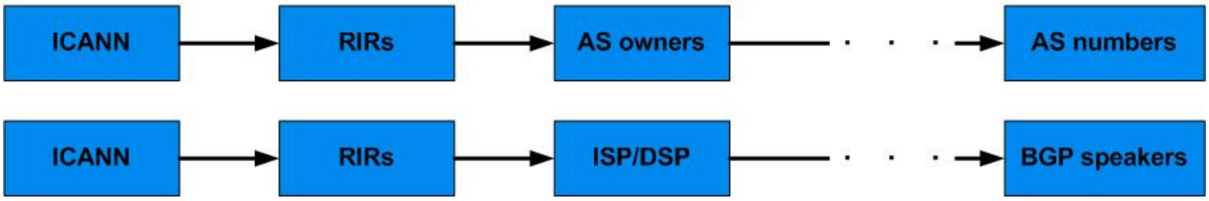


Figure5.3: Certification paths in AS number and BGP speaker identification PKI

ATTESTATIONS

After covering the different PKIs required for S-BGP, the goal of the asymmetric key management infrastructure is to use the certificates and keys to build Attestations. The objective is to prove that the AS that made the attestation is authorised by its issuer to advertise a path only in accordance to a specific address space. As defined by S. Kent et. al. in [50], there are two classes of attestations: **Address Attestations** (AA) and **Route Attestations** (RA).

Address Attestations are used to ensure that the advertising AS is authorised to send UPDATE messages. The organisation or the AS owner signs the AA, containing the AS as a subject, with its private key. It also provides its Certificate containing its public key with the AA. The AS Owner confirms that the AS is authorised to announce certain IP blocks of address space. This proves that the organisation in effect owns the address space. Thus, the receiver has the ability to verify the certificate, and then validate the signature within the AA. If there are many ASes per organisation, everyone should be provided with its own AA since each of them has its own address space and represents a different entity in the routing infrastructure.

Route attestations are carried in a new BGP optional attribute added to the UPDATE message. For this type of attestation, the subject has to be a transit AS. It can be signed offline by the management of the AS. However, it is preferred to be dynamically signed by the S-BGP speaker, by using the AS Assignments and Router Association PKI. It uses the private key that corresponds to the certificate that binds the BGP speaker to the subject AS to sign the RA. As described in [49] and shown in Figure5.4, a RA can result in an “onion style” attestation containing signatures from all routers along the path. When a speaker receives an UPDATE message, it validates it then signs it before sending it to its peer. When its peer receives it, it does the same before advertising it. This way, RAs provide path authentication.

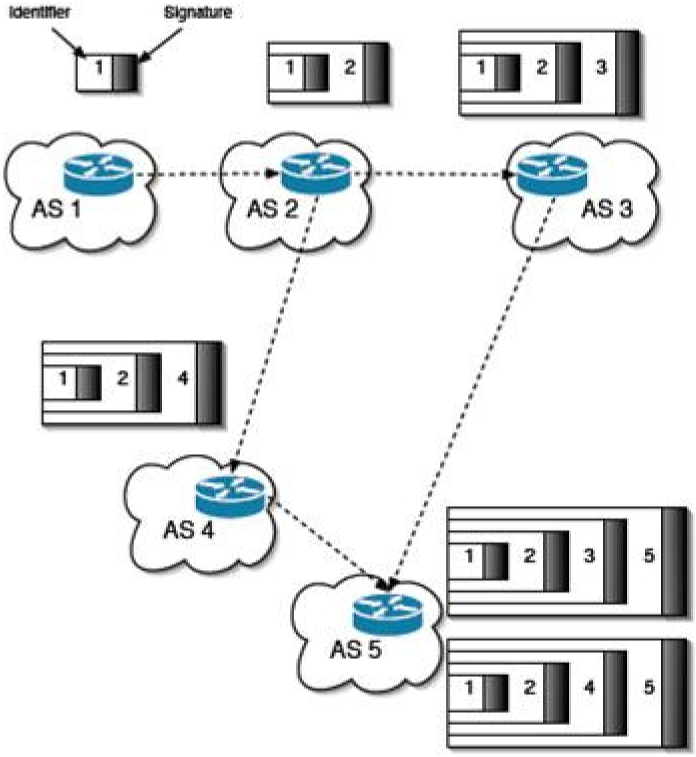


Figure5.4: Route Attestations [49]

ROUTE VALIDATION

To validate a route, attestations and certificates are used in conjunction to verify the chain or attestations in the path. This starts from the last AS that advertised the route to the first one. When the first one is validated, it means that each subsequent AS in the path has been authorised to advertise the route for the appropriate address blocks by the previous AS along the path.

For an AS to verify and validate a route received from its preceding AS, there needs to be four components available. First, there has to be one AA from every organisation owning an address block in the Network Layer Reachability Information (NLRI). The second entity is the certificates that have to be included with each AA. Thirdly, RAs from every speaker or AS which are present in the path need to be provided. The last entity is the certificates specific to route attestations. When a speaker receives an update, it uses the certificates provided with AAs to check if every AS or speaker has been given the authority to advertise a route in the address space provided in the UPDATE message. Then, it uses the second certificates to verify RAs one by one until it arrives to the source AS. All the certificates are checked against all relevant **Certificate Revocation Lists** (CRLs). CRLs are lists of certificates that are expired and must no longer be used. If a certificate is found in a CRL, the route is ignored and the UPDATE is dropped.

Attestations are only used for route advertisement. They are not used for route withdrawals since the authorisation of advertisement was already verified at the time of the UPDATES registered in Loc-RIB. Furthermore, if a BGP speaker is no longer authorised to advertise a route, the latter is no longer valid and ought to be removed. S. Kent et. al. state that the way to protect route withdrawal replay or spoofing is to use the IPsec on inter-router communication.

IPSEC

S-BGP has been armed with IPsec to overcome the issues of replay attacks; spoofed, lost or malformed packets based attacks. This aims at protecting the issues encountered with TCP is based attacks in the lower layer (i.e. Internet/Network Layer). The major problem with employing IPsec is key management. Since S-BGP provides the required PKI, the one established for BGP speaker and AS authentication is enough to provide the necessary certificates. S-BGP will use Encapsulating Security Payload (ESP) with NULL for encryption. This will provide authentication, data integrity and anti-replay mechanisms for the BGP session established. Authentication Header was not selected because the author claimed that it was not efficient. Internet Key Exchange will be used for dynamic key establishment and exchange, which will provided an added value of security comparing to the previous TCP MD5 authentication.

Proposed Deployment Mechanism

In order to deploy S-BGP effectively, collaboration of many groups in the Internet community needs to take place. First of all, main ISPs are obliged to implement the security mechanisms of S-BGP. Furthermore, ISPs and subscribers need to generate and distribute AAs in a collaborative way. IANA/ICANN needs to improve its system in order to generate certificates for ASes. RIRs are given the same responsibility and thus required enhancement of their processing and storage. In addition, BGP speakers need to be upgraded with supplementary storage and their software needs to be upgraded to support the security mechanisms.

S-BGP is incrementally deployable. However, non-neighbour ASes will have issues in exchanging RAs because of the required storage. The latter ASes will not have sufficient storage in their RIBs. However, neighbour ASes will gain full advantage of S-BGP from deployment. Moreover, because of the hierarchy imposed in S-BGP, only contiguous deployment ought to be attempted because of the complexity of a random non-contiguous one. Furthermore, if an AS switches one of its border routers to S-BGP, all the other should follow. This is required in order to preserve a regular and steady view of exterior routes. Moreover, this will avoid occurrence of loops to the AS.

2. Secure Origin BGP

After covering S-BGP, the other well-known solution is secure origin BGP (soBGP). soBGP covers roughly similar issues as S-BGP. The main concern of R. White et. al. is to deal with UPDATE messages and authenticity of the route advertised. Similar to S-BGP, we first cover the design overview of soBGP. Then, we describe in detail the security mechanisms or countermeasures adopted followed by the proposed deployment of such solution.

Design Overview

Secure origin BGP was not designed to overcome the security issues of the communication between routers. Instead soBGP proposes the ability of a speaker to verify the authorisation of an AS to advertise IP address blocks, which is a similar aim of S-BGP. Moreover, it endeavours to validate the path from the advertising speaker to the receiving end. This is also a similar approach to S-BGP which is route validation. In addition, soBGP aims to verify the policies of the originating AS regarding any particular block of IP addresses [57].

Similar to S-BGP, secure origin BGP requires a key distribution mechanism similar to Public Key Infrastructure. First, to authenticate each participant, soBGP will use a certificate that binds an AS number to a public key matching a private key to be used for signing other certificates. Second, the solution will include a way to verify that an AS is authorised to advertise a certain address block. Same for this situation, a certificate needs to be created that binds an AS to the IP address blocks that it is allowed to advertise. The design of soBGP contains three types of certificates. The last one is unique compared to S-BGP and it relates to the BGP policies. It is a certificate that describes policies related to specific blocks of addresses. In addition, it relates the connections between the advertising AS and its neighbours [60].

For a speaker to validate a path, a different approach is taken by soBGP. The design considers building a topology map of the paths of the entire internetwork. Every AS in the internetwork needs to build a certificate that includes a list of all its peers. Then, after considering a list of all transit peers, the outcome is a map of the AS entities in the internetwork [60]. Moreover, soBGP tries to take advantage of the existing Internet Architecture. It uses for example the trust relationships, loose AS associations and more. Furthermore, secure origin BGP has designed its protocol in a way that a new type of message for BGP is required. It aims at creating a security based message.

Proposed Security Mechanisms

As stated in the last section, the approach adopted encompasses key distribution system and different certificates. The key distribution system manages three types of certificates. The first aims at authenticating ASes. The second provides the authorisation mechanism. The third provides extra security to policies and ASes relationships. Moreover, a fourth certificate provides a way to build an internetwork topology map. This section covers in more detail these security mechanisms implemented in soBGP.

AS Authentication

The most important point to start with is to have a secure way of authenticating peers. soBGP overcomes this issue through the use of a certificate dedicated for AS authentication between peers. This certificate is called **Entity Certification**, or **EntityCert** [60]. An EntityCert binds an AS number to a public key(s). The key created is an asymmetric public/private key pair. The private key that corresponds to the public one is used by the AS to sign a range of other certificates. EntityCert is classified as an X.509v3 certificate similar to the ones used by IPsec. In order to know that the key provided in the certificate is effectively the one of the advertising AS, soBGP involves a Trusted Third Party (TTP) to approve and sign EntityCert.

Web of Trust

Since a TTP needs to be involved, there is a problem of creation of the trust. If there needs to be a signature from a trusted party, which entity signs the EntityCert of that trusted party? If we follow this chain, the "chicken and egg" causality dilemma rises. soBGP uses a concept that more or less covers this issue. A number of keys is distributed and configured manually to have a high level of trust. They are completely trusted by any AS since they were verified and authenticated beforehand, such as top-level backbone service providers and key authentication service providers [60]. As shown in Figure5.5, the trusted AS can used its key to sign EntityCerts of other validated ASes. Then, the web of trust can start where the new trusted ASes can sign other ASes entity certificates after validating their authenticity. This way, these EntityCerts will form a web of trust based on top-level trusted entities.

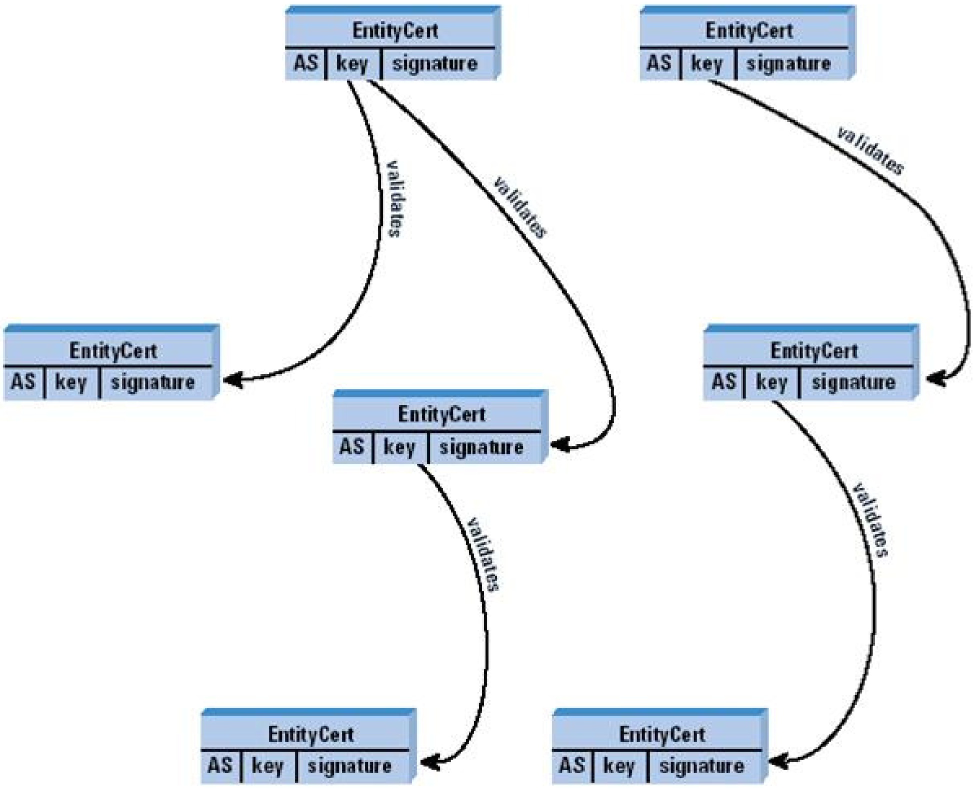


Figure5.5: Web of Trust in soBGP [57]

ADVERTISEMENT AUTHORISATION

Having the web of trust in place with EntityCerts provided for ASes, providing a proof for each AS that they are authorised to advertise certain block of addresses is the next step. soBGP uses another certificate to provide this security service. **Authorisation Certificates** or **AuthCerts** are used to bind an AS to the IP address space able to advertise [60]. Figure5.6 [57] illustrates an example of AuthCerts. In this example, the top AS gave the authorisation to AS number 65000 to advertise the prefix 10.0.0.0/8 by signing the authorisation certificate with its private key. Then, AS 65000 has the ability to delegate part of its address block to another AS. AS 65000 binds AS 65001 to the address space 10.1.0.0/16, by signing an AuthCert with its private key. This means that AS 65001 now has the ability to advertise within its address space. This is a delegation from AS to AS 65000 and from AS 65000 to AS 65001. The latter can also do the same as seen in Figure5.6 [57].

This way, any speaker or AS receiving these AuthCerts can verify with the public key of each AS the authenticity of AS and the delegation process provided to AS 65000, AS 650001 and AS 65002. This means that the speaker can check the validity of the authorisation by verifying up through the chain until it reaches the top AS, which is trusted or can be verified through its EntityCert.

To minimise the number of certificates, soBGP allows certifying blocks of addresses rather than prefixes within them. Hence, this will reduce the processing power and storage capacity required for ASes. soBGP also allows certifying single prefixes which can conclude into as many authorisation certificates as required.

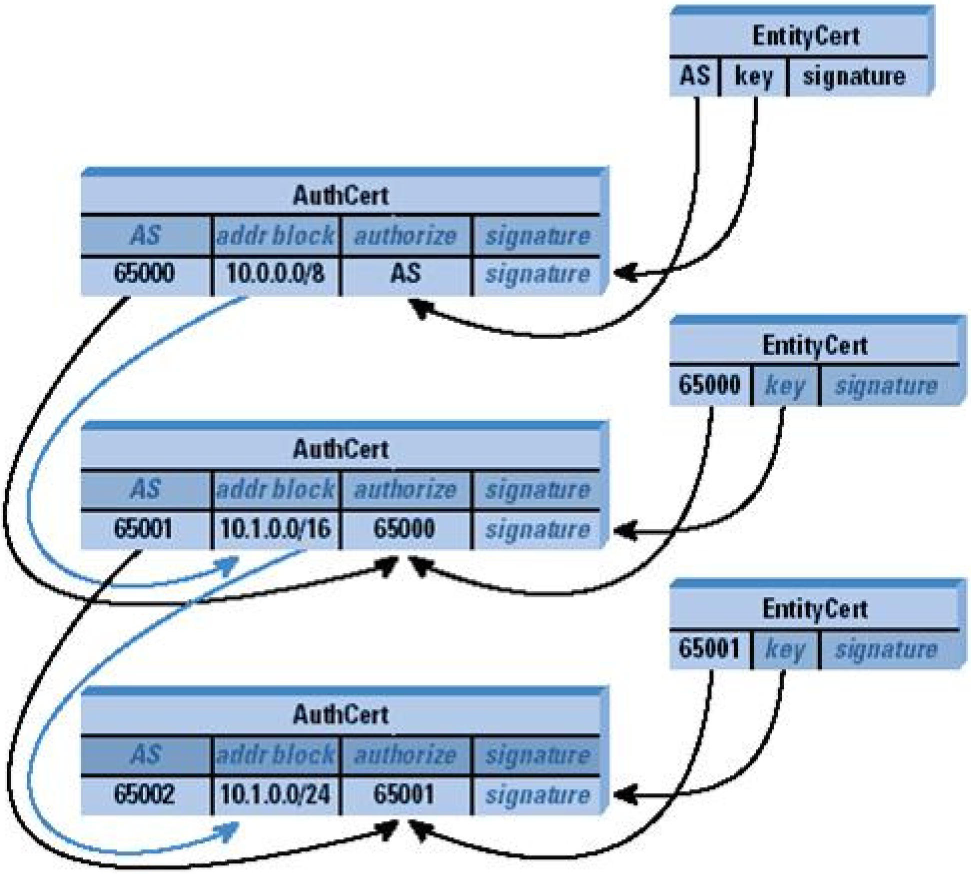


Figure5.6: Advertisement Authorisation Mechanism Example [57]

Secure origin BGP provides a higher depth for its certifications. Authorisation certificates are not advertised independently, but encapsulated into certificates that include a set of policies the originator enforces to the advertised prefixes. **PrefixPolicyCerts** enclose an authorisation certificate, the policies applied to the prefix within the certificate, and a signature signed by the authorised AS.

The policies that can be included are unlimited. They can include a list containing ASes not allowed to be present in a path destined to the address block. Moreover, it can include the maximum length of the prefix that can be allowed. The policies are versatile and flexible. The issue with them is the ability of enforcement of those policies received by other ASes. For a better functioning of this security mechanism, all ASes should follow with a 'MUST COMPLY' to prefix policies principle.

Topology Map

Secure origin BGP designed a way to verify that a given advertiser AS of a route has a real path to the destination. This is also solved through the use of certificates named **ASPocilyCerts**. Every AS creates this certificate by signing with its private key a list of its peers. This way, an internetwork topology map is assembled, as shown in Figure5.7 [57]. In the diagram below for example, AS 65003 sends an UPDATE message to AS 65005 claiming it is capable of reaching AS 65004 through the path {65003, 65001, 65004}. The receiving AS (i.e. AS 65005) can verify that AS 65003 has revealed concrete information. AS 65005 checks the ASPolicyCert of AS 65003 ensuring that it is connected to AS 65001, then the ASPolicyCert of AS 65001 validating that it is connected to AS 65003. It continues with a similar check for the link between AS 65001 and AS 65004 through both of their ASPolicyCerts. This way, it ensures that similar information is provided from both sides of the link and accepts the UPDATE. If the information provided by a speaker is wrong, the message will be directly dropped.

In addition, the use of this procedure can increase the level of flexibility through the addition of policies. This mutual similarity check can be combined with policy statements. For instance and following our previous example, AS 65001 can have a non-transit policy. This means that if AS 65003 sent the same AS 65004 reachability path (i.e. {65003, 65001, 65004}) to AS 65005, the path is wrong since AS 65001 does not allow transit traffic to flow. When AS 65005 starts checking ASPolicyCerts, it will know that AS 65001 has a no-transit policy and therefore the path is not valid. The receiving AS will drop the UPDATE message immediately.

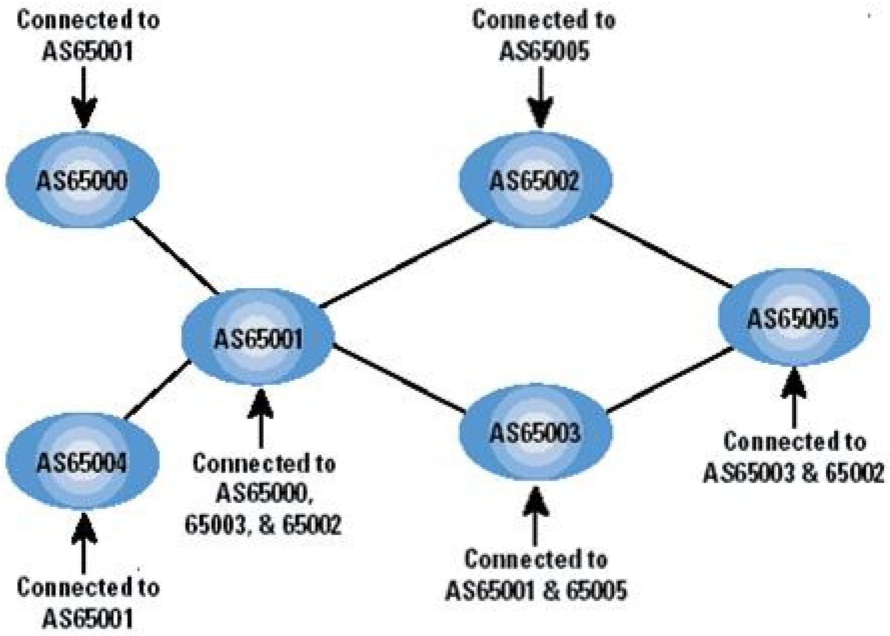


Figure5.7: Connectivity Topology Map Example [57]

COMMUNICATING CERTIFICATES

All the previous mechanisms have been discussed. They comprised of a set of certificates able to provide many security services relating to BGP. The only point left is the way these certificates will be communicated. Secure origin BGP designed a new BGP message that handles the transportation of those security mechanisms. The new SECURITY message is to be used to carry specifically soBGP certificates [58].

Prior to starting a BGP session, peers may negotiate and decide on the exchange of SECURITY messages. When the latter is negotiated and accepted, a SEURITY option message must be exchanged before any certificates or any other information is sent. Then, the speakers exchange the soBGP certificates in their local database. J. Ng has provided a more detailed explanation of what SECURITY message contains in [58].

PROPOSED DEPLOYMENT MECHANISM

Secure origin BGP provides three different examples of the way to deploy the solution. soBGP wants to prove that it can provide various options since it is not dependant on transportation nor on a yet to be built centralised set of servers. Majorly, soBGP deployment encompasses the distribution and supply of certificates [59].

The first proposed option requires routers to be able to conduct cryptographic functions and validate them (i.e. certificates and signatures validation). The certificate exchange will be done between peers themselves. Then, they must be able to validate them and carry all the mechanisms required by soBGP [57].

The second solution is meant for a situation when routers are not able to conduct cryptographic functions or the processing is too slow. BGP speakers would only exchange certificates and forward them to internal servers. The latter will verify and validate all received certificates. When a border router receives an UPDATE message, it can query the appropriate server for the validity of the message. Then, the speaker can proceed depending on the reply of the server [49].

The final proposed option does not rely on the routers forwarding security information to servers. However, internal servers communicate directly via a multi-hop session. This way, they can exchange certificates and process them. Then, border routers query the servers to validate receive UPDATE messages.

3. Conclusion

After covering those two solutions, S-BGP and soBGP provide differently their security countermeasures. Although they use the same primitives they rely on different architectures and designs. Therefore, both of them perform differently and secure the protocol differently. In the next chapter, we look at cover similarities and differences of these protocols in many parts of the solutions. Moreover, we provide qualities and drawbacks of S-BGP and soBGP along the way.

Chapter 6

S-BGP VS. SOBGP

After describing two actively researched solutions for securing interdomain routing, we need to compare them. The comparison includes the similarities and differences of those two protocols. It covers to what extent the security requirements are met through the different mechanisms involved. Moreover, we provide the residual vulnerabilities left when deploying each solution. After that, deployment and performance issues are examined. In the comparison, we analyse along the way advantages and disadvantages in each section.

1. SECURITY MECHANISMS

S-BGP and soBGP were designed to overcome certain security issues in interdomain routing. They both tackle the problems differently with a few similarities. In this section, we discuss the similarities and differences of the security mechanisms used in these protocols.

CRYPTOGRAPHIC MECHANISMS

S-BGP and soBGP both rely on the use of the same cryptographic mechanisms to build the entities that form the security modules. They both rely on asymmetric cryptographic functions. They use digital signatures to sign data and produce certificates. This is used to provide data origin authentication of the information exchanged. Every AS would be required having a public/private key pair.

In S-BGP, it is essential for an S-BGP speaker to be able to sign messages (i.e. conduct digital signatures on data). The requirement is mandatory because speakers are required to dynamically sign all S-BGP UPDATE messages. Moreover, they must have also the ability to verify and validate messages. This is one of the main issues of S-BGP because it will necessitate more processing power and a lot of storage when deployed. Thus, the level of security is higher but at an elevated cost.

However, soBGP does not obligate its speakers to have the ability to conduct excessive cryptographic operations. First of all because it does not dynamically sign UPDATE messages but uses a new SECURITY message. Secondly, it has different options of deployment that can prevent speakers from performing digital signatures and verifications. This way, soBGP is lighter but the security mechanism is not as dynamic as the one applied in S-BGP.

Therefore, S-BGP and soBGP rely on the same cryptographic primitives. However, the extensiveness of their use is dissimilar. While S-BGP requires a signature at every UPDATE, soBGP has a set of certificates that it uses in a relatively more static manner. We can state that, obviously, there is a tradeoff between security and cost.

Key Distribution

For both of these solutions, key distribution is a key factor to both the security and deployment aspects. Although the certificate type is similar for both (i.e. X.509v3), S-BGP and soBGP use different mechanisms for distribution. The difference occurred perhaps because of the historic issues discussed on the method used for S-BGP. However, there are issues on both sides.

S-BGP uses two different PKIs but parallel to each other. The first is the address allocation PKI, used to deploy asymmetric key pairs. The latter are used to generate certificates and most importantly Address Attestations. They aim to provide origin authentication by binding the address bock(s) to the source AS. The second PKI is used to assign ASes and bind routers and organisations to them. This aim is fulfilled through the use of certificates. Moreover, the keys provided by this PKI are used to sign Route Attestations which provide route validation. The issue regarding the approach taken by S-BGP is that it relies on a **single point of trust**. Following the hierarchy of authority in the Internet, it is the best way to apply a PKI since the infrastructure of authority is already present. However, the issue that rises is the possibility of one of the entities in the top of the pyramid to be compromised. For instance, if the private key of IANA/ICANN is compromised, attackers can create their own public private keys with their own AS number and IP prefix. This has a very low probability of occurrence, but still is a possibility. Moreover, the cost of PKI is very high and requires extra storage and special hardware for critical organisations, such as HSMs (Hardware Security Modules).

Secure origin BGP uses a rather different approach. It relies on a distributed web of trust. It starts with initial trusted certificates in key organisations. Then, using those certificates, trust is provided to other entities, realising a web of trust. The advantage of this model is that it provides distributed responsibility. This avoids the single point of trust issue that SBGP has with its PKI. However, the trust model is fuzzy. The conditions or trust model does not provide a certificate. In this web of trust, signatures have unclear semantics. Moreover, the issue is that transitive trust is assumed and allowed. Although flexible, this makes the web of trust weak and vulnerable to malicious users or intruders to the system.

To sum up, PKIs in S-BGP offer better security level than soBGP. However, they are more complex and expensive to implement and deploy. Although, the web of trust of soBGP is more flexible and avoids the issue of a single point of failure; the trust is distributed and therefore harder to manage and quantify the security level. Moreover, its definition is still fuzzy and the security level is still debatable. Yet again, there is a tradeoff issue between security, complexity and cost. However, S-BGP is better suited for key distribution.

Security Entities Exchange

S-BGP and soBGP have different ways to transport the new security related data. This is a crucial point because the requirement for both solutions is to be able to adhere to the backward compatibility principle.

Secure origin BGP uses a new SECURITY message. This is message will be used to transport security related data (i.e. certificates) to peers. The advantage of this is that it does not interfere with the BGP-4 protocol. All four messages stay the same and no change will be applied. However, a new message appears and requires addition to the protocol. Thus, it will require special negotiation with routers that use soBGP. If this is not conducted carefully, many routers will receive SECURITY messages that they do not understand and therefore drop the session. This will cause RFD which will in turn generate a denial of service.

Secure-BGP, in turn, uses a different approach. It adds a new attribute to the UPDATE message that would transport its certificates and signatures. The advantage of this approach is that no new message is added to the protocol and speakers need not to be updated. Moreover, the attribute is optional transitive. This means that it will be transported to the speakers that might use it. Furthermore, no additional negotiation needs to be established concerning the messages exchanged. In addition, S-BGP signs all its messages, providing dynamic data origin authentication.

Therefore, the best solution that does not require additional design issues is S-BGP new path attribute. However, in terms of performance, soBGP does better. In terms of security level, S-BGP provides a better dynamically signed message. Nevertheless, every message required cryptographic processing, which leads to more processing power and memory needed.

2. Security Achievements

Both of these protocols were designed to overcome the issues that surround interdomain routing security. The fact that they have been designed differently, the led to different security achievements.

S-BGP uses its mechanisms to overcome the security issues discussed in Chapter 4. Origin authentication is provided by utilising PKI and AAs. In S-BGP, address attestations are used to authenticate organisation’s ownership of IP addresses. Path validation is accomplished through RAs. These attestations are used to verify the path information by a transit AS. When these are combined with certificates from the PKIs, a speaker becomes able to authenticate every AS in the path and its authority to advertise the address blocks in the UPDATE message. In addition, hop integrity is supplied through IPsec with integrity and source authentication for every hop. However, there are other issues that are not covered so far by this protocol. Route withdrawal is not covered by the security mechanisms adopted by S-BGP. Moreover, there is the issue of the requirement of route updates.

Compared to S-BGP, soBGP is a lightweight solution. Similar to S-BGP, it relies on strong security mechanisms such as certificates and signatures. It provides source authentication of messages through its entity certification. However, there is still the issue of integrity of messages which is not ensured since it uses the new SECURITY message. Route validation is met at a very weak level. soBGP provides a static path plausibility rather than authenticity. Moreover, it does not provide hop integrity, claiming in the paper that it was not part of the problem [57]. Although it provides a policy checking mechanisms, it becomes more complex when more policies come into play. Furthermore, both path authentication and policy checking require an additional topology database and policy database respectively. This would increase complexity and dependence on many entities.

In terms of level of security, S-BGP dramatically takes the lead. Although it has not covered all of the issues, it provides well structured and secure measures. The issue with S-BGP is complexity, especially with the PKIs. As quoted by Prof. S. M. Bellovin: *"Complexity is the enemy of Security"*, the issue that S-BGP encounters is cost and ability of routers used nowadays to scale with its performance requirements. However, soBGP is more lightweight and therefore is a better choice on this side. However, it failed to even provide a proper path authentication, which is a crucial part of the protocol. While S-BGP protects against attacks anywhere along the path, soBGP can only protect against attacks or misconfigurations done by the originator of a prefix announcement.

3. Residual Vulnerabilities

Both solutions aimed at providing certain security measures that should surmount the vulnerabilities present in BGP. They both succeeded in some aspects. However, they failed to achieve some of their goals.

Route withdrawal in S-BGP is not protected by any means. A malicious BGP speaker is able to delete routes if it can spoof a session with an ordinary speaker. The use of IPsec can detect replay attacks that lead to loss or disorder of packets. However, if a speaker is compromised, no mechanism forces it to transmit UPDATES, especially for route withdrawal. Although it is not a priority, passive sniffing is not protected by the protocol. It can be, if ESP in IPsec is enabled which provides confidentiality. RAs (Route Attestations) provide proof of validity of routes. However, they do expire. This is an issue because routes withdrawn can be reasserted by a malicious speaker. This is because BGP does not protect the sequencing of UPDATE messages through sequence numbers for instance. This issue can be overcome, if a mechanism and a database, similar to the CRL one, is included for expired attestations. In addition, ensuring that BGP speakers, exchanging UPDATEs, are applying BGP rules and policies accordingly is not addressed by S-BGP [50].

Secure origin BGP has succeeded only in a few aspects. However, there are many issues that have been weakly overcome, or left untouched. soBGP does not protect the hop integrity. This means that it does not indicate any mechanism that can be used to guard peering sessions. Moreover, it claims that it provides path authentication or validity. However, it only provides plausible paths statically authenticated. This means that guarantee for security is very low. soBGP works through certificates transported in the new SECURITY message. Therefore, UPDATE messages are not authenticated and can be replayed or misused. In addition, soBGP does not provide a mechanism that identifies bad certificates, like CRLs for S-BGP. The issue that arises is how it will deal with certificates that are expired or reported to have been used maliciously. Finally, as S-BGP, soBGP does not provide a mechanism that overcomes passive wiretapping, correct application of policies, and some replay attacks.

To sum up, there are still residual vulnerabilities for both protocols. However, they are clearer in S-BGP and some solutions for them have been given in the definition. Although soBGP tries to include policies in its solution, it fails in providing the most important security service which is path validation. Moreover, it does not protect peering sessions and all residual vulnerabilities of S-BGP apply to it as well.

4. Deployment

After designing and implementing a solution, it needs to be deployed. It is one of the most crucial points of interdomain routing because of the large scale of the Internet. Both soBGP and S-BGP are incrementally deployable. However, they both hold a nebulous effectiveness when deployed incrementally. They cannot succeed completely, until fully deployed.

The major issue surrounding S-BGP deployment is performance. This solution requires most entities that play a role in interdomain routing to be enhanced. Routers should be upgraded in memory, processing power, storage, and with the security mechanisms required (i.e. new attribute including the processing mechanisms). ISPs and DSPs should also include safe key management. The cost of this is high and requires special hardware such as HSMs. Moreover, Registries and ICANN need to be protected immensely and provided with storage requirements for the keys and certificates. In addition, collaboration of many groups in the Internet community needs to take place. S-BGP is less incrementally deployable since it requires at least a few tiers in the hierarchical pyramid to be fully operational [67].

soBGP provides three different ways for deployment. It is more flexible than S-BGP since it is able not to rely on routers. It can use extra servers in each AS that can perform the validation of the different certificates. Moreover, it is really incrementally deployable because it only requires a few speakers to be given prior trust to. Although, the security is soft and still debatable, it requires less expensive cryptographic functions. These options grant soBGP greater ease and flexibility of deployment. However, this can create interoperability issues [66].

The flexibility of deployment of soBGP gave it a plus in comparison to S-BGP. The latter requires many prerequisites before it can be operational. However, soBGP can become fully operational without the need of as many requirements as S-BGP. Although soBGP shows quicker deployment, the latter is fuzzy and can lead to issues of interoperability in peering sessions. Coming back to our point, more security leads to more complexity. Thus, S-BGP offers greater security level than soBGP but the expense for deploying it is much higher.

5. PERFORMANCE

Generally, performance degrades when offering security services. S-BGP and soBGP try to overcome the security issues with less impact on the performance on BGP. However and not surprisingly, it is not the case for both of them, although one performs faster than the other.

Although S-BGP provides the most complete security solution compared to soBGP, it performs disastrously. First of all, S-BGP requires extensive cryptography at every message sent. A performance study regarding S-BGP has found that the added overhead is equivalent to the processing power (CPU) and memory provided by a personal computer [67]. Thus, the hardware requirement is not that large. However, the security added will require more bandwidth in order to perform at the BGP standard. Moreover, transmission bandwidth required can increase dramatically. Obviously, the overhead is higher in large ISPs because they are prompted and queried more than other organisations. On the whole, S-BGP is the best solution in terms of meeting the security requirements; but this pays the price. It performs much slower and requires more resources.

On the contrary, soBGP performs faster. It tries to mitigate the cost of signatures by long term authentication of routing elements. All authenticated data is signed, validated and stored at routers before starting the peering sessions. Moreover, all security related data is transported in a new message. soBGP does not extensively signs all updates and exchanges like S-BGP. Thus, the performance of soBGP is higher. Moreover, certificates are validated locally rather than through a PKI. Although the security is defined as soft and questionable, it gives advantage to soBGP on performance over S-BGP.

Thus, soBGP is more lightweight than S-BGP. This gives it a better performance in terms of processing power, memory and bandwidth. However, this has to pay the price of an unclear security level. S-BGP provides the most complete solution for securing interdomain routing. However, it is still questionable whether their resources requirements are much heavier than the infrastructure can sustain.

6. Conclusion

After comparing both S-BGP and soBGP, it is vital to come up with a conclusion about the solutions. In terms of security, S-BGP is far more complete than soBGP. It provides clear security requirements that work well theoretically. It arms BGP with security mechanisms that authenticate dynamically the path and ASes. Moreover, it uses IPsec for peer-to-peer communication. However, the complexity in S-BGP is immense. This leads to slow performance and convergence. Moreover, deployment for S-BGP is still questionable about its practicality. Although soBGP is lightweight and overcomes some of these performance issues, it only provides good origin authentication of ASes. Moreover, it does not afford dynamic path authentication. It can only cover a static path plausibility service. This means that paths can be changed and an attacker can intrude along path. To sum up, S-BGP and soBGP protocols similarly can provide origin authentication. While S-BGP provides full path authentication, soBGP provides a weaker static service for protecting the authenticity of paths. S-BGP on its own provides point-to-point connection security measures through the use of IPsec. Now, the issue relies on performance and complexity. There is a tradeoff between the level of security required and the performance and complexity issues. However, S-BGP is a much better solution to be further researched and endeavour to provide less extensive cryptographic primitives and a better way to deploy it.

Chapter 7

CONCLUSION AND FUTURE WORK

Interdomain routing has shown quite a lot of interest in the last decade. This is due to its importance to many organisations and the whole Internet community in general. The Internet has become a fundamental resource in academic institutions, government agencies and small to large businesses, as well as a vibrant part of our daily lives. This large network of networks requires the interconnection and collaboration of a significant number of autonomously controlled networks. The good functioning of communication in the Internet relies on routing, which is the component that determines feasible paths (or routes) for data to follow from a source to a destination.

Today and for nearly two decades, the Internet has seen a new born protocol that could cope with its scale of growth. The Border Gateway Protocol relies on the exchange of messages. More precisely, the routing information provided in tables relies on UPDATE messages exchanged between bordering routers in Autonomous Systems. The way BGP-4 was designed excluded it from all security aspects. This led to an insecure interdomain routing protocol deployed in the entire Internet.

BGP has shown many weaknesses and vulnerabilities to malicious behaviour. Since BGP requires the use of a TCP session, it inherited all the issues that the Transport Control Protocol has. It became vulnerable to even a larger number of different attacks. BGP can be subject to eavesdropping, replay, message insertion, message deletion, message modification, man-in-the-middle, and denial of service attacks. If the routing infrastructure is attacked and apprehended, it can be used to attack other systems on the Internet such as DNS.

Many countermeasures were built to secure BGP. However, they are not part of the protocol and some of them employ weak security mechanisms. In order to provide a comprehensive solution for interdomain routing, the security requirements of a well functioning BGP need to be defined. The major three issues that need to be emphasised on are hop integrity (peering session protection), origin authentication of ASes and speakers, and route validation.

Many solutions for securing interdomain routing have been proposed. However, majorly only a few have been discussed over the last five years. We covered two of them: S-BGP and soBGP. Both of these protocols have a similar aim which is to protect BGP-4. However, through their design, they seek to secure different parts of the protocol through the use of the same cryptographic primitives. On one hand, S-BGP uses two PKIs and attestations to provide origin authentication and path authenticity. Moreover, it uses IPsec to provide the BGP peering session with integrity, data origin authentication and confidentiality if required. Furthermore, it transports its data through a new attribute. On the hand, soBGP uses a different key distribution mechanism: the web of trust. It is majorly reliant on certificates. However, it does not require messages to be signed at every transmission. It carries the security data through a new message.

S-BGP and soBGP have advantages and disadvantages. Some can be tolerated but others represent the essence of securing interdomain routing. S-BGP provides a comprehensive solution. It overcomes the three security problems we initially set. Although, it has a few residual vulnerabilities, it presents a way of overcoming those issues. However, it fails at providing a mechanism that secures route withdrawal or obliges speakers to advertise. Moreover, it requires a lot of collaboration in the Internet community to be deployed. Furthermore, it is computationally expensive, and memory and storage dependent. Thus, it requires updates and upgrades for every router that uses the protocol. However, soBGP is more lightweight. It requires fewer resources since it does not rely on extensive cryptographic processing. Moreover, it succeeds at authenticating ASes. However, it provides less security services. For instance, it does not provide hop integrity and does no authenticate paths as required by the protocol. However, it only offers the plausibility of routes. This is for example not tolerable since route paths represents the essence of routing. The primary goal of securing BGP is to have healthy routing tables. If this is not met accordingly, it makes the protocol very weak. Regardless of its performance and numerous options for deployment, it does not provide fully the most important security service. However, in the security world, there is always a tradeoff between level of security, and performance and cost. Since S-BGP provides the most comprehensive solution, it requires a lot of effort and a high cost to deploy it; while the feasibility of the latter is still highly questionable.

Since S-BGP offers the best solution so far provided for interdomain routing, future research should emphasise on it. Trying to find a way to deploy it is a major issue. Moreover, PKIs in S-BGP become quite hairy because of the large scale of the Internet. If a solution to the deployment of PKI can be found, a large portion of the problem is solved. Moreover, cryptographic functions are generally expensive. Future BGP security research should try to make use of new cryptographic constructions for performance and efficiency matters. However, a lot of issues in soBGP need to be reviewed and perhaps redesigned. soBGP can see the light again but it needs to provide stronger security.

Interdomain routing security has progressed along the years. However, the next move is still on hold. A lot of research is conducted but fewer solutions have been delivered. Some operators use a few security mechanisms to obtain some protection. However, comprehensive solutions are still waiting to be deployed. This is because of the complexity of such large scale protocol. Securing BGP is very complicated due to the density of the Internet. Solutions exist. Some of them are temporary such as pretty secure BGP (psBGP)

[68]. This protocol can be deployed and used since it is operational, until further improvements are made to current solutions. This dissertation has shown the importance of securing BGP and compared two solutions (S-BGP and soBGP). BGP is a protocol that will be relied on for other many years. If it keeps this state of insecurity, we might be seeing disastrous attacks on the routing infrastructure. Finally, BGP needs to be secured and a good methodology to securing it must be taken in consideration. The example of such good methodology is S-BGP but unfortunately, so far it is too expensive to be operational and deployed.

REFERENCES

[1] R. Mahajan, D. Wetherall, and T. Anderson. ”Understanding BGP Misconfiguration”. In Proc. ACM SIGCOMM, pages 3.17, Pittsburgh, PA, Aug. 2002.

[2] S. Murphy, A. Barbir, and Y. Yang. “Generic Threats to Routing Protocols”. Internet Engineering Task Force, Oct. 2004. http://www.ietf.org/internet-drafts/draft-ietf-rpsec-routing-threats-07.txt, expired April 2005.

[3] N. Feamster, J. Borkenhagen, and J. Rexford. “Guidelines for Interdomain Traffic Engineering”. *ACM Computer Communications Review*, 33(5):19.30, Oct. 2003.

[4] Y. Rekhter et. al. “A Border Gateway Protocol 4 (BGP-4)”, Network working Group, Internet Engineering Task Force, January 2006, RFC 4271

[5] “INTERNET PROTOCOL”, Information Science Institute, University of Southern California, September 1981, RFC 791

[6] A. Feldmann and J. Rexford. “IP Network Configuration for Intradomain Traffic Engineering”. *IEEE Network*, 15(5):46.57, Sept. 2001.

[7] A. Chakrabarti, G. Manimaran. “Secure Link State Routing Protocol”, Technical Report, Dept. ECpE, Iowa State University, 2002.

[8] E. Jones et. al. “OSPF Security Vulnerabilities Analysis”, Routing Protocol Security Requirements, Technical Report, draft-ietf-rpsec-ospf-vuln-02.txt, June 2006.

[9] K. Egevang et. al.“The IP Network Address Translator (NAT)”. Internet Engineering Task Force, May 1994, RFC 1631.

[10] Y. Rekhter et. al. “An Architecture for IP Address Allocation with CIDR”, Internet Engineering Task Force, Septembre 1993, RFC 1518.

[11] V. Fuller et. al. “Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy”, Internet Engineering Task Force, Septembre 1993, RFC 1519.

[12] J. Hawkinson et. al. “Guidelines for creation, selection, and registration of an Autonomous System (AS)”, Internet Engineering Task Force, March 1996, RFC 1930.

[13] K. Lougheed et. al. “A Border Gateway Protocol (BGP)”. Internet Engineering Task Force, June 1989, RFC 1105.

[14] Y. Rekhter et. al. “A Border Gateway Protocol 4 (BGP-4)”. Internet Engineering Task Force, March 1995, RFC 1771.

[15] Y. Rekhter et. al. “Application of the Border Gateway Protocol in the Internet”. Internet Engineering Task Force, March 1995, RFC 1772.

[16] P. Traina. “Experience with the BGP-4 protocol”. Internet Engineering Task Force, March 1995, RFC 1773.

[17] P. Traina. “BGP-4 Protocol Analysis”. Internet Engineering Task Force, March 1995, RFC 1774.

[18] Y. Rekhter et. al. “A Border Gateway Protocol 4 (BGP-4)”. Internet Engineering Task Force, January 2006, RFC 4271.

[19] D. Estrin et. al. “A Unified Approach to Inter-Domain Routing”, Internet Engineering Task Force, May 1992, RFC 1322.

[20] Charles M. Kozierok. “TCP/IP Guide: A Comprehensive, Illustrative Internet Protocol Reference”, No Starch Press, Inc., San Francisco, 2005.

[21] Information Sciences Institute. “Transmission Control Protocol”, Internet Engineering Task Force, University of Southern California, California, September 1981, RFC 793.

[22] T. Bates et. al. “BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)”, Internet Engineering Task Force, April 2006, RFC 4456.

[23] P. Traina et al. “Autonomous System Confederations for BGP”, Internet Engineering Task Force, August 2007, RFC 5065.

[24] C. Villamizar et. al. “BGP Route Flap Damping”, Internet Engineering Task Force, November 1998, RFC 2439.

[25] Alfred J. Menezes, P. Van Oorschot, and S. Vanstone. “Handbook of Applied Cryptography”, CRC Press, 1996.

[26]R. Rivest. “The MD5 Message-Digest Algorithm”, Internet Engineering Task Force, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992, RFC 1321.

[27] A. Heffernan. “Protection of BGP Sessions via the TCP MD5 Signature Option”, Internet Engineering Task Force, Cisco Systems, August 1998, RFC 2385.

[28] N. Barret. “Penetration testing and social engineering: hacking the weakest link”, Information Security Technical Report, Vol. 8, No. 4, December 2003.

[29] E. Guttman et. al. “Users’ Security Handbook”, Network Working Group, Internet Engineering Task Force, February 1999, RFC 2504.

[30] V. Antoine et. al. “Router Security Configuration Guide”, System and Network Attack Center, National Security Agency, December 2005.

[31] P. Oechslin. “Making a Faster Cryptanalytic Time-Memory Trade-Off”, Laboratoire de Securite et de Cryptographie (LASEC), Ecole Polytechnique Federale de Lausanne, 23rd Annual International Cryptology Conference, CRYPTO ’03, 2003.

[32] V. Klima. “Tunnels in Hash Functions: MD5 Collisions within a Minute”, Charles University, Prague, Czech Republic, April 2006

[33] S. Convery et. al. “An Attack Tree for the Border Gateway Protocol”, Technical Report, Internet Engineering Task Force, November 2002.

[34] Z. M. Mao, J. Rexford, et. al. “Towards an Accurate AS-Level Traceroute”, ACM SIGOMM, Germany, August 2003.

[35] F. Gont. “ICMP Attacks against TCP”, Internet Engineering Task Force, Internet Draft, draft-gont-tcpm-icmp-attacks-03.txt, December 2004.

[36] “NISCC Vulnerability Advisory 236929: Vulnerability Issues in TCP”, NISCC Vulnerability Management Team, April 2004.

[37] S. Murphy. “BGP Security Vulnerabilities Analysis”, Network Working Group, Internet Engineering Task Force, January 2006, RFC 4272.

[38] P. Savola, “Backbone Infrastructure Attacks and Protections”, Technical Report, Internet Engineering Task Force, January 2007.

[39] P. Watson. “Slipping In The Window: TCP Reset Attacks”, CanSecWest 2004, April 2004.

[40] B. R. Greene and P. Smith. “BGPv4 Security Risk Assessment”, ISP Essentials Supplement, Cisco Press Publications, June 11th, 2002.

[41] Tuna Vardar, "SECURITY IN INTERDOMAIN ROUTING", Helsinki University of Technology, T-110.551 Seminar of Internetworking, 2004.

[42] H. Krawczyk et. al. “HMAC: Keyed-Hashing for Message Authentication”, Internet Engineering Task Force, April 1997, RFC 2104.

[43] S. Kent and R. Atkinson. “Security Architecture for the Internet Protocol”, Internet Engineering Task Force, November 1998, RFC 2401.

[44] R. Thayer et. al. “IP Security Document Roadmap”, Internet Engineering Task Force, November 1998, RFC 2411.

[45] D. Maughan et. al. “Internet Security Association and Key Management Protocol (ISAKMP)”, Internet Engineering Task Force, November 1998, RFC 2408.

[46] D. Carrel et. al. “The Internet Key Exchange”, Internet Engineering Task Force, November 1998, RFC 2409.

[47] G. Armitage et. al. “A Framework for IP Based Virtual Private Networks”, Internet Engineering Task Force, February 2000, RFC 2764.

[48] V. Gill et. al. “The Generalized TTL Security Mechanism (GTSM)”, Internet Engineering Task Force, February 2004, RFC 3682.

[49] K. Butler et. al. “A Survey of BGP Security Issues and Solutions”, AT&T Labs Research, January 2008.

[50] S. Kent, et. al. “Secure Border Gateway Protocol (Secure-BGP)”, IEEE Communications Vol. 18, No. 4, pp. 582-592, April 2000.

[51] M. G. Gouda et. al. “Hop Integrity in Computer Networks”, Proceedings of the IEEE International Conference on Network Protocols, 2000.

[52] S. Chokhani et. al. “Internet x.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, Network Working Group, Internet Engineering Task Force, March 1999, RFC 2527.

[53] K. Seo et. al. “Public-key Infrastructure for the Secure Border Gateway Protocol (S-BGP)”, Anaheim, CA, USA: IEEE DARPA Information Survivability Conference and Exposition II, June 2001.

[54] R. Housley et. al. “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, Network Working Group, Internet Engineering Task Force, April 2002, RFC 3280.

[55] C. Lynn, S. Kent and K. Seo. “X.509 Extensions for IP Addresses and AS Identifiers”, Network Working Group, Internet Engineering Task Force, June 2004, RFC 3779.

[56] M. Zhao and S. W. Smith. “Evaluating the Performance Impact of PKI on BGP Security”, Dartmouth College and University of Illinois, February 2005.

[57] R. White. “Securing BGP Through Secure Origin BGP”, The Internet Protocol Journal – Vol. 6, No 3, Cisco Systems, September 2003.

[58] J. Ng. “Extensions to BGP Transport soBGP Certificates”, Interdomain Routing Working Group, Cisco Systems, draft-ng-sobgp-bgpextensions-01, May 2005.

[59] R. White. “Architecture and Deployment Considerations for Secure Origin BGP (soBGP)”, Network Working Group, Cisco Systems, draft-white-sobgp-architecture-01, May 2005.

[60] B. Weis. “Secure Origin BGP (soBGP) Certificates”, Internet Engineering Task Force, Cisco Systems, draft-weis-sobgp-certificates-02.txt, July 2004.

[61] L. Gao et. al. “Stable Internet routing without global coordination”, IEEE/ACM Transactions on Networking, p. 681-692, December 2001.

[62] N. Feamster et. al. “Network-Wide BGP Route Prediction for Traffic Engineering”, In Proc. SPIE ITCom, vol. 4868, p. 55-68, Boston, MA, August 2002.

[63] CNET News. “Router Glitch Cuts Net Access”, URL: http://news.com.com/2100-1033-279235.html, April 1997.

[64] USA TODAY. “WorldCom suffers widespread Internet outage”, URL: http://www.usatoday.com/tech/news/2002-10-03-net-outage_x.htm, October 2002.

[65] N. G. Feamster. “Proactive Techniques for Correct and Predictable Internet Routing”, EECE dept, Massachusetts Institute of Technology, February 2006.

[66] S. Kent. “Securing the Border Gateway Protocol: A status update”, Torino, Italy, Seventh IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, October 2003.

[67] S. Kent, et. al. “Secure Border Gateway Protocol (S-BGP) real world performance and deployment issues”. ISOC Symposium on Network and Distributed System Security, February 2000.

[68] T. Wan, E. Kranakis and P.C. van Oorschot. “Pretty Secure BGP (psBGP)”, Carleton University, Ottawa, Canada, September 2004.