Interdomain routing security:
Motivation and challenges of RPKI

Amreesh Dev, Phokeer

Technical Report
RHUL–MA–2014–14
01 September 2014

Information Security Group
Royal Holloway, University of London
Egham, Surrey TW20 0EX,
United Kingdom

www.ma.rhul.ac.uk/tech
Amreesh Dev, Phokeer

Interdomain routing security:
Motivation and challenges of RPKI

Supervisor: Prof. Keith Martin
Abstract

Today we all know that the BGP protocol, considered as the cornerstone of the Internet, is vulnerable to different kinds of attacks and weaknesses. At the time BGP was conceived, security and trust in the interdomain routing were not an issue. This protocol, whose role is to allow routing information to propagate from one network to another, has two main vulnerabilities. It does not have any strong mechanism to prevent a network i.e. an Autonomous System from announcing an arbitrary route. In other words on the Internet today, any network can potentially announce “I am Google, please send all Google traffic to my network”. There is no mechanism to ensure origin validation. The other main issue is path validation. A BGP speaker has no means to validate the information it receives about a route to a certain destination.

After more than two decades of unsuccessful standardisation works, the SIDR (Secure Inter Domain Routing) working group of the IETF has recently released a series of protocols that should enable interdomain routing to become more secure and robust. The solution space is a framework known as the Resource Public Key Infrastructure (RPKI), where the key element is resource certification. RPKI itself will not solve all interdomain routing problems, but it does provide the building blocks on which other security solutions are to be built.

As RPKI is slowly being deployed, it is also facing lot of challenges from both a technical and environmental perspective. We have witnessed in the past how previously proposed BGP security solutions failed to receive wide-scale acceptance, especially because of the complexity they would engender and their impact on existing protocol. RPKI has been designed to be as simple as possible with minimum impact on BGP. There are however many questions still unanswered regarding the governance of RPKI and its side effects. This thesis proposes to analyse in details the different challenges from a technical, economical and operational point of view.

To help deepen the analysis, a survey was carried out to get qualitative information on routing security awareness and network operators’ willingness to deploy RPKI.
# Table of Contents

1 **Introduction** .................................................................................................................. 6
  1.1 Background of study ........................................................................................................ 6
  1.2 Problem description .......................................................................................................... 6
  1.3 Motivation and purpose of study .................................................................................... 7
  1.4 Structure ......................................................................................................................... 7
  1.5 Methodology ................................................................................................................... 8

2 **Interdomain Routing** ....................................................................................................... 9
  2.1 Internet ecosystem and address space management ......................................................... 9
  2.2 What is interdomain routing? .......................................................................................... 10
     2.2.1 Interior and Exterior Gateway protocols ...................................................................... 10
     2.2.2 Network types .......................................................................................................... 10
     2.2.3 Network tiers ............................................................................................................ 11
  2.3 **Border Gateway Protocol** ........................................................................................... 12
     2.3.1 How it works ............................................................................................................. 12
     2.3.2 Interdomain routing policy ....................................................................................... 14
     2.3.3 BGP State transitions and messages ........................................................................ 14
     2.3.4 BGP Route attributes and decision process ............................................................. 16
  2.4 Conclusion ....................................................................................................................... 17

3 **BGP Threat model** ........................................................................................................... 19
  3.1 Attacks between peers ..................................................................................................... 19
  3.2 Attack against confidentiality ......................................................................................... 19
  3.3 Attacks against message integrity ................................................................................. 19
  3.4 Fraudulent Origin attacks ............................................................................................... 19
  3.5 Subversion of path information ..................................................................................... 20
  3.6 Denial of service (DoS) attack ....................................................................................... 20
  3.7 Misconfigurations ........................................................................................................... 21
  3.8 Known BGP attacks ....................................................................................................... 21
     3.8.1 Pakistan Telecom and YouTube February 2008 ......................................................... 21
     3.8.2 China Telecom April 2010 ...................................................................................... 22
  3.9 Conclusion ....................................................................................................................... 23

4 **Interdomain Routing Security** ........................................................................................ 24
  4.1 BGP Security requirements and mitigation techniques ................................................ 24
     4.1.1 Security of the data payload ..................................................................................... 24
     4.1.2 Security of the data semantics .................................................................................. 24
  4.2 BGP Security proposals .................................................................................................. 27
     4.2.1 S-BGP ..................................................................................................................... 27
     4.2.2 soBGP .................................................................................................................... 27
  4.3 Deployment considerations ............................................................................................. 28
  4.4 Conclusion ....................................................................................................................... 29

5 **Resource Public Key Infrastructure** ............................................................................. 30
  5.1 Resource Certification through RPKI ............................................................................ 30
     5.1.1 Resource Certification hierarchy .............................................................................. 30
     5.1.2 Resource certificate types ....................................................................................... 31
     5.1.3 Resource certificate profile ..................................................................................... 32
     5.1.4 Algorithm and key size ............................................................................................ 33
     5.1.5 Validation ................................................................................................................ 33
  5.2 Resource Certificate management .................................................................................. 34
     5.2.1 Certificate Issuance and revocation ......................................................................... 34
     5.2.2 CA Key rollover ....................................................................................................... 35
     5.2.3 Up/Down protocol .................................................................................................... 35
  5.3 RPKI-Based Origin Validation ....................................................................................... 36
5.3.1 Route Origin Authorization ......................................................... 36
5.3.2 ROA management ........................................................................ 37
5.3.3 Publication of RPKI objects ........................................................... 38
5.3.4 RPKI in practice ........................................................................... 39
5.3.5 RPKI-RTR protocol ...................................................................... 41
5.3.6 Route Origin Validation using RPKI and ROA ................................. 41
5.4 Path Validation with BGPSEC .......................................................... 43
5.5 Conclusion ..................................................................................... 44

6 Security challenges and operational issues ............................................. 45
6.1 Internet number resources allocations inconsistency .......................... 45
6.2 Legacy space .................................................................................. 46
6.3 RPKI Trust model ........................................................................... 46
   6.3.1 Centralised control ..................................................................... 46
   6.3.2 Deliberate manipulations ............................................................ 47
6.4 Technical challenges ........................................................................ 47
   6.4.1 Global Trust Anchor (GTA) key management ............................... 48
   6.4.2 Repository scalability and performance issues .............................. 48
   6.4.3 Dealing with RPKI risks ............................................................. 49
6.5 Awareness and adoption survey ......................................................... 49
   6.5.1 Purpose .................................................................................... 49
   6.5.2 Results and analysis .................................................................. 50
   6.5.3 Conclusion and observation ......................................................... 54
6.6 Chapter conclusion .......................................................................... 55

7 Conclusion ........................................................................................ 56

8 Bibliography ....................................................................................... 58

Acronyms ............................................................................................. 65

Annex A – RPKI objects ........................................................................ 67
   Resource Certificate .......................................................................... 67
   Trust Anchor Locator (TAL) ............................................................... 68
   Route Origin Authorization (ROA) ..................................................... 68
   Manifest file .................................................................................... 69
   Certificate Revocation List (CRL) ....................................................... 70

Annex B – RPKI Adoption Survey .......................................................... 71
List of figures

Figure 1: Internet Number resource allocation hierarchy ................................................................. 9
Figure 2: Example of an interdomain routing network topology ......................................................... 11
Figure 3: Example of a network with an origin AS ........................................................................... 11
Figure 4: Relationship between the various tiers on Internet providers ............................................. 12
Figure 5: Growth of Advertised AS numbers ...................................................................................... 13
Figure 6: Growth of the interdomain routing table ............................................................................ 13
Figure 7: Timeline of the Pakistan Telecom YouTube hijack in February 2008 ................................... 22
Figure 8: China Telecom traffic interception ....................................................................................... 23
Figure 9: Example of routing information in a routing registry ............................................................ 26
Figure 10: Resource certification hierarchy ......................................................................................... 31
Figure 11: Subject-Child certificate issuance ....................................................................................... 36
Figure 12: Example of a ROA ............................................................................................................. 37
Figure 13: Use of SIA and AIA extensions in the RPKI ...................................................................... 38
Figure 14: Example of a manifest file .................................................................................................. 39
Figure 15: RPKI Architecture and components .................................................................................. 41
Figure 16: Issuing parties and relying parties global view ................................................................. 41
Figure 17: Illustration of a BGP path subversion attack .................................................................... 44
Figure 18: Profile of participants ......................................................................................................... 50
Figure 19: Awareness of interdomain routing vulnerabilities .............................................................. 50
Figure 20: Awareness of countermeasures ......................................................................................... 51
Figure 21: Participation in RPKI ......................................................................................................... 52
Figure 22: Hardware compliance to RPKI .......................................................................................... 52
Figure 23: Intention to deploy RPKI locally ....................................................................................... 52

List of tables

Table 1: BGP Common Header Format ............................................................................................. 15
Table 2: OPEN Message format .......................................................................................................... 15
Table 3: UPDATE message format ...................................................................................................... 16
Table 4: KEEPALIVE message format ................................................................................................. 16
Table 5: NOTIFICATION message format .......................................................................................... 16
Table 6: Steps in the BGP decision process ......................................................................................... 17
Table 7: BGP Security solutions comparative analysis ...................................................................... 28
Table 8: Resource allocation example ................................................................................................ 31
Table 9: Resource certificate profile .................................................................................................... 33
Table 10: BGP announcements and ROA matching and validity ......................................................... 42
Table 11: Announcements and signatures in BGPSEC ....................................................................... 44
Table 12: Most popular routing issues .................................................................................................. 51
Table 13: Drivers for improved routing services .................................................................................. 51
Table 14: Short-term incentives ........................................................................................................... 53
Table 15: Long-term incentives ............................................................................................................ 53
Table 16: Barriers in RPKI adoption .................................................................................................... 54
Table 17: Readiness to invest in RPKI ............................................................................................... 54
1 Introduction

1.1 Background of study

The Resource Public Key Infrastructure (RPKI), also known as, “Resource Certification” is a new technology developed by the Secure Inter-Domain Routing (SIDR) working group of the Internet Engineering Task Force (IETF). It makes use of an extended version of X.509 public key certificates [1,2] to attest that the holder of the private key has a “right-of-use” over the set of Internet number resources (INR), contained in the certificate. RPKI is one element of a larger architecture devised to secure the interdomain routing system. It actually lays down the foundation to certify resource allocations and to validate legitimacy of BGP routing announcements.

Interdomain routing security has been in the limelight for more than a decade now. As the Internet keeps expanding and becomes more and more ubiquitous, concerns have been raised as to what extent the routing system is reliable and secure. Disruptions in the routing system, either by accident or by malice, can have disastrous consequences on the day-to-day life of Internet users. Whether it is for financial transactions, electronic commerce or telemedicine, all internet-related activities rely on a robust routing system to ensure that data packets are delivered to the right destinations.

Over the recent years, we have witnessed many initiatives to secure the interdomain routing system. Many of which were never widely deployed due to an excessive technical overhead they required for implementation. A non-exhaustive list of previous attempts is S-BGP [3], SoBGP [4,5], psBGP [6] and IRR [7]. However, as the Internet keeps expanding, the number of accidents related to interdomain routing is also flaring up. Human errors and router misconfigurations have become very frequent as Mahajan R. et al. described in their paper [8].

A well-known incident is the “Pakistan Telecom - YouTube Hijack” in February 2008, where Pakistan Telecom advertised a prefix, belonging to YouTube, as theirs. Announcement got propagated to their upstream providers, which resulted in the hijack of YouTube traffic [9].

Securing the interdomain routing system requires securing the de facto interdomain routing protocol, the Border Gateway Protocol (BGP) [10]. RPKI actually sets the framework to enable network operators achieving this goal.

1.2 Problem description

The interdomain routing protocol, BGP, currently used as the main protocol to ensure routing across domains (autonomous systems), is known to have several weaknesses. Researchers and network operators all agree that those vulnerabilities can be detrimental to the smooth operation of the Internet and many incidents already happened in the past.

However, deploying out a new security mechanism overnight would be too unrealistic, due to the gigantic “size” of the Internet as it will obviously be very difficult to get all software, network equipment and other Internet applications compatible to a new security protocol.

Moreover, as the name is suggesting, the interdomain routing works with disparate networks called Autonomous Systems (AS). Those ASes function in a totally independent fashion and are tied to other ASes mainly based on business and commercial relationships. Routing policies, i.e. rules that determine how packets are
transmitted from one network to another, are based on those potentially conflicting relationships especially when competition and commercial interest get into the picture [11,12]. This state of affairs actually makes the problem of interdomain routing even more complex.

From a more technical perspective, added to the fact that environmental factors mentioned above already make the deployment of any new security technology very difficult to implement, the mechanisms behind interdomain routing security is not trivial. According to N. Feamster et al., in their study on the foundational problems of interdomain routing, there have been many incremental fixes to correct the different ills of the BGP protocol, but those were done at the cost of increasing complexity. The foundational issues which are “Origin Validation” and “Path Validation” were actually never resolved [13].

Works on RPKI are being finalised at the IETF level and the scientific community seems to have reached consensus on the fact that RPKI would provide the necessary framework to improve routing security. However, global acceptance of this new security interface still remains a challenge. Almost no studies have been carried out so far on the deployability and operability of RPKI and as any new technology, it comes with a capital and operational cost [14].

The work in this thesis is to analyse the different security challenges and operational issues in the management of a PKI for resource certification by taking into consideration economical, technological, organisational, environmental and ethical factors.

1.3 Motivation and purpose of study

As mentioned earlier, RPKI is a novel solution. Not much research have been carried out on this new security framework, even though, previous solutions have greatly influenced the design of RPKI. Regional Internet Registries (RIRs) are one of the first actors to implement RPKI, being responsible for the allocation of Internet number resources in their respective regions. As a lead implementer of RPKI at AFRINIC, the African Regional Internet Registry, I felt that it would be interesting to get more information about how difficult it is to deploy and operate this new technology at a large scale.

1.4 Structure

Chapter 2 explains how interdomain routing works and gives some details on the Border Gateway Protocol (BGP). We shall look into the different BGP messages and the BGP decision process of selecting the best routes. We will also explain how Internet number resources are distributed and managed and how they are linked to interdomain routing.

Chapter 3 is about the BGP threat model. It will describe the different attacks on interdomain routing especially attacks between two BGP speakers, attacks against confidentiality and message integrity, false origin attacks, path subversion, misconfiguration and denial of service. We will also analyse two well-known examples of a prefix hijacking and an interception attack.

Chapter 4 will provide details on the countermeasures and an in-depth analysis of those countermeasures. We shall first go through the requirements of interdomain security before enumerating the different solutions that have been proposed and implemented and why the solution space does not fully solve the main issues of interdomain routing.

Chapter 5 gives an in-depth description of the RPKI protocol. It explains what are the important components and how they are used together to provide origin validation and
path validation. Those are the two concepts constitute the problem space of interdomain routing. We shall also see how certificates are managed and how the products of RPKI are used to provide validation mechanism on routing announcements.

Finally, Chapter 6 talks about the different security challenges and operational issues in deploying and operating RPKI. We shall look into the technical and environmental challenges and see why it is not trivial to deploy RPKI at such a large scale. To help us better understand the challenges from a qualitative perspective, the results of a survey on RPKI awareness and adoption will be presented and analysed.

1.5 Methodology

RPKI has been deployed by the five RIRs and by some other resource holders such as National Internet Registries (NIRs) and large Internet Service Provider (ISPs). As things are moving forward and pilot implementations being deployed, many operational issues are being encountered. Based on several studies and feedback from operators, we will analyse the different security challenges and operational issues. A survey from a selected group of network operators and interdomain routing experts will help us better understand the different challenges from their perspective.
2 Interdomain Routing

2.1 Internet ecosystem and address space management

The Internet ecosystem is composed of different actors with different roles. Combined together, they make the Internet work in the way it is nowadays. From a protocol point of view, there are basically 2 main aspects: numbers and names. Information, on the Internet, is exchanged using the TCP/IP protocol and the Domain Name System (DNS) is used to map domain names to IP addresses.

Communication between different hosts on the Internet is achieved by the use of IP addresses which are categorised in 2 different family versions: IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 is a 32 bit long number and IPv6 is 128 bit long i.e. $2^{32}$ and $2^{128}$ different addresses respectively. However, not all addresses can be used publicly as parts of them are reserved for specific purposes such as multicast, 6to4 Relay Anycast or Private-Use Networks [15].

Internet number resources are managed by the Internet Assigned Numbers Authority (IANA) and by the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN acts as the subcontractor for the US Government to ensure the IANA function. As shown on figure 1, public IP addresses are distributed regionally to Regional Internet Registries (RIR) from the IANA, who in turn redistributes them to Local Internet Registries (LIR), National Internet Registries (NIR) or end-users such as businesses, governments or individuals. There are currently five RIRs: AFRINIC (African and Indian Ocean region), APNIC (Asia Pacific region), ARIN (North American region), LACNIC (Latin America and the Caribbean) and the RIPE NCC (European and Middle East region).

![Figure 1: Internet Number resource allocation hierarchy](image)

To ensure scalability of the Internet, Autonomous Systems (AS) [16] are used to represent a set of IP prefixes (or end hosts) which are under the same administrative control, usually called a *domain*. A domain shares the same routing policies and is identified by an Autonomous System Number (ASN). ASNs are 4-bytes numbers (originally on 2-bytes) managed by the IANA and assigned to the RIRs.
2.2 What is interdomain routing?

The Internet is usually referred to as the network of networks. It is basically a set of interconnected networks that provides end-to-end connectivity between the different nodes. A network consists of end points (i.e. host systems) and intermediate systems usually referred as gateways or routers. A set of end points and intermediate systems running under the same administrative entity is referred to as a domain.

A domain is represented by an Autonomous System and is assigned a unique identifier called an Autonomous System number (ASN). Organisations who want to advertise the routes to their network will need to get an ASN from an RIR. This allows them to enable interdomain communication with their upstream service providers.

2.2.1 Interior and Exterior Gateway protocols

An Autonomous System can also consist of several internal networks, made up of routers, switches and hosts. The way different routers share information about the network topology within the AS is called *intradomain routing*. *Intradomain routing* is the process of transferring packets from one point to another within the same AS and it uses Interior Gateway Protocols (IGPs) to determine routing within the Autonomous System. Some well-known IGPs today are Intermediate System-to-Intermediate System (ISIS), Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) [17].

On the other hand, when we want data to be transferred from separate networks on the Internet, i.e. from one public AS to another, communication is achieved using *interdomain routing*. Interdomain routing uses Exterior Gateway Protocols (EGPs) to determine the best routes between the ASes. An example would be the relationship of an organisation has with its Internet Service Providers (ISPs). The organisation’s internal network would run IGP to route traffic from within the different components of the internal network. The organisation can have multiple sites (networks) logically separated from each other but all under the same AS.

However, if the organisation wants external traffic to reach its network, EGP needs to be used to announce the prefix of the organisation to the external world. In that case, the ISPs would now know where to redirect traffic for the prefix the organisation is the holder of.

2.2.2 Network types

On the Internet, ASes are categorised in three main types. There are “single-homed” ASes, which are connected to only one AS, “multi-homed” ASes which are connected to multiple ASes and finally “transit” ASes commonly referred as the Internet backbone.

Multi-homed ASes provide resiliency as an AS can announce its prefix on two (or more) different networks. Routers that communicate using eBGP are called border routers, commonly referred to as network gateways. The Border Gateway Protocol is about how those border routers communicate with each other. A router configured to communicate using BGP is called a BGP *speaker*.

Figure 2 depicts a typical interdomain routing network topology with a single-homed AS (AS 5) and multi-homed ASes (AS 1, AS 2, AS 3, AS 4, AS 6). A multi-homed AS can allow traffic to pass through them and acts as a transit AS, but AS 5 for example, will not allow transit traffic. Those ASes are called *stub*.
Figure 2: Example of an interdomain routing network topology

Single-homed ASes are connected to only one upstream provider, i.e. traffic between AS 4 and AS 5 will be considered as local traffic. In this case, AS 5 can be assigned a private AS (64512 to 65535). Private ASes usually do not appear in AS paths in the routing table, which allow them to be reused on different networks.

The role of an AS is to originate one or more prefixes. Those ASes, also known as Origin AS, ensure that the prefixes are propagated on the Internet by advertising them to its peers or neighbours. The prefix represents a network and is expressed as a block of IP addresses with a net mask in CIDR notation [18]. For example, 134.219.0.0/16 is the network of the Royal Holloway and Bedford New College and is originated by AS 786 and seen by 186 different other ASes.

This information comes from the WHOIS database of the RIPE NCC, the RIR for the European and Middle East region.

<table>
<thead>
<tr>
<th>Prefix:</th>
<th>134.219.0.0/16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix description:</td>
<td>UNITED KINGDOM</td>
</tr>
<tr>
<td>Country code:</td>
<td>GB</td>
</tr>
<tr>
<td>Origin AS:</td>
<td>786</td>
</tr>
<tr>
<td>Origin AS Name:</td>
<td>JANET The JNT Association</td>
</tr>
<tr>
<td>RPKI status:</td>
<td>No ROA found</td>
</tr>
<tr>
<td>First seen:</td>
<td>2011-10-19</td>
</tr>
<tr>
<td>Last seen:</td>
<td>2013-06-30</td>
</tr>
<tr>
<td>Seen by #peers:</td>
<td>186</td>
</tr>
</tbody>
</table>

Figure 3: Example of a network with an origin AS

2.2.3 Network tiers

On the Internet, data packets are routed on different networks before reaching their final destinations. The networks, or more precisely the relationships between the networks, are
organised in different tiers to facilitate interdomain routing but also to provide several layers of indirection. There are today three “layers” of networks namely Tier 1, Tier 2 and Tier 3. Those are imaginary boundaries that group specific networks into a category depending on their role and the type of relationship they have with other networks.

The Tier 1 networks, usually referred as the Internet backbone, consist of a few Autonomous Systems (ASes) that are linked to each other and provide “free” peering services. This means that a network A would allow free transit for a network B and vice-versa. Thanks to the peering agreements, a packet on a Tier 1 network can actually reach any other part of the Internet with the need to buy transit. Tier 1 networks are therefore dependent on each other as together they form a mesh that would allow traffic to flow in any possible direction. Disruptions at the Tier 1 level would mean that part of the Internet could become unreachable.

Tier 2 networks are those who have peering agreements with other Tier 2 networks but normally have to buy transit from Tier 1 networks and they are usually operated by very large ISPs or telecommunication companies. Tier 2 networks in the same country or region usually enter into “peering” agreements and interconnect through Internet Exchange Points (IXPs) to share traffic with each other. Peering allows them to reduce the interconnection costs with Tier 1 providers, if traffic needs to stay local or regional.

Smaller ISPs are located at lower level known as Tier 3. Those networks have to buy transit from Tier 2 providers in order to operate. Tier 3 networks can either be single-homed or multi-homed and are usually those that provide Internet connection to end-users. The figure below shows how the different networks are layered and interconnected (Source Wikipedia [19]).

![Figure 4: Relationship between the various tiers on Internet providers](image)

### 2.3 Border Gateway Protocol

#### 2.3.1 How it works

The current version of the Border Gateway Protocol, BGP version 4, is described in RFC 4271 [10], which obsoletes RFC 1771, the base document of the protocol. BGP has been used for many years and is considered to be the only viable interdomain routing protocol adapted for large-scale communication over the Internet. The main role of this protocol is to update routing tables a.k.a. the Routing Information Base (RIB), which are found on routers.
A routing table holds data to describe all possible routes around a network and this information is vital to allow packets to be forwarded from one network to another. The routing information is used together with the local preferences of the network to determine the best possible routes to specific destinations. Information about the best paths, also called, reachability data, is stored in the forwarding table of the router. We should think about the routing table being a map of all possible destinations and the forwarding table as a set of itineraries between a point A and a point B.

On the global Internet, the number of advertised Autonomous Systems has grown significantly over the years with more than 40000 ASes as shown in figure 4 [20] along with more than 450000 active BGP entries in the Forwarding Information Base (FIB) entries in the global routing table [21]. See figure 5.
BGP speakers exchange routing information with the means of UPDATE messages. They send and receive information they hold in their routing table to their peers. This information is called the Network Layer Reachability Information (NLRI) and basically consists of a set of prefixes and AS paths. The exchange of information between routers is called the flooding process.

During active BGP sessions, ASes receive UPDATE messages from their peers and update their local Routing Information Base (RIB) with new routes and the old routes are removed. As the prefixes are advertised, the ASes establish the AS path of each prefix. This is the route that a packet will follow to reach its destination after that routing information has converged i.e. routing information has finished propagating. BGP is a path vector protocol based on the distance vector principle [22]. It will always consider the AS path with the shorter number of hops (AS Path length) as the "best path". Information about the different AS paths’ lengths is also stored in the routing table.

2.3.2 Interdomain routing policy

The distance metric used to calculate the “best path”, i.e. the number of intermediate ASes before reaching a destination, is not the only criterion that comes into play. Interdomain routing is based a complex set of physical, organisational, business or political relationships.

For example, an organisation advertising its network to two upstream providers might not have the same bandwidth on both connections. It can set the preference to the higher bandwidth connection and use the lower bandwidth service as backup. Such agreements are usually settled in contractual bindings in the form of SLAs (Service Level Agreement). Similarly, ASes can decide to enter into peering agreements and allow traffic to flow from one customer network to another, on a pro-bono basis, through an Internet Exchange Point (IXP) [23].

The flexibility of the BGP protocol easily enables the enforcement of different sets of policies and routing strategies. They are normally achieved by the application of ingress and egress filtering techniques to restrict traffic leaving and entering the network [24]. Barry R. Greene and Paul Smith (2002) also argued that ingress/egress filters help protect an ISP’s resources and its customers’ network - as it reduces the risk of the network being hijacked to launch attacks on other networks. They mentioned that by protecting their own network through filters, ISPs are working towards protecting the whole Internet.

2.3.3 BGP State transitions and messages

BGP speakers need to exchange messages between themselves to share routing information. In a BGP session, two speaking routers will exchange their full routing tables and will continue doing so incrementally as they are updated. RFC 4271 has defined 4 message types [10]:

- **OPEN**: to start a BGP session
- **KEEPALIVE**: to confirm the liveliness of the BGP peer
- **UPDATE**: to exchange reachability information
- **NOTIFICATION**: to notify the peer before closing a BGP session along with a reason code.

BGP sessions are established over TCP [25] connections to enable the exchange of reachability information between routers. BGP therefore relies on an operational IP functionality at the link level. The first message sent when a TCP connection is
established with a peer, is the OPEN message. The peer will respond back with a KEEPALIVE to acknowledge receipt of the OPEN message. Once this session is established, the peers can now exchange KEEPALIVE, UPDATE and NOTIFICATION messages [26]. RFC 2918 on “Route Refresh Capability for BGP-4” added a new message type called ROUTE-REFRESH. The aim of the ROUTE-REFRESH message is to allow dynamic exchange of routing information and subsequent re-advertisement of BGP outgoing update information [27].

All BGP messages have a common header as prefix as described in table 1 below. It shows the Common BGP header fields and field size.

<table>
<thead>
<tr>
<th>Field</th>
<th>Length (Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marker</td>
<td>16</td>
</tr>
<tr>
<td>Length</td>
<td>2</td>
</tr>
<tr>
<td>Type</td>
<td>1</td>
</tr>
<tr>
<td>Message</td>
<td>19 to 4096</td>
</tr>
</tbody>
</table>

Table 1: BGP Common Header Format

BGP sessions are initiated using the OPEN message that holds the Autonomous System number and the IP address of the router from which the message is coming from. The role of the OPEN message is to allow BGP peers to identify themselves and contains optional parameters to extended authentication capabilities. Table 2 describes the format of the OPEN message:

<table>
<thead>
<tr>
<th>Field</th>
<th>Length (Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Version</td>
<td>1</td>
</tr>
<tr>
<td>Autonomous System Number</td>
<td>2</td>
</tr>
<tr>
<td>Hold time</td>
<td>2</td>
</tr>
<tr>
<td>BGP Identifier (IP address)</td>
<td>4</td>
</tr>
<tr>
<td>Optional parameter length</td>
<td>1</td>
</tr>
<tr>
<td>Optional parameters</td>
<td>0 to 255</td>
</tr>
</tbody>
</table>

Table 2: OPEN Message format

Once the BGP session is established, routers can now start exchanging the routing table data via UPDATE messages. The UPDATE message will indicate the prefixes (routes) that cannot be reached (“Withdrawn routes” field) and another set of prefixes that need to be advertised (NLRI field). Withdrawals occur when a router cannot reach those prefixes (destinations) anymore. The path attributes are additional information that would help in the route selection process. The different attributes are explained in the next sub-section. Table 3 shows the format of an UPDATE message.

<table>
<thead>
<tr>
<th>Field</th>
<th>Length (Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Withdrawn routes length</td>
<td>2</td>
</tr>
<tr>
<td>Withdrawn routes</td>
<td>Variable</td>
</tr>
<tr>
<td>Path attributes length</td>
<td>2</td>
</tr>
<tr>
<td>Path attributes &lt;type, length, value&gt;</td>
<td>Variable</td>
</tr>
</tbody>
</table>

Table 3: UPDATE Message format
In order to check the liveliness of the communicating peers, **KEEPALIVE** messages are sent between the two parties at regular interval and so, before that **Hold Time** expires as defined in the **OPEN** message.

<table>
<thead>
<tr>
<th>Field</th>
<th>Length (Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marker</td>
<td>16</td>
</tr>
<tr>
<td>Length</td>
<td>2</td>
</tr>
<tr>
<td>Type</td>
<td>1</td>
</tr>
</tbody>
</table>

**Table 4: KEEPALIVE message format**

Finally, in case an error occurs in a BGP session between two peers, a **NOTIFICATION** message is sent to the other BGP speaker. Before terminating the TCP connection, the **NOTIFICATION** message is used to put the session in an “error mode”. Table 5 shows the different fields of a **NOTIFICATION** message:

<table>
<thead>
<tr>
<th>Field</th>
<th>Length (Octets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error code</td>
<td>1</td>
</tr>
<tr>
<td>ErrorSubcode</td>
<td>1</td>
</tr>
<tr>
<td>Length</td>
<td>2</td>
</tr>
<tr>
<td>Data</td>
<td>Variable</td>
</tr>
</tbody>
</table>

**Table 5: NOTIFICATION message format**

### 2.3.4 BGP Route attributes and decision process

BGP is a path vector protocol, which means that the number of hops between the source and the destination networks counts. The different hops constitute the **AS Path** and the number of hops is the **AS Path length**. However, as we have seen earlier, the shortest path is not always the best possible route. To achieve greater flexibility, BGP makes use of **path attributes**, which are also stored in the routing information base (RIB) of a router. The important route attributes are [26]:

- **LOCAL_PREF**: The local preference attribute is used within an AS to influence the route selection process by overriding the notion of shortest path. It is similar to the concept of “weight” where the higher the number, the higher will be the preference. For example, this attribute becomes handy when network administrators want to bypass shortest routes and take longer but cheaper alternatives.

- **AS_PATH**: As a route propagates over the Internet, each BGP speaker will add its own AS number to the path, before passing the information over to neighbouring speakers through **UPDATE** messages. The **AS_PATH** attribute contained in the **UPDATE** message is very important to avoid the creation of route loops. BGP has been devised to reject an **AS_PATH** containing a router’s own AS number. The set of different AS paths at the router level constitutes the routing table.
• **NEXT_HOP**: This attribute holds the IP address of the immediate neighbouring BGP speaker. NEXT_HOP is transmitted in an UPDATE message and would contain the IP of the outbound router. In the event where UPDATE messages are sent to routers within the same AS, the NEXT_HOP should remain unchanged.

• **ORIGIN**: When a BGP speaker is propagating routing information to its peers, it includes the originating AS number (itself) in the UPDATE message.

• **MED**: The *multi-exit discriminator* attribute’s role is to set a preference level as to which entry point of a network should be privileged. For example, an organisation may advertise several routes to the same prefix but, by setting a MED value to the announcements, a priority level is set.

In the absence of policy, routers will choose the distance metric (AS Path length) as preferred selection criteria. The path attributes give additional flexibility to fine-tune the selection process especially when dealing with tiebreaks. Table 6 below lists the different path attributes and the order in which they are used to determine the best possible route [22]:

<table>
<thead>
<tr>
<th>Step</th>
<th>Attribute</th>
<th>Controlled by local or neighbour AS?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Highest LocalPref</td>
<td>Local</td>
</tr>
<tr>
<td>2</td>
<td>Lowest AS Path Length</td>
<td>Neighbour</td>
</tr>
<tr>
<td>3</td>
<td>Lowest origin type</td>
<td>Neither</td>
</tr>
<tr>
<td>4</td>
<td>Lowest MED</td>
<td>Neighbour</td>
</tr>
<tr>
<td>5</td>
<td>eBGP-learned v/s iBGP-learned</td>
<td>Neither</td>
</tr>
<tr>
<td>6</td>
<td>Lowest iBGP cost to border router</td>
<td>Local</td>
</tr>
<tr>
<td>7</td>
<td>Lowest router ID (to tie break)</td>
<td>Neither</td>
</tr>
</tbody>
</table>

**Table 6: Steps in the BGP decision process**

Basically, if a BGP speaker receives two different announcements for the same prefix from two different neighbours, the router will first look for the highest LOCAL_PREF value of the corresponding ASes. If the LOCAL_PREF value does not allow selection, it will then choose the shortest AS Path length of the two received routes. If it still cannot tiebreak, it will check for the lowest origin type of the announcement and verify whether it comes from an internal source (same AS) or from an exterior (different AS). Next step in the route selection process would be to determine the preference based on the lowest MED as advertised by the neighbour. Routes received from eBGP sources will be privileged over iBGP-received routes.

However, if the router has received multiple iBGP-learned prefixes, the one having the closest NEXT_HOP address would win. Finally, if all the previous attributes are insufficient in the decision-making process, the lowest router ID is used as last resort.

### 2.4 Conclusion

This chapter provided us with an insight of how interdomain routing works and the important constituent messages of the BGP protocol. We have seen that the selection process of the “best path” is not always straightforward and depends on several
parameters. BGP has proved to be a very scalable protocol and is today behind the success of the Internet.

The flexibility, provided by the different BGP messages, made this protocol highly customizable and has therefore enable operators to easily implement the local network preferences, business relationships and other agreements into the route selection process. However, as we shall see in the next chapter, BGP has been designed with next to zero security and it has inherited from the different flaws of underlying protocols such as TCP/IP.
3 BGP Threat model

The Internet was conceived at a time where everything was based on mutual trust and good faith. Similarly, the underlying protocols supporting internetworking were based on the same trust model. But as the state of the Internet has evolved, the game has changed tremendously and now security is a major concern. BGP as we have seen, is devoid of any security mechanism and also relies on another protocol (TCP/IP) which is itself vulnerable to TCP/IP attacks such as IP spoofing, session stealing, TCP SYN attack and so on [28].

So far the most commonly used mitigation techniques are the protection of the TCP session by using TCPMD5 [29,30] and defensive BGP announcements filtering. Kevin Butler et al. (2005) in their paper “A Survey of BGP Security” classified the different BGP security threats as follows:

3.1 Attacks between peers

Two communicating routers will share a BGP session and communicate using TCP/IP. There is no mechanism that enables router A to authenticate to router B and vice-versa. Router A could be a malicious BGP speaker and so could be router B. On top of that, the communication channel is not protected and can be eavesdropped by a third party. Usually, this kind of attack is achieved when a router gets compromised and the BGP session is hijacked [26].

3.2 Attack against confidentiality

Messages exchanged between BGP speakers are not protected by default. Those messages can be intercepted and analysed unless protected by mechanism such as IPSEC [31]. But those mechanisms are optional and are not used by default in interdomain routing information exchange. IPSEC is a point-to-point technology and can only work if both BGP speakers agree to exchange their keys. This solution is difficult to scale when we need to apply IPSEC to thousands of routers. An example of where confidentiality is an issue is regarding peering agreements between network operators. An eavesdropper can analyse BGP traffic and try to guess the interconnection agreements the router and potentially unveil commercial secrets [32].

3.3 Attacks against message integrity

BGP sessions can be victim of man-in-the-middle attacks. The messages are sent as “clear-text” which means that they can easily be intercepted and modified. The attacker can add, delete or change a message therefore tampering with message integrity. Selectively removing messages will cause the BGP session to fail, therefore creating a Denial of Service (DoS) attack. It is even more dangerous when messages are changed to do traffic engineering. UPDATE messages can be tampered with and path attributes such as the NLRI can be modified. This would result in a falsification attack [30].

3.4 Fraudulent Origin attacks

The BGP protocol does not have any mechanism to prevent a BGP speaker to announce a route for which the latter is not the Origin AS. This is called prefix hijacking. Wrong origin information is passed in UPDATE messages sometimes unintentionally
(misconfiguration) or intentionally to cause harm. The neighbours receiving the announcements from their peers have little manoeuvre to verify the authenticity of the information being announced to them. Remember, in most cases, routing works “by rumour”, meaning that information received are most of the time trusted as authoritative.

In exceptional cases, an AS may decide to apply ingress filters on specific AS or prefixes, but this can only be done once the fraudulent origin ASes have been detected. The consequence of accepting fake routes can be a denial of service as traffic will be redirected to a malicious AS which will simply drop the packets (black-holing) or more seriously redirect to the traffic to a network where the datagrams can be analysed.

Another equally severe problem with BGP is prefix de-aggregation [33]. In the route selection process, a router will always select a route with a more specific address space. For example, if a router is receiving 196.0.0.0/16 from a peer and 196.0.0.0/8 from another peer, the route with the smaller address space will be preferred. This is because BGP follows the principle of “longest prefix match”.

Similarly, a malicious AS can advertise a smaller prefix to attract traffic towards its network; this is another form of prefix hijacking. When prefix de-aggregation is done abusively, it can negatively impact the performance of the Internet. The more de-aggregated the prefixes are, the bigger will be the routing tables and therefore routers would require more resources to manage the RIBs. There is also the risk of having redundant information scattered all around the Internet and this would ultimately result in an inconsistent state of the global interdomain routing table.

TeamCymru provide some statistics about the number of prefixes with fraudulent/inconsistent Origin ASNs, which amounts to 2436 representing 0.5% of the total advertised number of prefixes [34].

### 3.5 Subversion of path information

As routes get propagated throughout the different networks, their respective AS Path are updated by the AS they are traversing. This path is the “itinerary” a packet would take to reach a network or a final host. This means that this information is of upmost importance and is crucial to the proper operation of the Internet.

However, as we have seen, a BGP speaker does not know how to check the integrity of the AS Path attribute it receives with the UPDATE messages. An attacker sitting at a compromised AS, can change or inject data in the path attribute and this can result into legitimate traffic being redirected into some unwanted/illicit routes and eventually creating a Denial of Service attack.

### 3.6 Denial of service (DoS) attack

There are different ways in which an attacker can perpetrate a DoS attack. Creating a blackhole or a tunnel is an example. This works by redirecting traffic to a prefix that does not exist therefore creating a drop in reachability. We will see an example later in the YouTube/Pakistan Telecom case. DoS attack can also come from TCP attacks such as SYN flood attacks or TCP resets using ICMP [26].

Another type of DoS is through route flapping. By bringing down a router (for example by overloading the memory), connections to the router can become intermittent and unstable. The routes will therefore be withdrawn from the RIB of the router if the latter is found unreachable. The BGP protocol caters for this type of behaviour through a process called route flap damping and will reject announcements from those “flappy”
routers. The idea is to reduce the amount of change in the global routing state to limit processing requirements [35].

S. Murphy (2006) enumerated the different vulnerabilities that could arise in BGP messages (OPEN, KEEPALIVE, NOTIFICATION and UPDATE) [28].

3.7 Misconfigurations

Misconfigurations or “fat-finger” errors have always been an issue and is the first cause of Internet outages today. Although unintentional, misconfigurations can have same dire effects on the Internet ecosystem as real malicious attacks. Mahajan R. et al. (2002) in their paper “Understanding BGP misconfigurations” identified two forms of misconfiguration that are globally visible [8]:

1. An AS can accidentally inject a prefix it should not (origin misconfiguration) or it can also be an injection of a more specific prefix (prefix de-aggregation).
2. Export misconfiguration: a router is exporting a prefix it should normally have filtered out for example 127.0.0.0/16, which is not a routable address space.

For example, based on data provided by TeamCymru there are currently 290 bogan found in the global routing table, which accounts for 0.05% of the total number of prefixes advertised [34]. A bogan is basically a prefix that is not supposed to be routed either: because it is a reserved space by IANA or simply because it has not yet been allocated and is still in the free pool of an RIR (Regional Internet Registry).

3.8 Known BGP attacks

3.8.1 Pakistan Telecom and YouTube February 2008

On February 24th 2008, the website YouTube (www.youtube.com) was unreachable for almost two hours. BBC reported that in an attempt to ban YouTube in Pakistan, Pakistan Telecom (AS17557) “hijacked” the address space of YouTube and propagated it to the wider Internet through a Hong-Kong based provider PCCW (AS3491) [36].

The technique, called “sub-prefix hijacking”, has been used previously in the famous AS7007 attack [37,38]. As mentioned before, route selection is based on the principle of “longest prefix match” [39], meaning that BGP will always prefer a route where the more specific prefix is advertised. Such incident could have been prevented if a BGP speaker had the ability to validate an announcement received by a neighbour.

YouTube’s network (208.65.152.0/22) is normally advertised by AS36561, but on Sunday, 24 February 2008, AS17557 (Pakistan Telecom) deliberately decided to redirect all traffic going to YouTube to a “black hole”. To achieve this “hijack”, at 18:47 (UTC), AS17557 started to announce a subnet of YouTube’s network (208.65.153.0/24). All traffic to YouTube, within Pakistan Telecom’s internal network was effectively nulled - but they did one mistake: they forgot to add an egress filtering on their announcement and the hijacked route got propagated to their upstream provider AS3491 (PCCW Global).

AS3491 was not doing any ingress filtering either to check whether the route announced by AS17557 was correct. Therefore, BGP speakers around the world got notified about the “hijacked” route with the result that all YouTube traffic got redirected to Pakistan Telecom. At 20:07 (UTC), YouTube decided to advertise the same subnet, as a countermeasure, to attract traffic back to its network. It worked and some part of the world could reach YouTube’s network properly at AS36561.
However, end-users who were closer to Pakistan Telecom were still being denied access. To correct the situation, at 20:18 (UTC), YouTube decided to advertise more specific prefixes i.e. 208.65.153.128/25 and 208.65.153.0/25 to attract all traffic to its network. The result was seen at 20:51 (UTC). Routers around the world were prepending AS17557 to the AS PATH announced by PCCW (3491 17557 17557), making the path longer and therefore a less preferred route.

Finally at 21:01 (UTC), AS3491 (PCCW Global) filtered out the hijacked prefixes announced by AS17557 (Pakistan Telecom), henceforth restoring the situation back to normal.

Below is the event timeline as reported by the RIPE NCC’s Routing Information Service (RIS) [40]:

![Timeline of the Pakistan Telecom YouTube hijack in February 2008](image)

**Figure 7: Timeline of the Pakistan Telecom YouTube hijack in February 2008**

### 3.8.2 China Telecom April 2010

On April 8, 2010 network operators in the US and China started to witness an unusual behaviour on the interdomain routing coming from China. BGPmon.net, a service that *inter alia* monitors suspicious activities in the global routing table, generated an alert about what could be a potential prefix hijacking attack from China [41]. The event attracted much attention due to high political and security profile of the incident. As a matter of fact, Internet traffic to government agencies in the US namely the Department of Defense, the Department of Transport and the US Patent and Trademark Office, were affected, as reported by the US-China Economic and Security Review Commission [42].

Observers reported that at 15.50 UTC on April 8th, China Telecom started to advertise more that 50,000 prefixes, basically stating ownership of those networks. The US was the country which was most affected by this “hijack”, followed by China itself [43]. Questions were raised as to whether this incident was due to “sub-prefix hijacking” i.e. the announcement of more specific prefixes (e.g. 196.1.0.0/24 instead of 196.1.0.0/20). It was found that less than 1% of the hijacked address space was due to “sub-prefix hijacking” and the real problem turned out to be a major misconfiguration [44].

As opposed to the YouTube/Pakistan Telecom incident, traffic was not black holed but were correctly delivered to the final destinations. This kind of incidents happen all the time in the Internet, but they are quickly identified, as they would, most of the time, cause outages. If for example, a small ISP starts advertising a more specific prefix, traffic over the Internet will be redirected to that small ISP. If it does not have enough capacity to handle so much traffic, router will be overloaded and will eventually crash, creating a denial of service (DoS). China Telecom actually had sufficient resources to handle this
massive traffic going through its network and no disruption in service was observed, even if traffic was redirected through an illegitimate path.

AT&T

<table>
<thead>
<tr>
<th>peers</th>
<th>peers</th>
</tr>
</thead>
<tbody>
<tr>
<td>China Telecom</td>
<td>AS LEVEL3</td>
</tr>
</tbody>
</table>

Announces AS PATH LEVEL3, Verizon, Verizon-Wireless to 203.190.56.0/21

Fraudulently announced 203.190.56.0/21

<table>
<thead>
<tr>
<th>AS</th>
<th>customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verizon</td>
<td>203.190.56.0/21</td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
</tr>
</tbody>
</table>

Figure 8: China Telecom traffic interception

Figure 6 shows how the interception attack happened. AT&T received two announcements for the 203.190.56.0/21, one from China Telecom (fake one) and one from AS LEVEL3. Since both are advertising the same prefix, BGP will choose the shortest AS_PATH i.e. China Telecom. Luckily enough, China Telecom has correctly configured forwarding tables on their routers that understood that the traffic for 203.190.56.0/21 has to be forwarded to the correct network in the US. This is how traffic flowed from AT&T to Verizon Wireless through China Telecom.

3.9 Conclusion

This chapter showed us how the limitations of BGP can be detrimental to the interdomain routing infrastructure and by extension, to the whole Internet. We have also seen that BGP does not have any mechanism to protect the integrity of information and there is no means to validate the authenticity and freshness of BGP messages [28]. The lack of origin authentication means that a BGP speaker can potentially originate a prefix for which it does not hold the “right-of-use”. We have also seen that another major issue is path validation. BGP has no way to determine whether a route is valid and whether the path announced by an AS has not been tampered with.

Finally, BGP has some inherent vulnerabilities due to the fact that as it uses TCP/IP as transport mechanism. The consequences are multiple: passive attacks such as eavesdropping, denial-of-service attacks, prefix hijacking, and path modification. As trust has become an issue, having some secured means to validate announcements received by unknown BGP speakers is therefore of paramount importance.
4 Interdomain Routing Security

4.1 BGP Security requirements and mitigation techniques

The two previous examples of an interception attack (section 3.8.1) and a prefix hijacking (section 3.8.2), show us how vulnerable the interdomain routing is. Interdomain routing security is a multi-layer problem and should be tackled using a multi-layered approach. It is obvious that routers, like any other networking devices, need to be properly secured to prevent any unauthorised physical access. Bellovin S. (2003) indicated in his paper how cuts in a physical link could help to perpetrate interception attacks [45]. From a logical point-of-view, the security requirements are the protection of the integrity of messages being transmitted and the ability to get assurance of the validity of information. Christian and Tauber (2008) made some recommendations on the two main areas to secure, i.e. the data payload of the protocol and the data semantics of the protocol [46].

4.1.1 Security of the data payload

To protect the payload of BGP messages, we need to protect the BGP session and the transport mechanism i.e. TCP. Several techniques are used to ensure:

1. **Message Integrity**: TCP-AO (TCP Authentication Option) is the latest technique developed by the IETF and it obsoletes TCP-MD5 [47]. It makes use of MACs (Message Authentication Codes) to ensure message authenticity and it also protects against replay attacks - as it makes use of keyed-hash functions.

2. **Message confidentiality**: The BGP protocol does not have any in-built mechanism to ensure confidentiality of information. As BGP relies on TCP/IP, technologies devised for IP layer security can be used to protect BGP messages. IPSEC is one of them and it provides the authentication, data integrity and anti-replay services on a point-to-point basis, i.e. between BGP speakers [3].

3. **Hop Integrity**: This service enables BGP speakers to do entity authentication. If a router R receives a message M from another router R’, R should be able to verify that M is indeed coming from R’. R can therefore check that M has not been tampered with during transmission and is not a replay of an old message [48].

4. **Protection against message spoofing**: BGP UPDATE messages are normally exchanged between adjacent routers i.e. one hop away but there are cases where BGP speakers are separated by multiple of ASes (multi-hop BGP session). How would a router distinguish between a message coming from an adjacent hop and a message coming from a distant hop? BGP uses the Generalized TTL Security Mechanism (GTSM) [49], which basically assigns a value of 255 to a session and decrements it as it passes a hop. In that case, a router can accept or deny a message it is receiving from a neighbour by checking the TTL value. GTSM can help to prevent message spoofing.

4.1.2 Security of the data semantics

Now that the payload between a pair of communicating routers can be secured, how can we ensure the correctness of the information received? Without a means of validation, a legitimate BGP peer can be sending wrong information to another BGP peer. As we have seen earlier in the YouTube/Pakistan Telecom incident [9], a misconfiguration can propagate to the outside world, if not filtered, and cause networks to become
unreachable. There are four main security requirements when considering the security of data semantics:

1. **Origin authentication**: How can we confirm that an AS originating a prefix has the right to do so? For example, if a BGP speaker receives an announcement from AS1234 as origin AS for 196.1.0.0/16, how can we validate this information?

2. **Path Validation**: Suppose a BGP speaker receives an announcement from AS1234 as origin AS for 196.1.0.0/16. How can we make sure that AS1234 indeed can reach the network as it claims?

3. **Announcement authorisation**: Has the owner of the prefix authorised the AS to announce its network to its peers?

4. **Adherence to routing policies**: Is the route being announced following the routing policies as set by the relying party? Basically is the AS_PATH received an acceptable one based on local rules.

The current best practices to prevent such mistakes to occur are the use of bogus announcements filtering techniques and the use of Internet Routing Registries (IRRs) [7].

### 4.1.2.1 Enabling defensive filtering of bogus announcements

An AS can define its own routing policies that are implemented in the form of ingress (incoming) and egress (outgoing) filters [50]. Those filters are used to selectively accept or reject BGP UPDATE messages coming from neighbours. Filtering is necessary especially in the case of special use address blocks such as 10.0.0.0/8 (used for private networks) [51]. Operators should also filter bogus address space to prevent bogus route announcements. Those address spaces usually referred to as “bogons” are usually unallocated or reserved and they should not appear in a routing table.

However, address space allocations change very rapidly as the result of the rapid growth of the Internet and therefore “bogon” filters need to be kept up-to-date continuously. This can be achieved by making use of online sources of bogon addresses such as Team Cymru’s bogon IPv4 and IPv6 address space list [52].

Below are some common filtering guidelines as recommended by the NISCC Best Practices Guide on BGP and NIST [26]:

1. Address space reserved or assigned for future use should not be used for routing. E.g. 192.168.0.0/16 is used for internal networks.

2. Space that has not been allocated to anyone is considered as bogon space and should not be used for routing. Announcement of bogon routes by a BGP speaker is usually considered as a misconfiguration or a malicious activity.

3. Routes advertised should be aggregated as much as possible. Filters should be configured to deny multiple de-aggregated prefixes in order to keep the routing table consistent. Keeping the routing table small will also reduce the number of BGP messages between neighbours.

4. Reject over-specific routes. For example, advertising blocks that are smaller than 256 addresses (/24 in CIDR notation) will create exponential growth of the routing table and should be filtered out.

Filtering is a very important tool to protect the interdomain routing against misconfigured and bogon route propagation. However, due to the very dynamic nature of the Internet, filters are not always very accurate and can sometimes be out-of-phase with latest IP address allocations.
4.1.2.2 Internet Routing Registries

Internet routing registries (IRRs) form a set of databases holding routing information in a globally distributed fashion [7]. The role of an IRR is to provide a central repository where network operators can publish and exchange their routing policies. The registries operate by mirroring routing information from one another to provide a complete view of the Internet routing topology.

IRRs can help to reduce the problem network operators have with protective route filtering. BGP neighbours usually exchange information on a trust-based relationship, whether it is between peering networks or between provider and customer networks. This means that protective filtering is not always enforced. However, with an IRR, protective route filtering can be automated to change dynamically as routing policy information is made readily available. For example, an upstream provider can decide to create route filters based only on the information provided by its customers in a routing registry. In that case, any other prefix advertised by the customers and not in the routing database will be filtered out.

Most of the RIRs today maintain their own routing registry, as they are themselves responsible for IP resources and AS number allocations. Routing policies are stored in a special format called the Routing Policy Specification Language (RPSL) [53], which is the format used to store information in the WHOIS database [54]. The WHOIS database is the only authoritative database of resource ownership information. Routing registries maintained by RIRs have the advantage of being protected by the same authentication mechanism used to protect resource allocation. Fig. 8 shows network 196.1.0.0/16 being advertised by AS1234. AS1234 can therefore announce this prefix to AS3356, AS1299 and AS6939 and can receive any update from the same peers. Such information is then used to create routing configuration files.

```
aut-num: AS1234
as-name: Example ASN
descr: ASN announcing 196.1.0.0/16
country: MU
export: to AS3356 announce AS-CUSTOMERS
export: to AS1299 announce AS-CUSTOMERS
export: to AS6939 announce AS-CUSTOMERS
import: from AS3356 accept ANY
import: from AS1299 accept ANY
import: from AS6939 accept ANY
source: AFRINIC
```

```
route: 196.1.0.0/16
descr: Example Route object
origin: AS1234
country: MU
source: AFRINIC
```

Figure 9: Example of routing information in a routing registry

However IRRs have their own limitations. There is no guarantee that information stored in a routing registry is up-to-date and complete. If a network operator does not update its routing policies in a timely manner, inconsistencies can easily crop up and therefore this could engender routing issues. A study done by BGPmon.net showed that only 46% of all the prefixes in the routing table have a valid route object, which means that if everybody on the Internet decides to apply strict IRR filtering, 54% of all prefixes in the routing table will not be reachable [55].

Another main drawback is the reluctance of network operators to unveil their routing agreements with their peers as those are sometimes considered as trade secrets. Having this information public can help competitors to gain critical data about their network topology and peering agreements. It is also advocated that some IRRs today lack proper authentication and route information validation mechanisms [56]. We are therefore far from having a global, secure and consistent routing policy database.
4.2 BGP Security proposals

The mitigation techniques mentioned above have not proved to be sufficient enough in providing robust interdomain security. The main issues, which are message integrity, origin authentication and path validation remained unsolved. Much effort has been injected over several years to try to find a standard solution to BGP security and the most notable solutions proposed are S-BGP (Secure BGP) [3] and SoBGP (Secure origin BGP) [4], each having a different security v/s deployability ratio.

Other proposals not discussed here are Origin Authentication (OA) [57], Pretty secure BGP (psBGP) [58], Interdomain Route Validation (IRV) [59], Signature Amortization (S-A) [60], Secure Path Vector (SPV) [30] [61] and the Listen and Whisper protocol [62].

4.2.1 S-BGP

Secure BGP (S-BGP) was designed to provide message integrity, origin authentication and path validation. It is deemed to be one of the most complete security solutions to BGP security today. S-BGP ensures that UPDATE messages, exchanged between peers, are not tampered with during transit. This is achieved by using point-to-point security provided by IPSEC [31].

S-BP proposes two separate Public Key Infrastructures (PKIs) for two different purposes: (i) authenticating AS numbers, BGP speakers and router associations (ii) providing IP address allocation certificates. In both cases, ICANN/IANA has the role of trust anchor i.e. the top-most certificate authority (CA). IANA holds the database of all AS number assignments to RIRs, which are then entitled to re-allocate those AS numbers to different networks.

Three certificates are used here namely for: authenticating an AS, authenticating a BGP speaker and finally a third one to associate an AS number to a router ID. This architecture provides origin authentication by means of digital signatures i.e. when a BGP speaker signs a message with its private key, the relying party (another BGP peer) can verify the digital signature using the corresponding public key. The other PKI is used to bind an address block to an organisation. This is to certify that the organisation has a “right-of-use” over the IP address block.

Finally, the above-mentioned PKIs are used to create two sets of “attestations” based on digital signatures. The first one is an Address Attestation (AA), which basically allows an AS to advertise a prefix. The second attestation is the Route Attestation (RA) whose role is to authenticate an AS Path in a route announcement. This feature provides path validation.

However, S-BGP never achieved wide-scale deployment for mainly three reasons. The fact that path validation is ensured through the generation and verification of digital signatures, adds lot of computational overhead on the whole infrastructure. It is also very resource intensive due to the enormous amount of route attestations that it might generate. And finally, it is difficult to maintain two public key infrastructures side-by-side as it makes maintenance and operations rather bulky [12].

4.2.2 SoBGP

Secure origin BGP (soBGP) can be considered as the lightweight version of S-BGP. The design of soBGP does not include the protection of message between communicating BGP speakers but the main design goals of soBGP are quite similar to S-BGP i.e. origin authentication and path validation. Kent S. (2003) in his status update on BGP security, stated that soBGP has a different approach to validation of router attestation by reducing the overhead of signing every advertised [63].
Similarly to S-BGP, soBGP uses a centralised hierarchical PKI model based on the IP resource allocation hierarchy to certify “right-of-use” over an IP address space. To authenticate AS number, the concept of a decentralized “web-of-trust” is used.

soBGP makes use of three types of certificates:

- An EntityCert whose role is to bind an AS number with a public key
- An AuthCert (Authorisation certificate) which binds an organisation to a given prefix
- An ASPolicyCert authenticates the policies of an AS i.e. list of peers, import and export rules and other connection details important to ensure path validation.

### 4.3 Deployment considerations

Below is a summary of the different BGP security solutions and mitigation techniques that were devised and used over time as given by Butler et al. in their survey of BGP security issues and solutions [32]. In use gives the deployment status of the solution, Type indicates whether it uses cryptographic techniques or anomaly detection for error detection (or both).

The security services provided by the different approaches are: topology authentication (that ensures the AS_PATH attributes correspond to the correct topology), path and origin authentication.

<table>
<thead>
<tr>
<th>System</th>
<th>In use</th>
<th>Type</th>
<th>Topo. Auth.</th>
<th>Path Auth.</th>
<th>Origin Auth.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Filtering [22] [50]</td>
<td>yes</td>
<td>Anomaly</td>
<td>Weak</td>
<td>Weak</td>
<td>Weak</td>
</tr>
<tr>
<td>Routing registries [7]</td>
<td>yes</td>
<td>Anomaly</td>
<td>Weak</td>
<td>Weak</td>
<td>Weak</td>
</tr>
<tr>
<td>soBGP [4]</td>
<td>no</td>
<td>Both</td>
<td>Strong</td>
<td>None</td>
<td>Strong</td>
</tr>
<tr>
<td>Origin Authentication (OA) [57]</td>
<td>no</td>
<td>Crypto</td>
<td>None</td>
<td>None</td>
<td>Strong</td>
</tr>
<tr>
<td>psBGP [58]</td>
<td>no</td>
<td>Crypto</td>
<td>Weak</td>
<td>Strong</td>
<td>Weak</td>
</tr>
<tr>
<td>IRV [59]</td>
<td>no</td>
<td>Both</td>
<td>Strong</td>
<td>Strong</td>
<td>Strong</td>
</tr>
<tr>
<td>SPV [61]</td>
<td>no</td>
<td>Crypto</td>
<td>Strong</td>
<td>Strong</td>
<td>None</td>
</tr>
<tr>
<td>Signature Amortization [60]</td>
<td>no</td>
<td>Crypto</td>
<td>Strong</td>
<td>Strong</td>
<td>None</td>
</tr>
<tr>
<td>Listen and Whisper [62]</td>
<td>no</td>
<td>Anomaly</td>
<td>None</td>
<td>Weak</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 7: BGP Security solutions comparative analysis

As shown by table 7, the only solutions deployed are selective route filtering and Internet Routing Registries (IRRs). However, as we have mentioned before, the former solutions are not effective countermeasures to the different issues of interdomain routing. Most of the solutions involving PKIs faced major deployment issues due to the computational and technical overhead they represented.

Indeed, networks operators were wary about the effect cryptography might have on routers’ performance and this could adversely affect the convergence delay of BGP routes [64]. BGP routes are said to have converged when all UPDATE messages have propagated to the neighbouring BGP speakers such that all their routing tables hold the exact same reachability information.
4.4 Conclusion

The BGP protocol has proved its efficiency in enabling the Internet to grow and to scale to the size it is nowadays. However, its vulnerabilities and weaknesses create a fertile ground for attackers to easily subvert Internet traffic and create unwanted circumstances. We have also seen how easy it can be to break the Internet by propagating false routing information and how difficult it can be to troubleshoot interdomain routing anomalies in such distributed environment.

There have been several more or less successful attempts to reduce the attack surface of the BGP protocol. The problem however, remained unchanged, as most of those security fixes are built on top of the protocol and are optional. Preventive measures such as bogus announcement filtering and the publication of routing policies in Internet Routing Registries (IRRs), though necessary, have proved to be incomplete and rather inefficient.

Furthermore, security frameworks such as S-BGP and soBGP, faced lot of deployment issues due to their high level of complexity and technical overhead. Adoption of those bulky cryptographic security mechanisms proved to be a real challenge.

It was therefore important to adopt a more comprehensive approach to find a solution that would provide security, verifiability, scalability, reduced complexity and deployability. After years of research and unfruitful attempts, the solution space seems to converge on the Resource Public Key Infrastructure (RPKI) as the stepping-stone for interdomain security.
5 Resource Public Key Infrastructure

Resource Public Key Infrastructure (RPKI), also known as Resource Certification, is a PKI-based security framework built specifically for certifying ownership of Internet number resources. RPKI is a product of the Secure Inter-Domain Routing (SIDR) working group of the Internet Engineering Task Force (IETF), whose mission is to reduce the two main vulnerabilities of interdomain routing: \textit{origin authentication} and \textit{path validation} [65]. This chapter will explain the architecture behind resource certification and the security mechanisms used to provide interdomain routing security. We shall also look into the practical aspects of RPKI and see how the artefacts of the system are deployed and managed to provide the required security services.

5.1 Resource Certification through RPKI

As in a traditional public key infrastructure, RPKI makes use of X.509 public key certificates, which is based on the PKIX profile [66]. Examples of X.509 certificates are SSL certificates for domain name authentication or identity certificates used to bind a person’s identity to a public key. However, resource certificates have been extended to contain information about Internet number resources (IPv4/IPv6 addresses and AS numbers) as defined in RFC 3779 [67].

The aim of the certificate is to attest that the subject (an organisation) has a “right-of-use” over the resources mentioned in the certificate. The certificate issuer is the only authority (CA) that can attest resource “holdership” by signing the public key certificate of the resource holder using its private key. This action binds the subject of the public key certificate to the list of resources and validation can thus be established through signatures.

We shall see later on how those resource certificates are used to create other signed objects that are useful for the operations of the RPKI framework and most importantly Route Origin Authorization (ROA) objects that are used to enable \textit{origin authentication}.

5.1.1 Resource Certification hierarchy

We have seen that Internet number resources are managed based on a hierarchical model, with the top-most organisation being IANA (see section 2.1). Resource certification actually follows the same hierarchical delegation structure, where resource certificates are assigned to the five different RIRs and transitively from the RIRs to LIRs, NIRs or end users. By verifying the signature on a resource certificate, a relying party (RP) can have the assurance of the authenticity of the resource allocation [68]. Any entity holding resources or which can in turn re-allocate subset of those resources to a lower-level entity becomes a Certificate Authority (CA).

In the normal resource allocation scenario, IANA is the authoritative organisation as it holds the register for IP and AS number allocations. However, it is very likely that ICANN would become the agency entrusted by the five RIRs and other stakeholders, to operate the Global Trust Anchor (GTA) [69]. There are three different entities in the RPKI: (i) the root CA or the Trust Anchor (TA), which is a self-signed CA (ii) intermediate CAs and (iii) end-entities (EE) commonly referred as RPKI products or signed objects.

The role of the CA is to sign the public key certificate of other sub-CAs or sign attestations of resource ownership for end-users. The latter is achieved by means of End-
Entity (EE) certificates. Figure 9 below shows us the hierarchy of certificates mapped onto the hierarchy of resource allocation.

![Resource certification hierarchy diagram]

Figure 10: Resource certification hierarchy

The table below gives an example of resource allocation from IANA to an end-user. In a resource certification hierarchy, IANA will hold a self-signed certificate reflecting the resources of the IANA registries.

As the root CA, IANA will deliver CA certificates to AFRINIC to certify the resources they hold. AFRINIC can then deliver another CA certificate to LIR-A, which will in-turn would deliver another CA certificate to ISP-X, to attest that ISP-X is a legitimate holder of the address space.

The ISP can then use its resource certificate to issue EE certificates over designated resources to verify signed objects called ROAs (Route Origin Authorization), whose role is to explicitly authorise an AS to advertise a prefix. EE certificates are also used verify other cryptographically signed objects important to ensure integrity of the RPKI architecture. (See section 5.2 and 5.3)

<table>
<thead>
<tr>
<th>Organisation</th>
<th>IPv4</th>
<th>IPv6</th>
<th>ASN</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>IANA</td>
<td>0/0</td>
<td>0/0</td>
<td>1 - 2^32</td>
<td>Issues resources to RIRs</td>
</tr>
<tr>
<td>AFRINIC</td>
<td>196.0.0.0/8</td>
<td>2001:4200::/23</td>
<td>327680 - 328703</td>
<td>Issues resources to LIRs</td>
</tr>
<tr>
<td>LIR-A</td>
<td>196.1.0.0/16</td>
<td>2001:4200::/32</td>
<td>327681, 327682</td>
<td>Large ISP</td>
</tr>
<tr>
<td>ISP-X</td>
<td>196.1.0.0/23</td>
<td>2001:4200::/48</td>
<td>327681</td>
<td>Small ISP</td>
</tr>
</tbody>
</table>

Table 8: Resource allocation example

5.1.2 Resource certificate types

As mentioned before, there are three main types of certificate in RPKI. Those are the Trust Anchor (TA), the CA (Certificate Authority) and the EE (End Entity) certificates [68].
5.1.2.1 Trust Anchor (TA) and Trust Anchor Locator (TAL)

As in any conventional PKI, there is a Trust Anchor, which serves as a root certificate for relying parties (RPs) to validate a certificate or a signature. In the case of RPKI, the top-most CA is held by IANA. It contains all the resources sub-allocated in the tree below it. In an ideal world, there would be the one root certificate and its number resources would be:

- 0/0 for IPV4
- 0/0 for IPV6
- 1 - 4294967296 for AS numbers

However, the resource allocation and sub-allocation practices make it such that there are CAs and intermediate CAs. This means an RP (for e.g. an ISP) can choose to set it trust anchor to be an LIR (Local Internet Registry), an NIR (National Internet Registry) or an RIR (Regional Internet Registry), depending on the type of allocation that has been done. Similarly, the trust anchor an LIR would be an RIR and finally, the RIR would use the IANA’s Root CA as final trust anchor. In RPKI, a TA is distributed to RPs through a special object called a Trust Anchor Locator (TAL) [70].

For the time being, each RIR is running its own root and encoding its resources only. So for example, the AFRINIC’s trust anchor certificate will only contain IANA’s allocation to AFRINIC.

5.1.2.2 CA certificate

Resource holders such as RIRs, NIRs or ISPs would all receive a CA certificate, also known as a resource certificate, signed by the TA’s private key and used to attest that the recipients are the legitimate resource holders of the allocated Internet number resources. One notable difference between a traditional PKI and RPKI is that subject’s name is chosen by the CA and not by the subject. This is because the main objective of RPKI is to certify legitimacy over allocated resources but not to certify the identity of a certificate holder. The subject’s name in resource certificate is therefore insignificant to the outside world and therefore helps to reduce the liability of the issuer, in case the certificate is used for other purposes.

5.1.2.3 End-Entity (EE) certificate

EE certificates appear at the bottom of the PKI. They are issued by the CA certificates and their usage is limited to validate digital signatures. The private key of the EE certificate is used to sign special objects such as ROAs and manifests [71], which are based on the CMS (Cryptographic Message Syntax) encapsulation format [72]. The certificate is used to verify the validity of the CMS and the private key is used only once to generate the signature. This means that there is no need to store the private keys after generating the signature and can therefore be discarded immediately. It thus reduces the key management burden of EE certificates.

5.1.3 Resource certificate profile

Huston et al. described the profile of resource certificate in RFC 6487 [73]. The main fields are indicated in the table below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version number of the X.509 certificate. Currently on version 3</td>
</tr>
</tbody>
</table>
5.1.4 Algorithm and key size

The RPKI protocol has specified the use of RSA algorithm for the computation of certificate signatures [74]. The default profile for all RPKI related objects i.e. resource certificates, manifest files, Certificate Revocation Lists (CRLs) and ROAs is SHA-256 with RSA (sha256WithRSAEncryption) or SHA-512 (sha384WithRSAEncryption). The mandated RSA key size is 2048 bits and the public exponent of the RSA algorithm (e) is F4 (65,537) [75].

5.1.5 Validation

Validation works by establishing the chain of trust from the root CA. As in a traditional PKI, the root CA will sign the public key certificate of the child with its private key and the intermediate CA signs the EE certificate’s public key using its private key. RPKI also makes use of a Certification Revocation List (CRL) to maintain a list of revoked certificates relative to a CA instance [76]. Resource certificates can be revoked for a number of reasons. It may be due to a cancellation of agreement between an LIR and an ISP; shrinkage in the resource allocation set or in the case of a CA key rollover.

A certificate is considered as valid if the signature can be verified, by recursively validating the issuer’s certificate until verification at the root CA level. However, for resource certificates, RFC 3779, which defines X.509 extensions for IP addresses and AS numbers, adds validation on resource sets. For example, AFRINIC has a certificate (C_AFRINIC) with the resource set A: {IPv4: 196/8 | IPv6: 2001:4200/23 | ASN: 327680-328703} and delivers a certificate for LIR-A (C_LIR-A) with resource set B: {IPv4: 196/8, 202/8 | IPv6: 2001:4200/23 | ASN: 327680-328703}. Validation of certificate C_LIR-A will fail, as B is not a subset of A.
Similarly, EE certificates used to validate RPKI products (ROAs, CRLs and manifests) can be revoked by the issuing party. For example, Manifest files needs to be renewed on a daily basis to cater for changes in the RPKI repository. In that case, EE certificates used to verify the manifest file have a validity period of one day. The role of a manifest is to verifiably list the content of a repository or publication point of a certificate authority (CA) [76].

5.2 Resource Certificate management

To ease the deployment of this infrastructure, RPKI takes advantage of well-established certificate management technologies and best practices. The SIDR working group has defined a Certificate Policy (CP) for the RPKI based on the existing certificate policies of traditional PKI. Changes have been made for it to reflect the unique purpose for which it has been designed, which is the attestation of Internet number resources holdings [77].

The management of Internet number resources has a direct impact on the management of resource certificates. The PKI supporting resource certification therefore naturally inherits the address space allocation operations which are basically resource revocation, resource expansion and resource shrinkage.

5.2.1 Certificate Issuance and revocation

The relationship between an issuer and a subject of a certificate in RPKI is usually the one between an allocation body and a resource holder. This can be RIRs and its members or LIRs and its customers. The agreement between the resource allocator and resource user is usually bonded in the form of legal contract, only valid over a certain period of time. RPKI, therefore, needs to conform to those legal requirements and issue certificates that are time-limited.

When RPKI will be fully deployed, resource certificate will be de facto delivered to all resource holders, as a means to attest their “right-of-use” over those resources. As opposed to normal certification practices, the subject will not necessarily request a resource certificate but will be assigned one.

There are two main use cases in resource certification and those are resource expansion and resource shrinkage. Issuance and revocation are rather straightforward and once revoked all children certificates and products (ROAs, CRLs and manifests) will be invalidated. When an organisation receives additional resources from its resource provider, a new certificate is issued. The new certificate would actually cover the old certificate in terms of resources. The old certificate is not revoked but simply replaced by keeping the same Subject Information Access (SIA) which is the identifier used to make the link between the parent and the subject’s certificate repository. Only the “serial number” or “subject” will change and since issuance of the new certificate with additional resources is done using the same public and private key pair, validation will still succeed [76].

It is a little bit more challenging when dealing with resource shrinkage. There are circumstances where a resource holder will have to give back resources to its registry or ISP. In such cases, the old certificate shall be revoked to restrict attestation of resources “not held anymore”.

However, RPKI does not control subordinate certificates issued to clients and other resource holders down the chain. Similarly, the new “shrunk” certificate will have the same certificate name and SIA, meaning validation of certificates with resource sets within the new boundaries will succeed and those outside the new resource boundaries will fail. This can have an adverse effect on the validity of ROAs and can therefore affect
route information validation. Remember, an entity can select its own trust anchor and make validation against it.

If the trust anchor’s (TA) resource set has been shrunk but relying parties has not been updated, objects down the line will still be considered as valid. The best approach is a “bottom-up” propagation of the resource shrinkage and child certificates are re-issued accordingly [78].

5.2.2 CA Key rollover

Another scenario that requires certificate re-issuance is a key rollover. Key rollover is an important practice in any cryptographic key management. The idea is to renew the public and private key pair of the CA. It is normally practised on a scheduled basis, typically every year for a CA. However, in the event of a key compromise, an emergency key rollover procedure must be followed and a new key pair is generated. This automatically entails revocation of the old certificate and issuance of a new certificate for the CA.

Huston et al. described two main properties for key rollover in RPKI in their best current practice document [76]:

1. CA certificates issue EE certificates to sign RPKI objects, called ROAs, which are used at the router level to construct BGP filters (more details in section 5.3). A key rollover procedure, at the CA level, should ensure that validation of RPKI objects by relying parties, down the chain, remains consistent. As far as possible, the SIA and AIA parameters of the new certificate(s) should remain unchanged, such that validation follows the same certification paths all the time.

2. Even though in a key rollover procedure, the public and private key pair of a CA certificate will change, it is recommended that in RPKI, a key rollover procedure will ensure that issuances of all child certificates is not necessary and pointers (SIA and AIA) to the certificate and trust anchor should be preserved.

5.2.3 Up/Down protocol

In the RPKI, any resource holder that can sub-allocate their resources to other entities can become a CA and can either issue other CA certificates or EE certificates. There is a parent and child relationship between a CA (issuer) and a sub-CA (subject). To this end, the SIDR working group has defined a protocol for the provisioning of resource certificates commonly called the “Up/Down” protocol. The protocol basically defines a set of interactions that would allow a subject to request certificate issuance, revocation and retrieve status information from the parent [79].

The protocol is a simple query/response interaction between the client (subject) and server (issuer) over HTTP. The messages are exchanged using XML with a content type of “application/rpki-down” in both directions. The payload of the query and server responses are “well-formed” Cryptographic Message Syntax (CMS) [72] objects, encoded in the Distinguished Encoding Rules (DER) format for ASN.1 [80].

Before communication is started, the Trust Anchor (TA) of the signing key pair and the certificate chain are mutually established between the client and the server. The public key is used to verify the signature in the CMS message received.

The protocol caters for replay attack by operating on a sequential basis. Messages sent will always receive a response whether positive or negative and the server will deny any further requests of a client if it has not yet responded to a previous message. A simple certificate issuance scenario is illustrated in figure 10.
The different types of message are:

1. **LIST**: The subject starts by requesting the set of resources (resource class) for which it is entitled for and allocated by the parent.

2. **LIST_RESPONSE**: The issuer responds to the client by sending back a set of resources along with the different CA certificates for which the client is a subject.

3. **ISSUE**: The child chooses the resource class and the parent CA from which the new certificate needs to be issued. It also sends the list of resources to be certified.

4. **ISSUE_RESPONSE**: The parent sends a new certificate according so rules defined in [79].

5. **REVOKE**: is used when a child wants to instruct the parent to revoke all its certificates.

6. **REVOKE_RESPONSE**: is the corresponding response is a positive revoke message.

7. **ERROR_RESPONSE**: used in case of negative feedback, for example with malformed XML messages or inconsistent certificate issuance request is received by the parent.

### 5.3 RPKI-Based Origin Validation

Now that we have a framework in place to certify resource allocation and to verify whether a resource holder is actually a legitimate one, we can start tackling one of the main problems of interdomain routing: *origin validation*. The idea is about finding a solution that would allow relying parties to verifiably ascertain whether an AS is authorised to announce a prefix. This is achieved by using dedicated EE certificates to generate cryptographically signed route filters, called Route Origin Authorizations (ROAs).

#### 5.3.1 Route Origin Authorization

A ROA is a structured signed object whose role is to attest that an AS has been authorised, by the holder of a resource block, to originate all or part of the address space.
to other BGP speakers. ROAs, similarly as manifest files (see section 5.3.3), are products of the RPKI framework i.e. they have been signed by EE certificates issued by the Resource Certification framework. The format of a ROA is described in RFC 6482 [81] and it is basically made up with a CMS expressed in ASN.1 format, based on the RPKI profile for signed objects [71] and it contains the AS number and the set of IP addresses. The EE certificate, used in the CMS signing, is issued by a resource certificate (CA) and contains the set IP resources the ROA will cover.

ROAs by themselves do not contain any routing validation information; they only represent the authority of an AS over a prefix. We shall see how ROAs are used to achieve origin validation and to construct filters at the router level in sections 5.3.4 and 5.3.5. The validity of a ROA is tied to the EE certificate it encompasses. The EE certificate has a validity period determined by the resource holder. The ROA is signed by the private key corresponding to the public key in the EE certificate of the encapsulated CMS. Once a ROA is signed, the private key can be discarded, as the only required information is the public key to validate the signature.

Below is a simplified view of the content of a ROA (without the EE certificate):

```
version: 0
as_id: 37668
prefixes: 41.222.48.0/20-
  24
signing certificate:
  serial: 124 (0x7C)
  not before: 2013-07-17T11:21:40
  not after: 2037-07-17T11:36:40
  subject: CN=51e646d4-3ee4
  sia:
    signedObject:
      rsync://rpki.dev.mu.afrinic.net/repository/6196EEB14AA.roa
calIssuers:rsync://rpki.dev.mu.afrinic.net/repository/cgtKcjSWk.cer
resources:
  ipv4:
    41.222.48.0/20
```

Figure 12: Example of a ROA

The main information here is the “as_id” which contains the origin AS number authorised to advertise the prefix in the “prefixes” field. It also contains information about the EE signing certificate, namely the validity dates and public points of the issuer and as well as the subject. The “calIssuers” field points to the resource certificate which has issued the EE certificate. The prefix “41.222.48.0/20-24” includes the notion of maximum length (24 in this case) that describes the depth of authorisation. In other words, all prefixes of length /20 to /24 within the range will be covered by the ROA above.

5.3.2 ROA management

A ROA is said to be valid if the underlying EE certificate is valid and has not been revoked. In other words, it must be itself validated by the issuing parent certificate. The public key in the EE certificate must also be able to verify the signature of the CMS and the IP resources contained in the EE certificate must be within the boundaries of the issuer’s resource certificate. Similarly, a ROA can be considered as “invalid” if one of the above conditions is not met. The CA needs to update and publish the corresponding
CRL (Certification Revocation List) on a public repository such that relying parties can know which ROAs have been revoked and cannot be trusted anymore.

However, ROA revocation should be handle with care. In a fully or even partially deployed RPKI environment, revoking a ROA means that routing announcement corresponding to the routing information contained in the ROA, can be considered as untrusted. So the principle of “make before break” should apply in ROA management. Before revoking a valid ROA, another ROA with the same or greater coverage should be issued by the resource holder [68].

5.3.3 Publication of RPKI objects

One of the main components of the RPKI architecture is the repository. It is the central publication point where relying parties can fetch the resource certificates, CRLs and signed objects such as ROAs and manifest files. The trust anchor of the PKI is usually located in the repository of the top-most CA. In the case of RPKI, IANA would hold a repository with a trust anchor and five resource certificates for the five RIRs, together with an updated CRL and manifest file. However, we will see in Chapter 6 that it is currently not the case and why it represents a challenge.

5.3.3.1 Chain of trust

Any RPKI signed object in the repository (resource certificates, CRLs, ROAs and manifests) can be verified by another certificate. The issuing certificate in RPKI is a resource certificate and the chain of trust is built through SIA (Subject Information Access) and AIA (Authority Information Access) data. Those are URI that are found in the certificate such that a relying party can know which path to follow to validate a certificate. In figure 12 below, Certificate A has two child certificates (B and C). The AIA of Cert B and Cert C will reference Cert A as the issuing CA. The SIA of issuing CA (Cert A) will reference URI of the publication directory where the issuing CA will hold its CRL [68].

![Figure 13: Use of SIA and AIA extensions in the RPKI](image)

5.3.3.2 Manifest files

To ensure consistency of the repository, RPKI makes use of a special signed object called the “manifest”. Just as the ROA, the manifest comprises an EE certificate within the
CMS wrapper of the RPKI signed object. The EE certificate is used to verify the signature of the manifest and the issuer of the EE certificate is the resource holder. The manifest contains a list of all the objects that need to be present in the repository, together with their hash. Relying parties can therefore verify that the repository is consistent and that the object files have not been modified or deleted. The manifest has a lifetime, which is the validity period of the embedded EE certificate. This certificate needs to be reissued anytime there is a change in the repository.

In the example above, the manifest is listing the different objects in the repository it is “responsible” for. We have three ROAs and one CRL. The second column is a SHA256 hash of the corresponding file. Each manifest has a serial number and a validity period based on the EE certificate. Since the repository itself does not have any security mechanism, manifest files play an important role in keeping the database of RPKI signed objects consistent.

### 5.3.4 RPKI in practice

Managing an RPKI has nothing less to do with managing a normal PKI. RPKI requires the same level of security in terms of hardware and procedures. Certificate issuers, i.e. resource holders have to abide by a Certificate Practice Statement (CPS) as defined by the protocol. Furthermore, RPKI can be deployed in two distinct modes: “hosted” or “delegated”. Each mode has its set of advantages and disadvantages, as we shall see later on. At the end of this section, we will describe the different components of a typical RPKI implementation and their respective role in the management of resource certificates and RPKI signed objects.

#### 5.3.4.1 Certificate Practice Statement (CPS)

The CPS is a mandatory document that defines the management procedures of a Certificate Authority (CA) when running a PKI. The CPS is based on a higher-level document called a Certificate Policy (CP) that sets the base requirements and processes [82]. The CPS starts by defining the roles of every entity in the PKI, starting from the Certificate Authority (CA), the Registration Authority (RA), the subscribers, the relying parties (RPs) and other participants. It defines the acceptable use policies and intended usage of the certificates.

For an operational perspective, details are given on the publication and repository management. It englobes the definition of access control policies and the management of manifest and CRLs files to keep the repository consistent. Information on the naming principles, for example, the identification of the parent and the subject are also defined.

Finally, the CPS sets the key management parameters such as the minimum key size and signature algorithm to be used. The rules of the certificate life cycle and key management

![Figure 14: Example of a manifest file](image-url)
are explained thoroughly as well as the different security controls and procedures important for managing a CA.

5.3.4.2 Deployment modes (Hosted v/s Delegated)

There are two modes in which RPKI can be deployed; these are the “hosted” mode and the “delegated” mode. In the “hosted” mode, the RPKI engine is installed at the parent’s (resource issuer) level and the parent itself manages the child certificates. This means that the CA will hold the private key of the child as well as the keys that generated RPKI signed objects such as ROAs. If the child wants to issue ROAs, it will make use of the parent’s engine to generate the corresponding EE certificates. The advantage is that it lifts up the burden of managing a CA by the child and the latter can make use of security services provides by the CA such as access to a Hardware Security Module (HSM).

“Delegated” mode is when the child (resource holder), for example an ISP, decides to host its own CA locally. In that case, they would need to manage their own private keys, which can present some forms of challenges in term of risk acceptance and confidentiality. The parent will use the UP/DOWN protocol to communicate with the child and vice-versa. The child will need to maintain a fully-fledged PKI with an appropriate CPS.

5.3.4.3 Architecture and components

Figure 15 below describes the architecture of a sample implementation of two RPKI engines for a parent (resource holder and resource issuer) and the child (resource holder). Both entities manage their own CA, as it would be in the “delegated” mode. The schema has been taken from APNIC technical implementation details document [83].

The Child CA first starts by sending a LIST request from the Parent CA. The parent CA will first query its internal resource database (Registry DB) and reply with the list of resources the Child CA is entitled for. The Child CA then creates a Certificate Signing Request (CSR) containing the set of resources needed, which it sends to the parent CA. The parent will sign the request, generate a certificate and send it back to the child. Note that the parent does not know about the child private key as opposed to the “hosted” mode.
Now that the child has a certificate, it can start issuing EE certificates for ROAs and manifest files. The child certificate and its RPKI products will be published in its rsync repository. Similarly, the parent will publish its certificate as well as the necessary manifest and CRL.

### 5.3.5 RPKI-RTR protocol

Now that we can produce ROAs from resource certificates, we need a mechanism to use these signed objects at the router level. As mentioned before, ROAs themselves cannot secure interdomain routing but can be used to generate trusted BGP filters that are based on cryptographically verifiable objects, i.e. the ROAs. RFC 6810 defines the RPKI to Router protocol [84].

The idea behind the RPKI-RTR protocol is to lift up the burden on routers to validate ROAs in order to verify whether an announcement received is authoritative or not. The protocol defines the use of dedicated trusted validator caches, whose role is to regularly collect certificates and ROAs from global RPKI repositories (IANA, RIRs and ISPs) and validate the objects. They usually also act as local caches from which routers will come and pull validated ROAs.

Figure 14 shows on one side the “issuing parties” which are the resource holders and on the other side the “relying parties” which are the consumers of the RPKI objects. Routers can be configured to allow communication with selected validated caches over the RPKI-RTR protocol.

#### 5.3.6 Route Origin Validation using RPKI and ROA

Now the question is: how is origin validation achieved through the use of ROAs? In other words, how are BGP updates affected by ROAs coming from validated caches? Once the router receives the validated ROA payload from the validated caches, this information can now be used in the BGP decision process.
In a fully deployed RPKI scenario, each router can get a list of valid and invalid ROAs covering all prefixes in the global BGP table. However, such a scenario is unlikely to happen and therefore, the best we could expect is to have partial deployment. Therefore if there is no matching ROA for an announcement, we cannot consider it “invalid” by default. Protocol designers have decided to classify a BGP announcement into three different categories:

- **Valid**: If a BGP announcement matches exactly the content of a ROA (authorised AS number and prefix) and the EE certificate is valid, the BGP announcement is considered as valid.

- **Invalid**: If a BGP announcement matches or is covered by (i.e. the prefix is more specific) the prefix in the ROA but the origin AS does not match the authorised AS in the ROA, and no other ROA covers the announcement with the right AS, the announcement is considered as invalid.

- **Not found**: There is no ROA that covers the route prefix.

The table below gives some examples of prefix matching and validity between two ROAs and five BGP announcements.

<table>
<thead>
<tr>
<th>BGP Announcements</th>
<th>ROA: 196.1.0.0/16-24</th>
<th>ROA1: AS 10</th>
<th>ROA2: AS 22</th>
</tr>
</thead>
<tbody>
<tr>
<td>196.1.0.0/12 by AS 22</td>
<td>Not found (shorter than ROA 1)</td>
<td>Not found (shorter than ROA 2)</td>
<td></td>
</tr>
<tr>
<td>196.1.0.0/16 by AS 22</td>
<td>Valid (Matched by ROA 1)</td>
<td>Valid (Matched by ROA 2)</td>
<td></td>
</tr>
<tr>
<td>196.1.0.0/20 by AS 22</td>
<td>Valid (Matched by ROA 1)</td>
<td>Valid (Matched by ROA 2)</td>
<td></td>
</tr>
<tr>
<td>196.1.0.0/24 by AS 22</td>
<td>Invalid (outside ROA range)</td>
<td>Invalid (outside ROA range)</td>
<td></td>
</tr>
<tr>
<td>196.1.0.0/24 by AS 10</td>
<td>Valid (Matched by ROA 1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 10: BGP announcements and ROA matching and validity**

Depending on the risk-appetite of the operator, one can choose to apply a very strict or a more relaxed local policy. Some operators might choose to discard all invalid routes but at the stake of rejecting routes that are not covered by ROAs but yet legitimate. At the end of the day, it is up to the relying party to set their own rules.

Both routing incidents we have seen at the beginning (Pakistan Telecom/Youtube hijack and traffic interception by China Telecom) were due to the announcement of prefixes that did not belong the advertising AS. With RPKI and the use of defensive filters based on ROAs, this would not have been possible. For example, Youtube would have created ROAs and only authorise a specific set of ASes to originate its network. If now Pakistan Telecom decides to advertise Youtube’s network, the upstream provider of Pakistan Telecom (PCCW Global) would validate the announcement by checking whether there is a covering ROA allowing Pakistan Telecom to advertise Youtube’s network. In that case, this announcement would have been considered as “invalid” and would have been rejected.

This is why it is important for the main interdomain routing actors, especially the transit ASes operating at the Tier 1 and Tier 2 levels to adopt RPKI and create ingress and egress filters based on valid ROAs.
5.4 Path Validation with BGPSEC

Now that we have a solution to verifiably ascertain that an origin AS has the right to advertise a prefix, we need to look into finding a solution to the problem of path validation. How can we make sure that the origin AS received in a BGP UPDATE message is indeed coming from the AS it is claiming origin. Origin validation can only help BGP speakers detect misconfigurations or malicious announcements but it cannot prevent a malicious attacker to fake the AS_PATH in a BGP message. This is a work in progress at the SIDR working group and the protocol name to secure BGP path is BGPSEC [85].

We have seen in Chapter 2 the importance of the AS_PATH attribute in the BGP UPDATE message. Its role is to convey a route in terms of a sequence of hops (AS numbers) to a destination (a prefix). BGP speakers, receiving an UPDATE message will either accept or reject the route, based on several criteria. One criteria is the AS_PATH length, the shorter the route, the more likely it is going to be chosen by the best-path selection algorithm. An attacker can subvert the AS_PATH by either removing or adding a hop and therefore making the path invalid. If the path is chosen, this can result in a black hole attack or a traffic redirection, with known consequences.

So the question is how can we “verifiably” make sure that the sequence of AS numbers received in an AS_PATH is actually reflecting the real path to the destination. BGPSEC proposes a solution through “router certificates”. Those router certificates will be issued by the RPKI framework to a router, therefore attesting that the latter is the rightful holder of an AS number. The router equipped with a certificate and its private key would be able to sign outgoing UPDATE messages.

In the BGPSEC framework, BGP speakers would recursively sign the “signed” AS_PATH before sending it to the next hop. This creates an interlocking chain of signatures allowing the relying party i.e. the receiving BGP speaker to validate the signature of each AS in the AS path [86].

The fact that each hop is “forward signing” the BGP message, is fundamental in preventing man-in-the-middle attack as illustrated in the figure 15 [87]. The dark arrows show the real BGP announcements from one BGP speaker to another. Router Z is an evil router that is trying to advertise “fraudulently” a route to B. Suppose a packet needs to be delivered from A to B. Traffic always goes in the opposite direction of BGP announcements. The packet can either take the route AXWB or AXZWB. According to the BGP best-path algorithm, the shortest path will be chosen.

However, in the case above, Z is also claiming to have a route to B. AXWB and AXZB have the same path length. There is a high possibility the “fake” route is chosen and therefore traffic can be redirected and potentially eavesdropped by the malicious router Z.
Figure 17: Illustration of a BGP path subversion attack

Table 10 shows the signatures that the BGPSEC framework will add to the announcements to make the announcement verifiable. Since there is no signature Sb(B>Z) on the route Z->B, Z can only sign the authoritative message coming from W (see announcement 4). Therefore, the relying party X can validate the chain of signature up to B.

<table>
<thead>
<tr>
<th>#</th>
<th>Announcement</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>B to W</td>
<td>Sb(B-&gt;W)</td>
</tr>
<tr>
<td>2</td>
<td>W to X</td>
<td>Sw(W-&gt;X + Sb(B-&gt;W))</td>
</tr>
<tr>
<td>3</td>
<td>W to Z</td>
<td>Sw(W-&gt;Z + Sb(B-&gt;W))</td>
</tr>
<tr>
<td>4</td>
<td>Z to X</td>
<td>Sw(Z-&gt;X + Sw(W-&gt;Z + Sb(B-&gt;W)))</td>
</tr>
<tr>
<td>5</td>
<td>X to A</td>
<td>Sx(X-&gt;A + (Sw(W-&gt;X + Sb(B-&gt;W)) ))</td>
</tr>
</tbody>
</table>

Table 11: Announcements and signatures in BGPSEC

BGPSEC is still a work in progress and standardisation is not expected before a few more years of work. There are still a few questions such as how to deal with the expiry date of router certificates, interaction between BGPSEC speakers and non-BGPSEC speakers. Another concern is the load on routers that is required to validate signatures.

5.5 Conclusion

RPKI standardisation works have now reached a level of maturity and several RFCs have already been published. All the RIRs have deployed RPKI on a pilot to production basis and some ISPs are following the step by either using RPKI services from their RIR or by deploying their own RPKI engine. Origin validation is now possible and network equipment vendors such as Cisco and Juniper have released RPKI-compatible router operating systems. But on the other hand, BGPSEC is still under discussion and the standards have not been finalised yet.

While we are still in the very early phases of RPKI deployment, there are many impediments that are not helping a fast and wide-scale adoption of this technology. New technologies come with new challenges especially when implementing security frameworks. The next chapter will analyse some of the challenges and barriers to RPKI deployment and adoption.
6  Security challenges and operational issues

RPKI has been under experimentation for a few years now but it has only been deployed as pilot systems by the RIRs in 2011. The RIRs being the focal point of resource allocation for their respective regions have been the driving force for the deployment of this technology. Some large ISPs and NIRS have followed their steps by deploying their own RPKI engines. We currently have around 12 repositories consisting of approximately 2477 resource certificates [88] and more than 5710 ROAs [89].

However, as the stakeholders are gathering more experience in operating RPKI engines, repositories and validator caches, there are many operational issues that are being encountered and need to be addressed. Operating certificate authorities (CAs) and repositories at such large scale is not trivial and is especially complex when coupled with the already complex Internet number resources (INR) management.

We shall see, for example, how key management, which is a normal practice in traditional PKIs can potentially be disruptive in RPKI and can therefore affect network reachability in a fully deployed RPKI scenario. Added to this, there are political issues regarding the management of the root of trust and the subverted use of RPKI to intentionally bring down networks.

This chapter will analyse the different challenges in both the deployment and operation of RPKI from a technological, economical and environmental perspective. Finally, a survey on routing security awareness and RPKI adoption, amongst a few network operators and interdomain routing experts, would enable us to have better view of the challenges and issues pertaining to the deployment of interdomain routing security mechanisms.

6.1  Internet number resources allocations inconsistency

The basis of RPKI is the certification of resources assigned to the different entities in the allocation hierarchy (IANA, RIRs, NIR, ISPs, etc.). Information on the resource certificate should normally give an authoritative view of resource “holderness” and we should consider them as being the “ground truth” besides anything else. But this is not always the case, as flaws exist in the allocation databases across the hierarchy [90].

The databases of the different RIRs sometimes bear some inconsistencies that can affect proper resource certification if not fixed. An example is the existence of overlapping data sets from two different RIRs [91]. This means that there can be potentially two resource certificates with conflicting resources therefore compromising the authority of resource certification.

Moreover, RIRs are currently acting as their own trust anchor. In other words, RPKI has five different trust anchors instead of one authoritative one, which should normally be IANA. The reason behind this design is more political than technical, as we will see in section 6.3. Having multiple roots means that an authority can mistakenly (or intentionally) ascertain ownership of resources it is not entitled for. Resolving such inconsistencies become difficult when it involves certificates and relying parties already in possession of signed objects.

The solution to this issue is the implementation of a single root of trust that would certify the resources of the five RIRs, therefore reducing the possibility of having duplicate or overlapping entries.
6.2 Legacy space

Legacy address spaces are Internet number resources that have been allocated to organisations before the RIRs started operations. Those organisations do not have any contractual agreement with their respective RIR. In the African region for example, 10% of all IPv4 resources managed by AFRINIC is legacy space [92]. Globally speaking, 35% of IPv4 addresses have been allocated to different companies prior to the RIR system are considered as legacy space [93]. Only part of those resources are being used and actually advertised in routing tables. The fact that RIRs do not have any legal binding with the legacy holders makes the game rather difficult. Being totally unrelated, they do not have any obligation to abide by RIRs policies in regards with the management of those resources.

As at now, only a few legacy address blocks have been registered by RIRs. Those legacy spaces can therefore be certified in RPKI. On the other hand, the majority of the legacy space commonly referred as "swamped space" are scattered around the globe. It is today very difficult to accurately determine the usage and utilisation rate of those spaces, especially that a big chunk of legacy space is used in private networks.

Since there is no legal obligation to follow RIR rules and policies, legacy space holders only routinely register or update their assignments in the WHOIS database of the RIRs. The WHOIS database is the only authoritative database of resource ownership information. Consequently, without authoritative and proper registration data, it will be difficult generate consistent resource certificates.

6.3 RPKI Trust model

RPKI has been designed with a single authoritative trust anchor in mind, known as the Global Trust Anchor (GTA). As we have seen earlier, RPKI is based on the existing resource allocation hierarchy with IANA, being responsible for the global management of Internet Number Resources. The latter is therefore the most obvious option as the RPKI “root of trust”.

The Internet Architecture Board (IAB) and the IETF have always been pushing towards a single trust anchor to minimise the risk of having certificates with duplicate or conflicting resources [94]. Such cases would be very difficult to detect and correct without disrupting validation of RPKI signed objects such as ROAs and manifest files down the validation chain.

6.3.1 Centralised control

Although there is consensus in the technical sphere that a single trust anchor is the way to go, it is not currently the case. So far, things have been functioning based on an informal social trust model made of loosely coupled relationships between the different stakeholders. RIRs’ role, in the Internet, has always been to simply guarantee uniqueness of resource allocations. RPKI is now changing the rules of the game.

Routing is currently the prerogative of the networks operators and this is on what the routing business model is built on. The Internet is working because network operators have either business or partnership agreements (for e.g. peering) between themselves. Cash flows in the opposite direction of traffic.

With RPKI those agreements will now be tied to “a chain of adjacent Certificate Authorities and socially compromising a Certificate Authority in the network is as easy as socially compromising an ISP” as claimed by Masataka Ohta, an Internet veteran from
Japan. Indeed, the rules will change as RPKI have now created hard cryptographic links between resource allocation and routing. Certification powers are now concentrated in the hands of a few namely the RIRs, NIRs, the LIRs and IANA as the trust anchor. This automatically implies lot of responsibilities in terms of accountability and regulatory frameworks should be implemented to prevent any form of abuse.

Finally, the question that remains is who actually owns the root of trust? IANA, who is supposed to take over this responsibility, is a United States Department of Commerce contracted agency whose role is to maintain continuity and stability of Internet related services [95]. The U.S. government imposed that the agency should be “wholly U.S. owned”. Other countries are not very comfortable about this idea of giving the “key” of the interdomain routing system to a U.S. contracted agency.

The compromise, in order to launch RPKI was the use of multiple roots, which is deemed as a more politically correct alternative. Each RIR or any RPKI operator can have its own trust anchor. Only recently, RIRs have started discussion with ICANN for the management of the global trust anchor. ICANN is considered to be a better alternative to IANA, though headquartered in the United States, because of its multi-stakeholder’s nature of its decision making process [96] [97].

### 6.3.2 Deliberate manipulations

Similarly as for any other security mechanism, it all depends on the kind of usage we are making out of it. As much as RPKI can be useful in protecting routing announcements, it can also be a harmful tool to bring down networks. The fact that RPKI is based on a hierarchical authority model, the relying party will always be dependent on the signing party (the certificate issuer), who in some cases is the trust anchor.

For example, a big ISP has delegated resources to a small ISP and generated a resource certificate in this regard. Business relationships between the service provider and the customer got bad and for some reason the big ISP decides to remove part of the allocated resources. In RPKI, the corresponding resource certificate of the small ISP is also renewed and if the removed network is still active, it will no more be reachable, as corresponding ROAs cannot be validated anymore. In a recent study, Brogle K. et al., demonstrated how RPKI can be used to make “surgical” manipulations affecting IP reachability of a network [98].

Another issue raised with the advent of RPKI is the problem of censorship. In some jurisdictions, the top most organisations for Internet number resources management are NIRs. NIRs are usually government-mandated agencies to allocate resources to local ISPs of their jurisdiction. The concern is that government can start using RPKI as a censorship tool by revoking or refusing to issue certificates to “unfriendly” network operators.

### 6.4 Technical challenges

RPKI is a novel security framework still in its very early days of deployment and has not been extensively tested. As the technology is being rolled out, operators are encountering different challenges in terms of operations, performance and scalability. As we have seen earlier, RPKI can also be used in a harmful way if diverted from its normal usage or if misconfigured. This section will give us an analysis of the most important issues currently being faced and some recommendations.
6.4.1 Global Trust Anchor (GTA) key management

In PKIs, the trust anchor (TA) needs to be rolled over in either at regular intervals (planned key rollover) or in the event of a key compromise (emergency key rollover). Even though, trust anchor certificates are usually valid for very long period of time (usually more than 10 years), provision should be made to rollover the private keys as a matter of best practice.

For example, new and more secure signature algorithms might become the standard or current key length can be considered as not secure enough. However, this task might not be as easy as it seems due to the scale at which RPKI will be deployed in the future, especially taking into consideration the number of relying parties (RPs) in a fully deployed RPKI.

Planned key rollovers though complex can be achieved in a highly coordinated way. In RPKI, the trust anchor is identified by the Trust Anchor Locator (TAL), which holds the URI of the root certificate and a hash of its public key. RPs need this TAL object to validate RPKI products up to the root. In the case the root is rolled over, a new TAL should be distributed to all RPs. This can be a challenge as there is currently no official record of all relying parties. There should be a mechanism in place to allow RPs to retrieve the new TA without disrupting validation. A staging period with two root certificates will therefore be needed, while we wait that the old TA to phase out.

However, in the event of an emergency rollover, things get quite complicated. There is no mechanism to rapidly broadcast a new TA to all RPs. In a key compromise scenario, the TA must be revoked and replaced by a new one, with a new TAL. By the time, the RPs get the new TAL, validation would not work.

6.4.2 Repository scalability and performance issues

What will be the size of a fully deployed RPKI? This is the research question that Osterweil E. et al. tried to answer in their study on the “Sizing estimates of a fully deployed RPKI” [99]. While the model used to represent the different RPKI objects and operators is perfectible, the study gives a more or less commendable analysis of the scalability and performance of this technology. They argued that in key rollover scenarios (new keys or new algorithms), repositories should store old and new objects during a staging period of about a month. This situation inevitably causes performance issues as the number of objects has suddenly doubled. The result of the study showed that with an estimate of around 600000 objects (without deployment of BGPSEC) and some 2600000 objects with BGPSEC, RPs will take from 15 to 30 days to fully synchronise their local caches.

Another issue detected by early adopters is the problem of cache synchronisation, especially those operating a validator [100]. Validators use the rsync protocol to fetch data from the different RPKI repositories [101]. When the repositories start to have a considerable number of objects, synchronisation delay increases. The consequence is that by the time the resource holder updates all objects in its repository and by the time the validator caches retrieve the new objects, the validator’s cache is “invalid”.

For example, an RP can retrieve a new manifest file, containing new objects currently not in the repository or the new manifest file comes with a different hash of the CRL. Different situations can have different impacts depending on how the RP handles those scenarios, sometimes making validation decisions unclear and difficult to automate.
6.4.3 Dealing with RPKI risks

We have argued before that inconsistencies in Internet numbers registration data can be detrimental to the smooth running of RPKI. Resource certificates form the basis of secure interdomain routing and it is important that accurate information is fed into the routing system. RPKI however, does not have any mechanism to prevent misconfigurations or unintentional mistakes. It is up to the service provider, for instance an ISP, to put the necessary checks to ensure correctness of data in order to prevent IP reachability downtime.

An example of an unintentional mistake is when a resource certificate is expired and is not renewed in a timely manner. Another one could be when a ROA is issued covering only part of a route prefix, meaning that a legitimate routing announcement can be considered as invalid as it is not fully covered by any ROA. So operating RPKI without proper checks and balances can eventually cause routing incidents.

Another concern when dealing with RPKI data is freshness. How can the RP make sure that data it holds at a particular point in time is correct? Objects in its cache could have been revoked at the repository level and without a refresh (which may takes time as we have seen before) the RP would not know that an object is still valid or has been replaced. Note that repository polling and validation of RPKI objects is resource-intensive and is not done in a systematic way.

Finally, RPKI can only be deployed in a piecemeal manner. As adoption progresses, we shall see islands of secure networks on the routing map. The good thing about RPKI is that it has been built on top on the existing BGP protocol; therefore there is a certain assurance of backward compatibility.

As seen earlier, RPKI produces ROAs that are used to create BGP filters. If an upstream provider decides to apply stringent rules to reject all “invalid” BGP announcements, then there is also a risk that RPKI breaks routing. So it all depends on the local policy of the receiving BGP speaker. It is therefore important to plan the deployment of RPKI in a coordinated and staged process. This will help network operators gain experience and deal with invalid object by adjusting their level of “sensitivity”.

6.5 Awareness and adoption survey

6.5.1 Purpose

The different technical and operational challenges we mentioned earlier are the feedback given by a community of early adopters. Some studies on the scalability and performance also helped us to understand the different limitations of the current RPKI framework. However, it was important to get some qualitative data to understand the underlying barriers and critical success factors of this technology - from a user perspective.

A survey was carried out to get some information about routing security awareness and the readiness of the community to adopt RPKI. The survey was carried out mainly amongst African network operators and they were questioned on their knowledge of interdomain routing issues and their awareness of routing security technologies. They were then asked about their plans and apprehensions regarding the deployment of RPKI. The survey was sent out to different mailing lists of network operators and 18 of them responded to the survey.
6.5.2 Results and analysis

6.5.2.1 Respondent profile

18 persons participated in this survey and the majority (72%) were from different ISPs and network operators. Most of them were technical person (67%) and remaining were either managers or businesspersons.

![Profile of participants](image)

6.5.2.2 Awareness of interdomain routing vulnerabilities

Almost 100% of the respondents claimed to be aware of the different interdomain routing vulnerabilities, with 56% to be only “somewhat” aware and 44% “aware”. This means that the respondents are all more or less aware of potential routing breaches, especially for those operating networks as a business.

![Awareness of interdomain routing vulnerabilities](image)

6.5.2.3 Most popular interdomain routing issues

The most popular issue is “BGP misconfiguration” (31%) followed by “Prefix hijacking” (25%). “AS Path manipulation” and “Route leaks” are also well known. Misconfigurations commonly called “fat-finger errors” are quite common and happen on the Internet everyday without us noticing. The survey shows us that networks operators are aware of those issues even if some of them (for e.g. misconfigurations) can be detected and fixed rather easily with the use of BGP filters. Prefix hijacking, also well known, is more difficult to detect, as it is rather difficult to distinguish between a misconfiguration and a real route hijack.

<table>
<thead>
<tr>
<th>Routing issues</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Misconfiguration</td>
<td>31</td>
</tr>
<tr>
<td>Prefix hijacking</td>
<td>25</td>
</tr>
<tr>
<td>Route leaks</td>
<td>22</td>
</tr>
<tr>
<td>AS Path manipulation</td>
<td>20</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
</tr>
</tbody>
</table>
6.5.2.4 Most popular countermeasures

“Session security” (30%) and “Defensive route filtering” (26%) are the most popular, followed by IRRs and RPKI both at 22%. Session security mechanisms are a well known countermeasures to routing insecurity. Defensive routing filtering is also very common amongst ISPs who have transit AS services. Filters are used to control incoming and outgoing traffic, and the same filters are usually extended to add routing security. IRR and RPKI are equally popular.

<table>
<thead>
<tr>
<th>Countermeasures</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session security (TCP MD5, IPSec, BGP TTL Security Hack, etc.)</td>
<td>30</td>
</tr>
<tr>
<td>Defensive filtering of suspicious BGP announcement</td>
<td>26</td>
</tr>
<tr>
<td>Use of Internet Routing Registries (IRRs)</td>
<td>22</td>
</tr>
<tr>
<td>Resource Public Key Infrastructure (RPKI)</td>
<td>22</td>
</tr>
</tbody>
</table>

Figure 20: Awareness of countermeasures

6.5.2.5 Routing incident experience

Out of the 18 respondents, six organisations have already been victim of a routing incident. Most of the participants claimed that routing incidents are taken very to quite seriously in their respective organisation. 29% foresee a reduction in their companies' performance and possible breach of SLA with their customers. 37 % fear a loss of reputation following a routing incident, while 34% are afraid of potential financial loss. However, more than 50% are not bound by any kind of agreements (SLA with customers or contracts with upstream provider) to protect their routing information with proper security mechanisms.

6.5.2.6 Drivers of secured routing services

The drivers for implementing secured routing services are quite clear-cut. The protection of critical services, the preservation of trust and the reduction of operational costs due to routing failures are the main drivers of the deployment of RPKI as interdomain routing security technology.

<table>
<thead>
<tr>
<th>Drivers</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection of critical services</td>
<td>33</td>
</tr>
<tr>
<td>Improved reputation towards business partners and customers (more trust)</td>
<td>33</td>
</tr>
<tr>
<td>Reduction of operational costs (for e.g. less risks of services failures due to routing incidents)</td>
<td>31</td>
</tr>
<tr>
<td>Don’t know</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 13: Drivers for improved routing services

6.5.2.7 Participation in RPKI

Five over 18 (28%) respondents are already participating in RPKI and 12 (67%) are not but would be interested. This means that there is a big majority of network operators aware of the vulnerabilities of interdomain routing and would like to protect their network from being hijacked through the use of RPKI.
6.5.2.8 Hardware compliance to RPKI (RFC 6810 and RFC 6811)

Routers must be able to interpret data coming from validated caches. In other words, routers must implement RFC 6810 and 6811 (RPKI-RTR protocol). The survey shows that 50% of the respondents’ routers are not yet compliant to RPKI. This can be a major hurdle in the deployment of this technology. However, it might only be as simple as updating the router’s firmware to make the devices fully compliant.

6.5.2.9 Intention to deploy RPKI locally

41% have claimed not to be interested in deploying RPKI locally. Only 29% responded to having the plans to deploy and manage their own CA. Managing a CA for resource certification is known to be a rather cumbersome activity. It involves quite a lot of human, technical and capital resources for an activity usually not considered the core business of a network operator.

6.5.2.10 Short-term incentives in deploying RPKI

In terms of short-term incentives, the most popular one is a network operator being keen to get its resources “certified” as a proof of ownership (23%). There is almost an equal percentage of respondent that are wary of prefix hijacking attacks on their networks. Similarly, the same percentage considers RPKI as a protection mechanism against prefix hijacking of customer’s network or RPKI as a value-added services to their customers. Only a few responded by saying that the current security measures are not enough.
<table>
<thead>
<tr>
<th>Short-term incentives</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>I want to get my resources certified as a proof of &quot;holdership&quot;</td>
<td>23</td>
</tr>
<tr>
<td>My organisation is wary of prefix hijacking and its consequences</td>
<td>21</td>
</tr>
<tr>
<td>My customers want their network to be protected from routing hijack/misconfiguration</td>
<td>17</td>
</tr>
<tr>
<td>I can provide RPKI as value-added services to my customers</td>
<td>17</td>
</tr>
<tr>
<td>Current routing security measures are not enough</td>
<td>11</td>
</tr>
<tr>
<td>My upstream provider(s) have deployed RPKI</td>
<td>4</td>
</tr>
<tr>
<td>My peers have deployed RPKI and are signing their announcements</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 14: Short-term incentives

6.5.2.11 Long-term incentives in deploying RPKI

The long-term incentive that was the most selected (35%) was that routers, in the future, would be selecting secure routes instead of insecure routes. This means that unsecure networks are most likely to be less reachable and this can be considered as a loss of revenue, especially for transit ASes. Transit ASes get revenue from allowing data packets to flow through their networks. Second with 24% is that RPKI can be used as a revenue-generating mechanism and would therefore adapt their business model accordingly. This would encourage network operators to adopt RPKI.

The issue of IPv4 address space trading seems to be a concern as well, and the third most selected incentive is that RPKI will be a useful tool against unsolicited commerce of Internet number resources and therefore represents a good incentive for adoption.

Finally, government can play an important role by imposing RPKI as a mandatory security measure to protect national networks from being hijacked. Such actions potentially represent a strong incentive for RPKI adoption.

<table>
<thead>
<tr>
<th>Long-term incentives</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routers will prefer to choose secure routes as opposed to non secure routes</td>
<td>35</td>
</tr>
<tr>
<td>Operators will develop a new business model based on routing security</td>
<td>24</td>
</tr>
<tr>
<td>IPv4 is getting depleted, RPKI might help to prevent unauthorised address space trading</td>
<td>22</td>
</tr>
<tr>
<td>Government will impose the adoption routing security mechanisms on network operators</td>
<td>16</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 15: Long-term incentives

6.5.2.12 Barriers to RPKI adoption

Regarding the obstacles to RPKI adoption, the first one to come out is lack of training and awareness (20%). RIRs as early adopters should push for more training and routing awareness programmes in their respective regions. Awareness of the dangers and consequences of routing incidents will incite network operators to invest into security measures. Another potential barrier, even if RPKI is considered an important security tool, is the lack of rapid return on investment (RoI). Network operators have a business model and needs to justify the need for heavy investments, especially if they want to host their own resource certification system.

Only a few think that the technology is not mature and robust enough. The perception of routing being disrupted in case of a key compromise is not considered as an undermining factor.
Table 16: Barriers in RPKI adoption

<table>
<thead>
<tr>
<th>Long-term incentives</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of training and awareness</td>
<td>20</td>
</tr>
<tr>
<td>No immediate return on investment/financial benefit</td>
<td>14</td>
</tr>
<tr>
<td>Technology is not mature enough</td>
<td>13</td>
</tr>
<tr>
<td>In case of key compromise, the whole routing system can be disrupted</td>
<td>10</td>
</tr>
<tr>
<td>Managing a Certificate Authority is not the core business of an operator</td>
<td>10</td>
</tr>
<tr>
<td>RPKI can have major performance impact on BGP operations</td>
<td>7</td>
</tr>
<tr>
<td>In the future, traffic flowing through secure routes might cost more than traffic through non-secure routes</td>
<td>7</td>
</tr>
<tr>
<td>High initial setup cost (infrastructure and human resources)</td>
<td>6</td>
</tr>
<tr>
<td>Possibility of using RPKI as the censorship tool by governments</td>
<td>6</td>
</tr>
<tr>
<td>No trust in ICANN/IANA as RPKI root (Trust Anchor)</td>
<td>3</td>
</tr>
<tr>
<td>Current routing security measures are more than enough</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>4</td>
</tr>
</tbody>
</table>

6.5.2.13 Readiness to invest in RPKI

Most of the respondents are keen to invest in their human capital regarding RPKI training, customer outreach and capacity building. On the other hand, 67% are not willing to invest in the purchase of equipment (servers, Hardware security modules, etc.). This is surely because of the high cost of maintaining a CA and the operational risks associated to it. More than 50% are willing to upgrade their current equipment to support prefix validation through RPKI.

<table>
<thead>
<tr>
<th>Investment</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training of human resources</td>
<td>72</td>
<td>28</td>
</tr>
<tr>
<td>Purchase of equipment (Servers, HSM, etc.)</td>
<td>33</td>
<td>67</td>
</tr>
<tr>
<td>Customer outreach and training</td>
<td>61</td>
<td>39</td>
</tr>
<tr>
<td>Monitoring</td>
<td>78</td>
<td>22</td>
</tr>
<tr>
<td>Equipment upgrade to support RPKI</td>
<td>56</td>
<td>44</td>
</tr>
</tbody>
</table>

Table 17: Readiness to invest in RPKI

6.5.3 Conclusion and observation

The results show that most network operators are aware of the different vulnerabilities of the current interdomain routing system. Some of them have experienced a routing incident before and are quite sensible about the consequences. Routing security is taken quite seriously in different organisations and this may impact revenue and the trust relationship with their customers.

The most popular issue is a BGP misconfiguration, which is quite frequent and easily detected but other issues such as prefix hijacking, AS Path manipulation and route leaks are equally well known. In terms of solutions, session security and defensive filtering came out to be the most popular and are also the most used ones. RPKI, though very recent, has started to slowly gain ground and has become as popular as an older
alternative to secure the interdomain routing system – the Internet Routing Registries (IRRs).

It came out that hardware/software compliance of routers to RPKI might be an issue and can hamper rapid deployment of RPKI. However, there is an indication that operators would be willing to upgrade routing equipment in the event of RPKI deployment within their organisation. The results were quite obvious on the intention of operators to deploy their own CA. Many advocated that it is not the core of their business and investing in a CA will cause a huge cash flow without immediate return on investment (RoI). A barrier to wide-scale deployment is also the problem of training and awareness. RPKI being quite a complex system, networks operators need to be trained adequately because misconfigurations in RPKI can also lead to network reachability outages.

RPKI however, in the long run can be envisaged to become a revenue-generating activity for network operators and other resource holders. The fact that in the future, security-aware routers will probably choose secure routes instead of non-secure routes represents an incentive for unsecure networks to deploy RPKI. Besides securing their networks, resource holders have understood the importance to have their resource certified as a proof of ownership. This can come handy especially when illegal trading on IP address space is becoming more and more common with the depletion of IPv4 addresses.

6.6 Chapter conclusion

This chapter presented the main challenges and some of the critical success factors of the adoption of RPKI. We have seen how manipulations in RPKI, which is itself a robust and cryptographically strong system, can also be harmful to interdomain routing. Misconfigurations in RPKI are bound to happen, as the system itself has not been conceived to detect and correct its own mistakes. Some routes can be considered as invalid because a certificate has not been renewed or a ROA has been misconfigured.

There are still a few technical issues to be sorted out especially regarding the global consistency of the Internet number resources database and the management of the legacy address space. Furthermore, the issue of the “root of trust” is quite a spiny one as it involves political agreements at the Internet governance level, usually where a compromise between different stakeholders is sometimes difficult to reach.

Scalability of RPKI can only be measured as and when new systems are deployed. Some studies have showed some dire figures regarding the expansion of RPKI and its stability but those studies are quite questionable since emulating a fully deployed RPKI is almost impossible.

Finally, the survey on routing security awareness and RPKI adoption carried out helped us to confirm some of the issues pertaining to the wide-scale deployment of RPKI. It also helped us understand the underlying business incentives and barriers that influence users to consider RPKI as a viable and cost-effective solution to protect their networks from routing incidents.
7 Conclusion

This paper presents an in-depth analysis of the motivation and challenges of deploying RPKI to protect the interdomain routing system. We have seen at what point the current Border Gateway Protocol (BGP), which is at the centre of the Internet, is vulnerable to a number of different types of attacks and weaknesses. It is today widely acknowledged that having a robust interdomain routing infrastructure is important for the scalability of the Internet. BGP has been designed without taking into consideration potential security loopholes and it is today suffering from two main ills, which are false origination of prefixes and AS path manipulations. We have seen how both vulnerabilities can have important consequences such as denial-of-service or packets eavesdropping. Some of the notorious routing incidents, such as the YouTube outage and the China Telecom interception attack, have set off the alarm bells of policy makers especially in a time where cyber espionage and sabotage are not uncommon.

After more than two decades of unsuccessful trials and experimentation, protocol designers have converged on a common solution space with the deployment of a PKI to enable resource certification. The ability of certifying Internet number resources has proved to be a key element of interdomain routing security. We have seen that with RPKI, resource holders can now create Route Origin Authorization (ROAs) to allow specific AS to originate their networks, therefore bringing a remedy to the problem of origin validation. As for path validation, the RPKI framework proposes to use router certificates to sign AS path attributes therefore allowing relying parties to detect false AS paths.

As RPKI is in process of being deployed globally, it was important to understand the underlying challenges pertaining to its acceptance and adoption within the technical community. Based on existing research, an analysis was made on the most well known issues currently being faced by early adopters, such as the RIRs. We found out that the challenges with not only technical or operational but also political. We saw that data consistency of Internet number resources is a major impediment and can slow down the adoption rate as long as they are not fixed. Another major issue is the problem of the legacy space holders on which RIRs do not have any authority upon. Convincing them to join the “RPKI club” is considered as a major hurdle.

On a more political note, some studies showed that people are scared of the “bad intentions” behind the motivation of RPKI. It is not to be forgotten that interdomain security main pusher is the Department of Homeland Security of the U.S. The “root of trust” will eventually be hosted by U.S. incorporated organisations (IANA or ICANN) and this subject has for a long time been in a political turmoil. Furthermore, people are wary about governments using RPKI as a censorship tools to bring down networks. We have all witnessed the role the Internet has played in the Arab Spring in 2011.

Besides the existing studies in literature, it was important to get a grasp of some qualitative information about the perception of routing security and RPKI. To this end, an online survey was carried out amongst some networks operators and interdomain routing experts. The aim of the survey was to see how aware network operators are about interdomain routing vulnerabilities and what do they really think about RPKI as a solution to those problems. A sample of 18 participants, coming from different backgrounds, was taken mainly in the African region. Unfortunately, a bigger sample would have been more representative of current state of the interdomain routing as we can assume there is same amount of networks as there are advertised ASes i.e. ~ 40 000 on the Internet.
It came out that networks operators are very well informed about interdomain routing security issues. Many of them have also been victim of routing security breaches and that affected their operations and the most common issues are BGP misconfiguration and prefix hijacking. The survey showed that service providers are very careful about their reputation and are willing to deploy routing security mechanisms to prevent any new routing incidents. The most common forms of countermeasures are session security and defensive BGP filtering even though RPKI has put up on popularity. However, the results also showed that there is a huge gap in training and awareness regarding the operations and deployment of RPKI. Another major barrier is backward compatibility with current routing equipment since not all routers on the Internet are RPKI compliant. However, it would have been interesting to make a more in-depth research about equipment compliance and its direct correlation to RPKI adoption rate. Scalability and robustness of RPKI was another concern that was raised by respondents. Indeed, some studies have shown that there might be performance issues in a fully deployed RPKI scenario.

The survey indirectly demonstrated that there is a certain level of resistance against change. Some people advocated that IRRs are more stable and robust than RPKI and can do the same job. We have seen that IRRs are only used by a handful of operators and therefore cannot be considered as a global solution especially that IRRs themselves are known to have issues with consistency of data and are devoid of security mechanisms. Moreover, the resistance against change can also be due to the high cost involved in upgrading the network equipment but also to operate a CA in the event, the network operators chooses to host its own RPKI engine. The good news though is that RIRs today are offering hosted RPKI engines where downstream resource holders can operate RPKI without the need to invest in expensive hardware security equipment. The survey clearly demonstrated that the delegation of CA activities to a “trusted” organisation, such as an RIR, represents a very important incentive for deployment. Many respondents advocated that running a CA is not the core business of a network operator. However, there are some trade-offs to consider in this configuration, for example, the delegation of the management of the resource holder’s private key.

This thesis only gave a qualitative perspective to the different aspects of routing security and RPKI. In the long-run more focus should be made on the quantitative aspects of deployment such as studying the impact of deployment of RPKI at the Tier 1 and Tier 2 levels. RPKI today, should not be considered as the miracle solution to interdomain routing security problems. There are still many other problems that need to be tackled, two examples being route leaks and AS hijacking attacks. More research questions need to be raised such as the performance impact on the Internet with partial deployment of RPKI.

To summarise, the main challenges are a lack of training and awareness coupled with high implementation and operational cost in the case of hosted CAs. Added to this, there is the problem of data consistency and legacy address spaces. Perception about the stability and robustness of RPKI is still an issue and more studies should be carried out on this subject matter. We should see in the future more investment into research that would ensure a certain level of quality-of-service (QoS). The problem of trust in the RPKI hierarchy can only be mitigated through more dialogue and consensus especially on how the “root of trust” is governed. Finally, as much as obstacles to RPKI adoption are finance related, the survey clearly indicated that in the future, a new business model around RPKI would be a critical success factor. Indeed, the possibility that non-secured routes would be less preferred than secured routes would represent a potential loss of revenues for transit providers.
8 Bibliography


[16] K. Hawkinson and T. Bates, "Guidelines for Creation, Selection and Registration of


http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7262071.stm

[38] J. Qiu, L. Gao, S. Ranjan, and A. Nucci, "Detecting Bogus BGP Route
Information: Going Beyond Prefix Hijacking," in SecureComm 2007, Nice, France,
September 2007.

http://www.merit.edu/mail.archives/nanog/1997-04/msg00340.html

[39] S. Halabi and D. McPherson, Internet Routing Architectures, 2nd ed.: CISCO PRESS,
2000.


http://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/

[42] P. Brookes, R. Cleveland, J. Fiedler, P. Mulloy, W. Reinsch, D. Shea, P. Videnieks,
Economic and Security Review Commission. [Online].
http://origin.www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-
Congress.pdf


A Case Study of the China Telecom Incident," in Passive and Active Measurement
Conference, Hong Kong, 2013.

[45] S. Bellovin, "Using link cuts to attack Internet Routing," in USENIX Security '03,


5925, June 2010.

Mechanism (GTSM)," RFC 5082, October 2007.


http://www.team-cymru.org/Services/Bogons/http.html


# Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>Autonomous System</td>
</tr>
<tr>
<td>ASN</td>
<td>Autonomous System Number</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BGPSEC</td>
<td>Border Gateway Protocol Security</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>EE</td>
<td>End-Entity</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>GTA</td>
<td>Global Trust Anchor</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Number Authority</td>
</tr>
<tr>
<td>IBGP</td>
<td>Interior Border Gateway Protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>INR</td>
<td>Internet Number Resources</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>IRR</td>
<td>Internet Routing Registry</td>
</tr>
<tr>
<td>IRV</td>
<td>Interdomain Routing Validation</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>LIR</td>
<td>Local Internet Registry</td>
</tr>
<tr>
<td>NIR</td>
<td>National Internet Registry</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PKIX</td>
<td>Public Key Infrastructure (X.509)</td>
</tr>
<tr>
<td>psBGP</td>
<td>Pretty Secure Border Gateway Protocol</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>RIB</td>
<td>Routing Information Base</td>
</tr>
<tr>
<td>RIR</td>
<td>Regional Internet Registry</td>
</tr>
<tr>
<td>ROA</td>
<td>Route Origin Authorization</td>
</tr>
<tr>
<td>RoI</td>
<td>Return on investment</td>
</tr>
<tr>
<td>Abbr</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>RP</td>
<td>Relying Party</td>
</tr>
<tr>
<td>RPKI</td>
<td>Resource Public Key Infrastructure</td>
</tr>
<tr>
<td>S-BGP</td>
<td>Secure Border Gateway Protocol</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>soBGP</td>
<td>Secure Origin Border Gateway Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TA</td>
<td>Trust Anchor</td>
</tr>
<tr>
<td>TAL</td>
<td>Trust Anchor Locator</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TTL</td>
<td>Time to Live</td>
</tr>
</tbody>
</table>
Annex A – RPKI objects

Resource Certificate

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 10 (0xa)
Signature Algorithm: sha256WithRSAEncryption
Issuer: CN=AfriNIC-Root-Certificate
Validity
Not Before: Dec 15 13:07:58 2011 GMT
Not After : Dec 13 13:07:58 2016 GMT
Subject: CN=AfriNIC-Root-Certificate
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (2048 bit)
    Modulus:
      00:c6:c0:2a:02:15:88:3b:e3:8d:d8:47:fd:a1:10:
      19:51
  Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Certificate Policies: critical
  Policy: 1.3.6.1.5.5.7.14.2
  X509v3 Basic Constraints: critical
    CA:TRUE
  X509v3 Key Usage: critical
    Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
Subject Information Access:
  CAREpository -
    URI:rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657DB931367AE7D/
    1.3.6.1.5.5.7.48.10 -
    URI:rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657DB931367AE7D/62gPOpWmxx
    uDsaQa4vQYUBkAM0Y.mft
  sbgp=autonomousSysNum: critical
    Autonomous System Numbers:
      1228-1232
      36864-37887
      327680-328703
  sbgp-ipAddrBlock: critical
    IPv4:
      41.0.0.0/8
      102.0.0.0/8
      105.0.0.0/8
      154.0.0.0/8
      196.0.0.0/7
    IPv6:
      2001:4200::/23
      2002::/12
Signature Algorithm: sha256WithRSAEncryption
34:8f:3f:1f:ce11:69:35:a:7fa:0:3c:97:e0:6f:16f:3e:6e:19:
7c:9e:e7:ff:ff:ff:ff:02:43:60:12:37:8ff:bf:de:52:45:39:
c9:eb:8e:14
```
Trust Anchor Locator (TAL)

rsync://rpki.dev.mu.afrinic.net/repository/AfriNIC.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxsAxhWIO+ON3f9dKpXxv+AfmSLrWtjrvLyUaXbPb3r+KvR0HUEwT auuypF0P9tu5SH2C1rUaVvTH
vve6xNF5U30XTCgEzXMZy+ctX0bde2SMMDvdb0Z2+TH9gNKhHc197UV0u1q4LeJH
k3X0f5u3s346YrGAOSv6/AaBXYQXXxa0e9z3vqF6mz0pReQhe/W13qfFKXgZpfzFQL
6Y7FDPDysYdAvoXPPXSXt74f46KLA/28m/BL/b0w/Lf2FvIAGhDrjqqqq=+/9w1kEl
L/vqyIVnV18aaKtXnltKtT/A/BfS1lYw2K7qV573XyuyqCkno/iyLYR1DToB2EZ
UQIDAQAB

Route Origin Authorization (ROA)

version: 0
as_id: 37301
prefixes: 196.192.124.0/32-32
signing certificate:
serial: 15 (0xF)
not before: 2013-07-30T09:43:31
not after: 2013-03-31T00:00:00
subject: CN=51f78ac4-4b6c
ski: 3d17ce511333e8e82e2f1d4288a8452c8592d
serial: FRSXHHez_v6O6uf9PbJrFLHNS0
issuer: rsync://rpki.dev.mu.afrinic.net/repository/F3634D22/BEB50730F06B11E29652F36
9616D64AA/7CD6F6AEF8FC11E2BAB19D9D3616D64AA.ros

resources:
ipv4: 196.192.124.0---BEGIN CERTIFICATE-----

MIIFGCChCASdApIgDzANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxsAwQFz6uQXJ3RjYMX0YU4Q/6M/1O+uA93dO conditioned on: 2013-07-30T09:43:31
subject: CN=51f78ac4-4b6c
ski: 3d17ce511333e8e82e2f1d4288a8452c8592d
serial: 15 (0xF)

---END CERTIFICATE-----
Certificate Revocation List (CRL):

Certificate Revocation List (CRL):
Version 2 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer:
/CN=AFRINICTESTPROD/serialNumber=374E802284C331BCF6A6282BFDDDB798F2B37479
Last Update: Aug 25 03:00:15 2013 GMT
Next Update: Aug 27 03:00:15 2013 GMT
CRL extensions:
  X509v3 Authority Key Identifier:
X509v3 CRL Number: 325
Revoked Certificates:
Serial Number: 67
  Revocation Date: Jul 31 03:00:11 2013 GMT
Serial Number: 70
  Revocation Date: Jul 31 03:00:10 2013 GMT
Serial Number: 79
  Revocation Date: Jul 28 12:21:29 2013 GMT
Serial Number: 7C
  Revocation Date: Jul 28 12:23:35 2013 GMT
Serial Number: 7F
  Revocation Date: Aug 1 13:16:11 2013 GMT
Serial Number: 81
  Revocation Date: Aug 1 03:00:10 2013 GMT
Serial Number: 8D
  Revocation Date: Jul 31 12:04:50 2013 GMT
Serial Number: 8F
  Revocation Date: Jul 31 12:40:07 2013 GMT
Serial Number: 92
  Revocation Date: Jul 31 12:40:07 2013 GMT
Serial Number: 94
  Revocation Date: Jul 31 12:40:06 2013 GMT
Serial Number: 9A
  Revocation Date: Aug 23 00:59:56 2013 GMT
Serial Number: 9C
  Revocation Date: Aug 1 13:16:11 2013 GMT
Serial Number: 9F
  Revocation Date: Aug 1 13:16:23 2013 GMT
Serial Number: A4
  Revocation Date: Aug 1 13:26:54 2013 GMT
Serial Number: A7
  Revocation Date: Aug 1 13:26:55 2013 GMT
Serial Number: D8
  Revocation Date: Aug 23 03:00:19 2013 GMT
Serial Number: D9
  Revocation Date: Aug 24 03:00:14 2013 GMT
Serial Number: DA
  Revocation Date: Aug 25 03:00:14 2013 GMT
Signature Algorithm: sha256WithRSAEncryption
Annex B – RPKI Adoption Survey

This is an informal survey about routing security awareness and RPKI adoption. This survey is being carried out as part of an Msc thesis in Information Security on the topic of "Security Challenges and Operational Issues of RPKI".

The idea is to assess the impact of deploying routing security technologies, namely RPKI, amongst African network operators. This work can be used as a premise for more in-depth research about routing security in Africa.

Your input would be much appreciated as a selected group of target network operators and interdomain routing experts from various organisations and companies over Africa.

1. What is your responsibility within your organisation? *
   - Policy/Managerial level
   - Business/operational level
   - Technical/Infrastructure level
   - Other:

2. Are you aware of the different vulnerabilities of inter-domain routing? *
   - Yes
   - No
   - Somewhat

3. Which of the following issues have you heard about? *
   - Prefix hijacking
   - BGP Misconfiguration
   - AS Path manipulation
   - Route leaks
   - Other:

4. Which of the available security countermeasures are you aware of? *
   - Session security (TCP MD5, IPSec, BGP TTL Security Hack, etc.)
   - Defensive filtering of suspicious BGP announcement
   - Use of Internet Routing Registries (IRR)
   - Resource Public Key Infrastructure (RPKI)
   - Other:

5. Has your organisation ever been victim of a routing incident? *
   - Yes
   - No
   - I don't know

6. How would you rate the severity of the incident? *
   - Very serious causing disruption in service availability
Minor disruptions, got fixed easily
No disruption at all
Irrelevant

7. How important is it for your organisation to deploy security measures against routing incidents? *
   Very important, top priority
   Quite important
   Not important
   I don’t know

8. What critical risks do you foresee for your organisation in case of breach of routing security? *
   Reduced performance and SLA breach
   Loss of reputation
   Financial loss
   None
   Other:

9. Are you bound to protect your routing information by? *
   Customers (SLA, contracts, etc.)
   Upstream or transit providers
   Peers
   None
   Other:

10. What would you think would be drivers for improved routing services? *
    Protection of critical services
    Reduction of operational costs (for e.g. less risks of services failures due to routing incidents)
    Improved reputation towards business partners and customers (more trust)
    Don’t know
    Other:

11. RPKI is currently being deployed wide-scale and RIRs are already offering production grade services. Are you already participating in RPKI? *
    Yes
    No, but I would like to
    No, I am not interested

12. Are your current BGP routers RPKI compliant (RFC 6810 and RFC 6811)? *
    Yes
13. If you are an LIR and you are allocating resources to customers, do you intend to deploy your own RPKI CA engine?
   - No
   - Yes
   - No
   - I don't know

14. What in your opinion would be the short-term incentives for you to deploy RPKI? *
   - My organisation is wary of prefix hijacking and its consequences.
   - My customers want their network to be protected from routing hijack/misconfiguration
   - My upstream provider(s) have deployed RPKI
   - My peers have deployed RPKI and are signing their announcements
   - I want to get my resources certified as a proof of "holdership"
   - I can provide RPKI as value-added services to my customers
   - Current routing security measures are not enough
   - Other:

15. What in your opinion would be the long-term incentives for RPKI adoption? *
   - Routers will prefer to choose secure routes as opposed to non secure routes
   - Operators will develop a new business model based on routing security
   - Government will impose the adoption routing security mechanisms on network operators
   - IPv4 is getting depleted, RPKI might help to prevent unauthorised address space trading
   - Other:

16. What in your opinion are the barriers for RPKI adoption? *
   - Technology is not mature enough
   - Lack of training and awareness
   - Managing a Certificate Authority is not the core business of an operator
   - No immediate return on investment/financial benefit
   - High initial setup cost (infrastructure and human resources)
   - RPKI can have major performance impact on BGP operations
   - In case of key compromise, the whole routing system can be disrupted
   - No trust in ICANN/IANA as RPKI root (Trust Anchor)
   - Possibility of using RPKI as the censorship tool by governments
- In the future, traffic flowing through secure routes might cost more than traffic through non-secure routes
- Current routing security measures are more than enough
- Other:

17. RPKI requires a non-trivial amount of resources (human, capital and technical), in case your organisation what to become a Certificate Authority. Is your organisation ready to invest a considerable amount of resources in *

<table>
<thead>
<tr>
<th>Investment</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training of human resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase of equipment (Servers, HSM, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer outreach and training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment upgrade</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

18. Is there any other point you would like to raise regarding routing security and RPKI adoption in general?

19. Organisation name (Not mandatory)

20. Organisation type *
   - ISP or Network Operator
   - Content Provider
   - Data carrier services provider
   - Network equipment supplier
   - Public body
   - Academic/Research
   - Regulator
   - CERT organisation
   - Other:

21. Where are you activities based?