INTERNET ROUTING SECURITY: AN APPROACH TO DETECT AND TO REACT TO INCORRECT ADVERTISEMENTS

Ines Feki, Xiaoli Zheng, Mohammed Achemlal
France Telecom R&D, 42 rue des coutures, Caen, France

Ahmed Serhrouchni
Telecom Paris, 46 rue Barrault 75013 Paris, France

Keywords: Internet routing, Security, BGP.

Abstract: Internet is composed of thousands of autonomous systems (AS). The Border Gateway Protocol (BGP) is the exterior routing protocol used to exchange network reachability information between border routers of each AS. The correctness of the exchanged information in BGP messages is crucial to the Internet routing system. Unfortunately, BGP is vulnerable to different attacks that have considerable impacts on routing system. Network prefix hijacking, where an AS illegitimately originates a prefix is one of the most important attacks. It allows the attacker to receive traffic in destination to the prefix owner. The attacker is then able to blackhole the traffic or to force it to take another path. Proposed solutions rely on public key infrastructures and cryptographic mechanisms to prevent incorrect routing information propagation. In practice these approaches involve many parties (Internet Service Providers, Operators, Vendors, and Regional Internet Registries) and are difficult to deploy. In this paper we formally define routing information correctness, especially the legitimacy of an AS to originate a prefix. We also propose a method to associate with an AS a legitimacy level to originate a prefix. We use Regional Internet Registry databases to initialize the legitimacy level. We also use received announcements and public routing data to update this legitimacy level. We finally describe all conceivable reactions facing origin AS changes.

1 INTRODUCTION

Internet is composed of a set of interconnected autonomous systems (AS). Each autonomous system is a collection of IP networks administrated by a single authority. An ISP may have several autonomous systems. An interior gateway protocol is used to route IP packets locally and to apply one local routing policy. When exterior network prefixes should be reached, border routers use routing information received from a neighboring AS's border router. The Border Gateway Protocol (BGP) (Rekhter, Y, 2006) is used to exchange this dynamic reachability information between ASes's border routers which will be used to forward IP packets.

When a BGP session is initiated between two neighboring routers, they exchange the content of their routing table. Then, when events happen leading to a change in reachability information (session shutdown, restart, routing policy change, etc...) BGP Updates are sent between routers to keep each neighbor informed about the new reachability information. BGP is a path vector routing protocol; updates contain a path composed of a sequence or a set of ASes. This AS path should be used to reach the announced network prefixes. A BGP router does not have a global view of the topology; it only knows the neighbor capable of reaching a destination. When the reachability changes it just sends updates to its neighbors which forward them to their neighbors and so on.

BGP allows the application of policies used for different reasons (traffic engineering, load balancing, etc...). Business relationships play an important role in defining these policies. It is possible, for example, for an organization to deny its traffic to traverse a competitor and to prefer another path, even longer. The agreements between ASes dictate routing policies. Moreover, providers often compete with one another for customers but must

Feki I., Zheng X., Achemlal M. and Serhrouchni A. (2006).
INTERNET ROUTING SECURITY: AN APPROACH TO DETECT AND TO REACT TO INCORRECT ADVERTISEMENTS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 110-117
DOI: 10.5220/0002104201100117
Copyright © SciTePress

nonetheless cooperate to offer global connectivity to hundreds of millions of hosts. Routing policies are used to select which routes are advertised to which neighbors and which paths are used to send packets to any given destination.

The way routing information is exchanged and the content of routing information are crucial for Internet connectivity, reliability, and robustness. If this network prefix reachability information is incorrect, traffic may not reach its destination, networks may be isolated, and traffic may be subverted to unintended networks. There are many reasons why this information may be incorrect. First, BGP has vulnerabilities; its messages are subject to modification, deletion, forgery, and replay. At the beginning of Internet, there were few interconnected ASes and there was an implicit trust relationship, nowadays their number is increasing considerably (approximately 30 per week (Huston, 2006)). Even if the peering agreements between two ASes helps to build a trust relationship, the hop by hop routing paradigm and the ability of each hop to modify BGP messages decreases the trust relationship. Information traverses unknown ASes and is subject to modification or deletion maliciously or due to misconfigurations.

The remainder of this paper is structured as follows. Section 2 reviews the related work. Section 3 formally defines identified requirements. In section 4 we introduce the background materials and we describe the methodology that we used to identify incorrect announcements, we discuss this proposal. We conclude in section 5.

2 RELATED WORK

Several efforts have been made to solve internet routing security problems. They vary from the utilization of cryptographic methods, the utilization of the forwarding plane to validate announcements, to anomaly detection based on routes monitoring.

Different solutions are based on cryptographic methods aiming to avoid and to prevent incorrect information propagation. One of these approaches is Secure BGP (Kent, 2000). Its goal is to assure the integrity of BGP messages, the authorization of a router to originate and to announce a route. IPSec is used to provide messages integrity and peer authentication. A public key infrastructure is used to support the authentication of the ownership of address blocks and autonomous system identities, the given BGP router's identity and its right to represent the AS it claims. Certificates are issued as address blocks and autonomous systems numbers are allocated by Regional Internet Registries (RIR). Another public key infrastructure is used to express the authorization of a router to send an announcement to another router. The main disadvantage of SBGP is to add complexity and increase the convergence time. In addition, the strict hierarchal public key infrastructures (PKIs) make it difficult to deploy over Internet (Atkinson, 2004). Zhao et al (Zhao, 2004)(Zhao, 2005) addressed these drawbacks and proposed some enhancements. They used different cryptographic methods in order to make it less complex and to minimize the added convergence time. In addition, SBGP does not address issues such as detecting policy violations or incorrect propagation of route announcements or withdrawals. Secure Origin BGP (White, 2003) is a second solution using cryptographic methods. It uses a PKI to authenticate the AS; RIRs are not involved as Certificate Authorities (CA) for their authentication. ASes issue certificates to authorize other ASes to announce their prefixes. So, SoBGP is based on the idea that ASes publish their policies which may be considered as a drawback since some ASes consider them confidential. Pretty Secure BGP (Wan, 2005) uses both centralized and distributed trust models used in SBGP and SoBGP. The first model is used for AS number authentication and the latter is used for IP prefix ownership and origination verification. The three solutions described above were presented in IETF Routing Protocols Security Working Group but there was no consensus on those solutions (RPSEC). A new IETF working group that will focus on Interdomain routing security (SIDR) is currently under proposal.

Besides cryptographic solutions, other works focused on the MOAS conflicts. Wu et al worked on BGP anomalies and MOAS visualization tools (Teoh, 2003)(Teoh, 2004). Anomaly visualization is not efficient enough againt anomalies, it would be more efficient to have a mechanism that detects and reacts to anomalies as the routing system is running or even a mechanism that prevent those attacks. Zhao et al proposed to create a list of multiple ASes who are entitled to originate a prefix and attach it to BGP community attribute in announcements (Zhao, 2002). In order to validate received paths, Kim et al proposed to use forwarding plane information and used ICMP traceback messages (Kim, 2005). The disadvantage of this approach is related to ICMP filtering practices currently used. Moreover there can be legitimate differences between BGP AS paths and paths derived from forwarding plane (Huyn, 2003).

Another solution that validates announcements is Interdomain Route Validation (IRV) (Goodell, 2003). It introduces a new protocol and a framework to validate routing information announced between ASes. IRV allows ASes to acquire and validate static (policies) and dynamic (advertisements) interdomain routing. The approach is based on an interdomain routing validator which resides in each participant AS. This validator receives requests from the other elements placed in the other ASes. These latter elements send a request in order to validate the routes they have just received or consider them as malicious or abnormal. The reasons that trigger the requests are not mentioned. It is left to the AS to choose its algorithm. This can be considered as an advantage and a drawback also since it gives flexibility to the AS but if the validation process is not frequent benefits will be reduced.

3 REQUIREMENTS DEFINITION

In this paragraph, we address all the requirements for a resilient and robust interdomain routing system. Internet resources can be seen in global routing system only if they have been delegated by IANA to RIRs then allocated to ISPs by RIRs and assigned to end users. So, one of the global requirements is that private and non delegated resources should not be present in global routing. It is possible to ensure this if all ASes filter received and sent announcements using prefix lists that filters private and unallocated prefixes, and filter lists that filter AS numbers. The challenge consists in updating filters as ASNs and prefixes are allocated. This type of information is distributed via emails and there is no automatic and "on line" way that permit all ISPs to update their filters.

If we take a look at the requirements of an AS, the basic need is to be sure that its inbound and outbound connectivity is assured. That means that a stub AS needs to be sure that its prefixes are announced correctly by their providers and that they will let it reach all networks sought. Furthermore, if this AS is multihomed and uses BGP to apply some traffic engineering rules and policies, it needs to be sure that its policies are applied. In the same way, a transit AS needs to be sure that not only its prefixes but also those of its customers are correctly announced and that the traffic in their destination won't be subverted, redirected or blackholed. They also need to be sure that their sent traffic reaches its intended destination. So, if an AS needs to verify all these requirements before accepting any announcement, its border routers need to check its content and verify:

- Internet resources validity (public and allocated ASN and prefixes)
- Origin AS legitimacy to originate the prefix
- Policy conformance of the path

We address every requirement and some operational requirements below. First, let us define all the elements involved in the routing system. Paths and routes are defined in a graph where nodes correspond to ASes and links correspond to their interconnections. Nodes are directly connected and exchange reachability information using BGP. A path is a sequence or a set of interconnected nodes. A route is a unit of information that pairs a set of destinations with attributes (local preference, path length, etc...) of a path to those destinations. It is used by ASes on the graph to select paths to destinations. The destination refers to a single node or a group of nodes identified by an IP prefix.

Let AASN the allocated set of AS numbers. Let O be the set of all organizations that use BGP. Let RIR be the set of Regional Internet Registries. For each organization $C \in O$ let ASN(C) be the set of ASN that have been assigned to it from IANA or any registry. Note that $\forall C \in O$, $ASN(C) \in AASN$. IANA delegates IP prefixes to RIRs. We note this relation $IANA \xrightarrow{P} R$ where $R \in$ RIR. At the beginning of the Internet deployment, a classful address architecture was used. The address architecture has evolved and changes to a classless architecture. During the first period resources were allocated using classes and were provided to organizations with minimum requirements. Some organizations have maintained these allocations. Let OIP(IANA) be the set of these early allocations. RIRs allocate prefixes to Internet Service Providers (ISP) or Local Internet Registries (LIR). We note this relation: $R \xrightarrow{P} C$.

The latter sub-allocates them to other ISPs or assigns them to end users. We note this relation: $C / \xrightarrow{P} C'$. Let IP(IANA) be the set of IP addresses that IANA already delegated to RIRs or assigned to ISPs. Let IP(R) be the set of IP addresses that a Registry $R \in$ RIR allocated. Note that $IP(R) \subset IP(IANA)$. Let us note the providers of an organization C as Providers(C). RIRs allocate also IP prefixes to exchange points. Let IP(IX) be the set of prefixes allocated to an exchange point IX. Let ASN(IX) be the set of ASes that participate in this exchange points.

3.1 Resources Validity

A prefix or an ASN is considered valid if it has been delegated by IANA to a RIR and allocated by the RIR to an organization. This defines the following rule:

P is valid if $P \in \bigcup_{R \in RIR} IP(R)$

ASN is valid if ASN ∈ AASN.

3.2 Origin AS Legitimacy

Origin legitimacy is the ability of an AS to originate a prefix. This ability is deduced from prefix delegation and allocation hierarchy, and ASes relationships. RIRs allocate prefixes to organizations and AS numbers independently. Any AS number that an organization handles can be a legitimate origin AS of the prefixes that have been allocated to the organization. An AS originates legitimately a prefix if:

- IANA has directly allocated the prefix to the AS (early allocations)
- The prefix was delegated to a RIR. The RIR allocated it to the AS. The prefix may be assigned to this AS or sub allocated to another organization.
- The prefix is allocated by a provider to a multihomed AS that announces it to all its providers.
- The prefix is allocated to an exchange point and the AS is one of the autonomous systems in this exchange point.

Formally this legitimacy may be defined as follows:
∀ASN ∈ AASN ∀C, C' ∈ O ; ASN∈ ASN(C)
ASN originates legitimately P if:

- P∈ OIP(IANA) and $IANA \xrightarrow{P} C$ (early allocations)
- *or P ∈ IP(R) and* $R \xrightarrow{P} C$
- *or P ∈ IP(R) and* $R \xrightarrow{P} C'$ *and* $C' / \xrightarrow{P} C$
- or P ∈ IP(R) and $R \xrightarrow{P} C'$, and C ∈ Providers(C).
- or P ∈ IP(IX) and ASN ∈ ASN(IX)

3.3 Path Validity and Policy Conformance

Path validity may be defined by its existence physically and logically. A path exists physically if a BGP session exists between routers of ASes in the path. It exists logically if routing policies of each AS in the path authorizes its creation and advertisement. Let import(AS) and export(AS) be AS's import and export policies where AS ∈ AASN. Here are examples of policies:
- import: from AS2 action pref = 1; accept {128.9.0.0/16} : this example states that the prefix 129.9.0.0/16 is accepted from AS2 with preference 1.
- export: to AS2 announce AS4 : in this example, AS4's routes are announced to AS2

Policy conformance: A path containing a sequence of ASn ASn-1 ….. AS2 AS1 to a destination d is valid and policy conformant if:

export(AS1) contains announce d to AS2 or any
and import (AS2) contains accept d from AS1
and export(AS2) contains announce d to AS3
……..
and import(ASn-1) contains accept d from ASn-2
export(ASn-1) contains announce d to ASn or any
import(ASn) contains accept d from ASn-1

3.4 Operational Requirements

One of the operational requirements is a low cost of the solution to be deployed. When deploying a secure routing protocol using cryptographic features to attest address ownership, expenses of issuing credentials is an ISP and RIR responsibility. It is a costly solution since it requires RIRs and ISPs involvement while their benefits from this investment are limited. A second requirement is related to BGP convergence time which should not be heavily increased. Finally, the solution that will be adopted should be incrementally deployable.

4 BACKGROUND, METHODOLOGY AND DISCUSSION

It is likely to be some time before a cryptographic mechanism for routing information authentication is deployed and have a significant security benefit. Our viewpoint is that in the meantime we need an intermediate solution that detects incorrect routing information. Routing system needs an "online" - runs while the routing is running- verification system which instantaneously distinguishes between suspicious and legitimate routes.
We describe in this paragraph a system able to detect and to react to anomalous announcements. It is based on available information retrieved from

Internet Routing Registry databases, received routes, and archived public routing data. The first goal is to facilitate the decision process when a change of a prefix's origin AS is received. We present in this paragraph the sources of data that we use and the methodology we followed.

4.1 Internet Routing Registry Database

The Internet Routing Registry (IRR) represents a framework for ASes cooperation. The IRR is a distributed set of routing databases that are individually operated by organizations such as Verio, Merit and by RIRs like APNIC, ARIN, and RIPE. RIRs databases contain data related to IP prefix and ASN allocation. Some ASes publish their routing policies and the policies of their customers. Routing Policy Specification Language (RPSL) (Alaettinoglu, 1999) is used to specify ASes policies that are stored in these object oriented databases. RPSL can also be used to produce router configuration files (IRR).Unfortunately, all the ASes are not members of this IRR community and do not register their routing data. Therefore some data may not be available. Siganos et al (Siganos, 2004) designed a tool that analyzes IRR databases. This tool tests policies consistency and compares the registered data to real routing data. The analysis showed that RIPE database is the most consistent database and that RIRs databases generally provide useful information. RIPE has also a project aiming at checking their database consistency (RIPE RRCC). RPSL is object oriented; different classes are defined in this language. The **route** class is one of the classes used in RPSL to define policies and administrative objects. This class is used to register prefixes and their origin AS.

4.2 Public Routing Data

Routeviews (Routeviews) and RIPE RIS (RIPE RIS) are two major measurement projects that deploy route collectors and provide publicly available BGP data. A route collector is a measurement box that peers with commercial ISP networks via BGP sessions. It receives BGP messages from its peers, but it does not advertise any prefixes back to them. Periodically, the collector dumps its full routing tables and routing updates received from its peers.

4.3 Methodology

The aim of our system is to enable origin ASes changes detection and to decide which action to carry out after this detection among predefined actions. The idea is to associate with an AS a legitimacy level to originate a prefix P based on regional internet registries databases, received announcements and an analysis of public routing announcements.

4.3.1 System Architecture

The conceptual model architecture of our system is composed of the following components:

- Origination legitimacy database: we store in this database a legitimacy level to originate a prefix associated with an ASN.
- Data collection module: this module collects data from RIR databases. This data is used to initialize the values of the legitimacy level of an AS to originate a prefix. This legitimacy level is updated as received announcements are processed. This module collects also announcements from public routing data.
- Data processing module: collected data from the previous module is processed in this module. One of the functions of this module is to detect origin AS changes. A second function is to process received announcements and public routing data to infer legitimacy level from received announcements.
- Decision module: This module is able to decide which action to carry out from the predefined set of possibilities. When an origin AS is detected the received announcement may be filtered, dampened. The router may also de-aggregate its prefixes if it detects that its prefixes were originated by another AS.
-

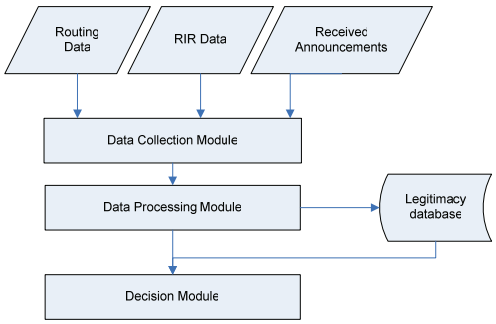

Figure 1 : System architecture.

4.3.2 Components Functions

Data collection: This module collects the required data from RIR databases. Registry databases do not contain all the required data and legitimacy cannot be validated to every tuple (prefix, AS). We applied our model to validate the tuples (prefix, origin AS) of the routing information in a routing table of one router of a provider. 20% of the prefixes present in its routing table were allocated to RIPE. In the RIPE database, available tuples represents 96% of these prefixes. This module collects also public routing data and received routing data in the AS in order to infer a legitimacy level to missed data. Since, there is no explicit data about multihomed ASes and their providers. This means that we cannot collect this information and have the set of providers of an AS. We assume that an AS is a potential originator of a prefix if it is one of the ASes to which the owner AS exports this prefix and if it imports this prefix from the owner AS. This module collects also export and import policies of ASes and the correspondent prefixes.

Data processing: Collected data from registry databases is processed in this module in order to infer the legitimacy level of an AS to originate a prefix. This level is a real number between 0 and 1. It is considered as the probability of announcement correctness. The highest level is associated with route records (origin, prefix) that are registered in RIR databases. A threshold is associated with tuples (AS, prefix) if the AS is a potential originator as the definition we have defined above. If a part of these conditions is satisfied then the legitimacy value associated with the tuple is the half of the threshold. If the conditions are not satisfied then the value is null. If we consider the hypothesis that RIR databases are not complete and not updated frequently, this value changes in time. This change depends on the received advertisements and the public routing data. These data are also used in a heuristic way to infer legitimacy level of a tuple when there is no information about the export policies of the owner AS of this prefix.

Collected export and import policies are stored in a database where the relation between prefixes, their origin ASes, ASes to which they are exported and ASes from which they are imported is more explicit. This data is then used to associate the legitimacy level with tuples. If the origin AS of a prefix exports the prefix to an AS (or a set of ASes) and symmetrically the AS (set of ASes) imports the prefix then the threshold of legitimacy is associated with the tuple (AS, prefix). If the AS does not import the prefix then the half of the threshold value is associated. Finally, ASes that are not in the export list of the origin AS are considered illegitimate, and the value associated is null. This value changes in time according to the received advertisements and the public routing data.

Public routing data is used to observe multiple origin announcements for prefixes for an observation period. A report is carried out containing prefixes originated by multiple ASes and their origin ASes. We focus on origin ASes that do not satisfy the conditions above (ASes that are not registered in RIR databases as origin of the prefixes and ASes that are not potential originators of the prefixes). We observe the time period where the prefix is originated by those ASes. A threshold is set to the period. If this period is shorter than the threshold the advertisement is considered as a misconfiguration or a hijacking. The AS is considered suspicious. The threshold is an important parameter in our system. It should be well tuned in order to let the heuristic be efficient and to avoid false positives.

We used RIS collected data for the month of October 2005, we observed daily MOAS reports. We focused on prefixes that are present more than 25 days in these reports. 65 % of these prefixes do not have a registered origin AS, although 70% of these prefixes are delegated to RIPE and this database is considered the most complete one. The remainders 35% have a registered origin AS, but all the origin ASes observed are not mentioned in the export policy of the registered origin ASes. So, according to our model all these announcements are considered suspicious. But the number of times these ASes originate these prefixes is considered high and the period is long, so the legitimacy may be estimated once again. At this step, we need a neural network which considers all the new announcements and evaluates the legitimacy level as announcements are monitored. The consideration of some other RPSL attributes like the description of network (inetnum, maintainer, email addresses)(IRR) may be used as a heuristic to readjust the model we specified. In this module, public routing data is also used to help a provider detecting if another AS is originating its prefixes or the prefixes of its customers.

Received announcements are monitored in order to avoid incorrect ones. They are stored and analyzed to infer the legitimacy level of tuples (AS, prefix). A route will not be selected before the ending of the data processing and decision process execution. When a new advertisement is received, the origin AS is compared to the one in the routing table. If an

origin AS change is detected then the legitimacy database is checked. The action which will be performed by the decision process depends on this value. The decision process is explained in the next paragraph. All the parameters of the announcement are stored in order to infer the legitimacy level of the correspondent tuple. The model used in the analysis is similar to the one used in the analysis of public routing data. It is based on the number of times the tuple is received. The difference resides in the ability of the AS that monitors the routes that its routers receive to use other parameters. The parameters are the trust level it associates with its peers that send the announcement containing the tuple and its routes preference generally based on business relationships. Moreover, when an origin AS change is detected for the first time, another parameter can also be considered. If we assume that the incorrect route was sent for the first time due to a misconfiguration or a short lived hijacking attack, then the route may be ignored for a brief period of time. During this period of time, the router waits for another announcement with the same attributes that withdraws the previous or for a different route. This period should be well tuned in order to let the router enough time to receive the second announcement. In summary, the legitimacy level inferred depends on the number of times the tuple is received, the peer that sends the tuple, and the announcements that follows.

Decision Module: There are different actions that can be performed when an origin AS change is detected in received announcements and public routing data. The action depends on the source of the data. First, when an origin AS change is detected in received announcements, the legitimacy database is checked in order to find a value for the received tuple (Prefix, Origin AS). If the value is higher than the threshold then the announcement may be selected. Note that this verification should be applied before the execution of the BGP best route selection process. We mean that the preference for non suspicious routes should be the first step in the route selection process before the local preference and the AS path length. However, this may introduce an economic trade off for the AS. Generally the preference of a route is business relationship-driven. Customers' routes are preferred to provider routes. The AS gains revenue by directing as much traffic as possible through downstream customers. The reception of non suspicious routes from the provider would constrain the AS to choose a route that goes against its business model.

In the other case, if the legitimacy value is lower than the threshold, then the announcement is discarded. If the received prefix is less specific than the one in the routing table and was aggregated then this aggregation is considered in the legitimacy level evaluation. If the legitimacy level of the received tuple has not been yet evaluated, due to a lack of information in RIR databases or because the announcement was sent for the first time, then the announcement will not be discarded but the selection will be delayed. The decision process will wait for more information to evaluate the legitimacy level.

Next, when the analysis of public routing data reveals to the AS that one of its prefixes or its customers' prefixes is originated by an unauthorized AS, then the AS may de-aggregate the affected prefix. This will guarantee that no traffic will be lost. Then, the AS may use filters based on prefixes to block the announcement. When the unauthorized announcements disappear the AS disable those filters. The length of the prefix, that was announced by an unauthorized AS, may raise a problem. In fact, if the prefix is a /16 then, announcing /17 may solve the problem. But if the prefix is a /24, announcing /25 will not solve the problem since most of the ASes filter prefixes more specific than /24.

4.4 Discussion and Future Work

We defined in this paper a system able to detect incorrect Internet routing announcements. This approach is simple and may be deployed immediately since no protocol changes are required. We believe that it is an efficient approach that can be used today until rigorous solutions based on public key infrastructure will be deployed. Our approach is based on available data from registry databases. The registered data may be updated by their owners. The legitimacy level that we infer from this data should also be updated. An automatic update feature of the database should be added and scheduled.

We use a statistics-based approach to identify incorrectness related to unavailable data. Like all the statistics-based approaches, our approach is faced to the "magic number" problem. In fact, the legitimacy level that we evaluate depends on the number of times the tuple (prefix, origin AS) is announced during a period of observation. This period is also a key parameter which must be well tuned in order to avoid false positives. In the legitimacy level inference, we assumed that when an AS aggregates a prefix it can be considered as legitimate originator.

Further verifications should be applied to aggregators. We are working on the definition of conditions for these verifications. Moreover, the evaluated legitimacy level may be exchanged between ASes that trust each other. It can be considered in the decision process of each AS participating to a collaborative architecture. Finally, the system we have defined may be extended to support the policy conformance verification of a route.

5 CONCLUSION

In this paper we defined formal correctness rules that BGP advertisements should satisfy. We designed a system able to detect incorrect announcements and to classify them in order to be considered in the decision process. We used available data in regional Internet registries to verify the legitimacy of an AS to originate a prefix. We also defined a methodology to infer this legitimacy level to the missed data. We believe that registry databases contain useful information that can be used for route announcements verification.

We also believe that some enhancements to these databases can have a significant impact on routing security. The problem that we tried to settle is the distinction between invalid multiple origin AS announcements for prefixes and valid ones. Multihoming is one the cases where prefixes may be originated by multiple ASes. Unfortunately data related to multihomed ASes, their providers and their prefixes is not available. The availability of this data would ease this distinction between multihoming BGP advertisements and wrong multiple BGP advertisement. We think that this data should be added to registry databases.

In the future, we expect to further enhance our approach and to define methods to verify the policy conformance rules we have defined in this paper. Further work will be to make routers ore intelligent and to automatically react to anomalous announcements.

REFERENCES

Rekhter, Y, 2006. The Border Gateway Protocol. RFC 4271

Huston, G. 2006. www.potaroo.net

Kent, S., 2000. Secure Border Gateway Protocol. In *IEEE Journal on Selected Areas in Communications, Vol. 18, No. 4, pp. 582-592*

Atkinson, R., 2004. IAB Concerns and Recommendations Regarding Internet Research and Evolution. RFC 3869.

Zhao, M., 2004 Evaluation of Efficient Security for BGP Route Announcements using Parallel Simulation. *In Journal on Simulation Modeling Practice and Theory*

Zhao, M., 2005. Aggregated Path Authentication for Efficient BGP Security. *In proceedings of ACM Conference on Computer and Communications Security*.

White, R., 2003. Securing BGP through Secure Origin BGP. *In Internet Protocol Journal, Cisco, Vol. 6 Num 3, p15-22*.

Wan, T. 2005. Pretty Secure BGP. *In proceedings of Network and Distributed System Security Symposium Conference*.

RPSec WG, www.ietf.org/html.charters/rpsec-charter.html

SIDR WG, www.ietf.org/proceedings/06mar/minutes/sidr.txt

Teoh, S.T., 2003. Visual-based Anomaly Detection for BGP Origin AS Change (OASC) Events. *In DSOM2003, 14th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management*.

Teoh, S. T., 2004. Combining visual and automated data mining for near-real-time anomaly detection and analysis in BGP, *CCS Workshop on Visualization and Data Mining for Computer Security*.

Zhao, X., 2002. Detection of Invalid Routing Announcement in the Internet. *In Proceedings of International Conference on Dependable Systems and Networks*.

Kim, E., 2005. Global Internet Routing Forensics: Validation of BGP Paths using ICMP Traceback. *In Proceedings of the First annual IFIP WG 11.9 International Conference on Digital Forensics*.

Hyun, Y., 2003. Traceroute and BGP AS Path Incongruities. *In the proceedings of the International Working Conference on Performance Modeling and Evaluation of Heterogeneous Networks*.

Goodell, G., 2003. Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing. *In proceedings of Network and Distributed Systems Security.*

IRR. www.irr.net

Alaettinoglu, C., 1999. Routing Policy Specification Language. RFC2622

Meyer, D., 1999. Using RPSL in Practice, RFC2650.

Siganos, G., 2004. Analyzing BGP Policies: Methodology and Tool., i*n Proceedings of IEEE INFOCOM.*

RIPE RRCC Project, www.ripe.net/projects/rrcc/index.html

Routeviews, www.routeviews.org

RIPE RIS Project, www.ripe.net/projects/ris/index.html