Internet Hardening via Routing Registries

Larry Blunk Manish Karir
Merit Network, Inc., Ann Arbor, MI 48105
{netrd}@merit.edu

Abstract— **The Internet in its current form relies on extensive cooperation between network operators to ensure the integrity and security of its core infrastructure. Here we describe how routing registries can be used to improve the security of the Internet infrastructure in general and the BGP routing protocol in particular. Routing registries can be used to generate accurate prefix filter lists as well as detect and protect against anomalous routes that can disrupt the flow of Internet traffic. In addition, when used with a hierarchical and distributed authority model, routing registries can be used to implement a scalable solution to the problem of hardening the Internet. Due to the smaller number of existing prefixes, IPv6 can serve as an ideal testbed to demonstrate the ideas, which when proven can also be implemented in IPv4. The success of the proposed approach lies in ensuring that the data in the routing registries is valid and accurate. Merit Networks, which manages the Routing Assets Database (RADB), is developing a suite of tools to enable users to easily view, analyze and update their routing assets information. Merit operates the largest IP network in Michigan, and manages the North American Network Operators Group (NANOG), the leading forum for information sharing and collaboration among network service providers. It is clear that any effort to harden the Internet infrastructure will require extensive cooperation among network service providers, and it will need to be implemented in an incremental fashion. There is no single solution to security. Security needs to be added to the Internet at all levels. Here we describe the role routing registries can play in helping to secure the Internet infrastructure.**

I. Introduction

The Internet currently relies on a cooperative system of interconnected network service providers. The Border Gateway Protocol (BGP) serves as the underlying routing protocol among these providers. However, BGP is vulnerable to both accidental configuration errors and malicious attacks. Fully addressing these vulnerabilities requires modifications to the core BGP protocol. There have been several efforts to add security to the BGP protocol, however they have failed to gain wide spread acceptance in the network operations community. Securing the infrastructure requires that functionality be added at various levels. Even though current efforts at securing the base BGP protocol have been successful only in ensuring message authentication via MD5 checksums, there are other approaches that can serve to add a layer of resilience to the Internet. It is important to look beyond protocol modifications to BGP to determine what additional actions can be taken.

An important class of assets in securing the Internet is the various Internet Routing Registries. The routing registries were originally developed to serve as public databases of routing policy. This public information would facilitate network operators in configuring routing protocols in their network domains in a secure and efficient manner. In this paper we describe various methods by which routing registries can help to protect the Internet infrastructure.

The security limitations of the BGP protocol have long been recognized. The lack of security mechanisms that are an integral part of the protocol, has led to the use of provisional security measures such as filtering BGP routing update messages. For example, the NSFNET (1986-1995) employed a filter list consisting of the networks which were allowed to transit the backbone. This list was created from a registration database and was necessary due to the lack of an authorization mechanism in the BGP protocol itself.

With the decommissioning of the NSFNET in 1995, control of the backbone routing on the Internet passed to multiple commercial Internet providers. As part of the transition, the NSF sponsored a Routing Arbiter project to coordinate inter-provider routing. Like the NSFNET before it, the Routing Arbiter employed a database of authorized network routing information for filtering routing announcements. This database became known as the RADB routing registry.

The Routing Arbiter utilized devices known as Route Servers at a fixed number of Network Access Points (NAPs) where network providers could connect. However, as the complexity and number of interconnection points among network providers increased, the role of the Routing Arbiter and NAP sites lessened. Without Route Servers performing verification of routing updates at these alternate interconnection points, it became incumbent upon the providers to perform this verification directly with their routing peers. For those who do not verify routing announcements, there is a greater likelihood of erroneous configurations or malicious attacks impacting Internet routing.

Hardening the Internet requires a coordinated effort involving the research community, the infrastructure equipment development community as well as the network service operator community. The inherent potential of the valuable information in routing registries can be exploited to create more secure policies. These include not only prefix filter generation, but also anomalous routing event detection and notification. The routing registries contain valuable information that can be used to detect, isolate and guard against such potentially disruptive routing events.

II. Internet Hardening via Routing Registries

A. Attacks on the Internet Infrastructure

We motivate the need to include the use of routing registries in the process of Internet hardening by first briefly describing some of the attacks that are possible on the core Internet infrastructure, which routing registries may help to mitigate. Most of these are fairly well understood, and some have even been witnessed in the Internet in the past. The reason routing registries are critical to the process of Internet hardening is that when properly used, they serve as databases that can help us distinguish and identify anomalous events. Some of the vulnerabilities described below are described in detail in [11].

- Route Hijacking/Black Hole Routes: In this type of an attack, a BGP node simply starts advertising reachability for routes that belong to someone else. There are two forms of this attack. In the first, the malicious node simply starts advertising a more specific route to one that is already being advertised by someone else, in effect, hijacking these more specific subnets and routing all traffic destined for these to itself. In the second version of this attack, the malicious node can start advertising the entire prefix already being advertised by someone else. In this case the impact will be limited to the portions of the Internet that conclude that the malicious node represents the shortest path to that network. This type of attack, though unintentional in this case, has already been witnessed in the Internet [12][13].
- Worm Holes and Man in the Middle Attacks: While route hijacking attacks can atleast be detected if not prevented, worm hole attacks constitute a much more stealthy class of attacks. Worm hole attacks when used in conjunction with traffic proxying can create an extremely effective man in the middle attack.
- Modification of BGP Attributes: In this type of attack, a compromised BGP speaker, starts performing subtle but possibly critical changes to the BGP messages it sends to its peers. It can silently modify, insert or delete communities, ASPATH, MED, as well as several other key attributes that can affect the routing behavior of the Internet.

In the subsections below we describe how routing registries can be used to mitigate the threat to the Internet infrastructure. As the weaknesses in the Internet infrastructure are present at different levels, it is not possible to protect against all malicious activity with the help of routing registries. However, we believe that when properly used, routing registries can play a very significant role towards hardening the Internet infrastructure.

B. Routing Filters

Prefix filters constitute the most commonly used method of attempting to add some security to the BGP routing protocol. [6] outlines various threats against BGP and advocates the use of aggressive filtering to ensure that malicious routing events are identified and eliminated. By ensuring that routing updates and messages are only obtained from trusted peers we take a step forward towards securing the Internet. In addition, simple sanity checking on any routing messages obtained from peers can easily identify either malicious attacks or potentially problematic misconfigurations. The operational problem with this approach is that these filter lists quickly get very large, and are difficult to manage manually.

This is a scenario where we can easily use routing registries to enhance the security of BGP. The routing registries are ideally suited for the task of appropriate prefix filter list generation. Some service providers do in fact rely on such automated filter generation for customer peers, but a significant number of the network service providers do not. This may be due to the added complexity of filter generation and lack of knowledge concerning routing registries. There are also concerns about the validity and completeness of the data. The problem of the completeness of data in the routing registries is something that can be eliminated over time, as more people begin to rely on that information.

C. Routing Anomaly Detection and Notification

Routing registries can play an important role in securing the Internet by assisting in the ability to detect anomalous routing events, which might be potentially malicious. For example, some simple checks that one can perform on routing information are to ensure that the party that is responsible for them is advertising routes. A simple check in a routing registry database will provide this information. If an anomalous event is detected an alarm or notification messages can be generated. An implementation of this system would include extending the existing routing registry software and specification standards to encompass event triggers, notification mechanisms, and other relevant features. These extensions would relate to existing

registry functionality, which specifies the expected origin AS of an IP Prefix, AS Path relationships, and other BGP attributes. These extensions will allow an operator to be notified upon deviations from expected routing policy.

In addition to the modifications outlined above, it is also important to develop collection and archival processes for existing BGP routing data collection projects. Such projects include the University of Oregon Routeviews Project [14] and RIPE's Routing Information Service (RIS). These services collect BGP routing update data via peering sessions with numerous network providers throughout the world. This data will serve as the input to the detection and notification tools. Upon detection of an anomalous routing event, the appropriate notification can be sent to the owner of a network prefix or AS.

There is also a need to design aggregation and archival data formats and databases for archived BGP collection data. The current formats employed by routing collection projects are generally too verbose to allow quick and efficient searches of the data. Developers must often independently devise their own aggregated and intermediate formats in order to process the data when examining it for anomalous events. Having standardized aggregated formats, and software tools for processing these formats, could greatly benefit future research. It would provide the ability to look back for historic anomalous behavior, as well as provide the ability to search for patterns in such events.

The ultimate goal of this scheme would be to be able to perform such route anomaly checking in an online manner and to couple this with the elimination of the anomalous event from the network. Anomaly detection could be a short term goal while widespread filtering and elimination of anomalous events requires improvement in the accuracy of routing registry data.

D. Developing an Authority Model for Routing Registries

The routing registries currently operate independently of each other. At best, their level of interaction with each other is limited to mirroring of each others registry databases. There are instances where routing information in these databases is inconsistent, inaccurate, or conflicting. This structure limits the utility of the routing registry system. Not only are the results of querying routing registries incomplete, but it is possible to obtain different results from queries to different registries. Clearly there is a need to develop a comprehensive framework into which each of the routing registries can fit. One of the principal requirements of such a framework is that it should be able to maintain the level of freedom that each of the routing registries currently enjoys. In addition, the framework should be able to scale to accommodate both the prefix and the routing policy registration information for the entire Internet. Careful co-ordination is necessary to ensure that the existing routing registries all agree on their respective roles in this authority model.

There has been some work in this direction in the past. For example rfc2725[7], and rfc2769[8] outline a framework for organizing the routing registries into a single cohesive framework. These need to be re-examined for their applicability. A system modeled along the lines of hierarchical DNS could be developed, however any such effort would need to included the Internet and NANOG communities from the start. It is also important to ensure that the authority model includes appropriate security mechanisms in the query/response procedures as well as the data maintenance procedures. If routing protocol hardening is to be based on information derived from routing registries, it is essential to ensure that additional vulnerabilities are not introduced as an artifact of this process.

E. Securing IPv6

IPv6 presents an ideal opportunity to develop and implement the coupling of routing registries with BGP. IPv6 is still in an early growth phase, and currently there are approximately only 500 prefixes being announced. This can serve as an ideal testbed to demonstrate the concepts outlined in this paper. All the problems that we have described for IPv4 above also exist in IPv6. For example, recently there was a scenario where a misconfigured IPv6 BGP speaker suddenly started to advertise 178 prefixes [10]. It is much easier to implement and demonstrate an online anomalous route detection and elimination system with such a small number of prefixes. Routing registries such as the RADB already support IPv6 route registration, and the task of ensuring the validity of only approximately 500 prefixes is quite manageable.

F. Ensuring Validity and Accuracy of Routing Registry Data

The basis for the use of routing registries in validating routing protocol information is based on the premise that the data maintained in the routing registries is accurate. Unfortunately, today, this is not the case. We are currently working on implementing a suite of tools that will assist in improving the accuracy of routing registry data. These tools consist of customized report generation for each registered organization. Making it easier for registrants to view, analyze and modify their registered data will help improve the accuracy of this data. The software suite includes personal web portals, anomalous route alerts, routing filter generation tools, as well as proxy maintainer email addresses to ensure that responsible parties are always reachable to address issues related to their organization.

III. Related Work

There are several efforts being made to improve the security of BGP at the protocol level, we only describe some of the most relevant projects here. While it is clear that these projects are important in addressing BGP vulnerabilities, due to the large-scale changes required, it is unlikely that these improvements will be deployed in the near future. There are currently three initiatives of note to improve BGP protocol security. These vary in security scope and level of deployment complexity. Inter-domain Routing Validation (IRV) [1] proposes a protocol that works in concert with the existing BGP protocol rather than adding new semantics to BGP. It is posited that IRV can be deployed in an incremental manner with modest changes to existing router software. Secure BGP (S-BGP) [2] incorporates a number of changes in the BGP protocol to improve security. It addresses the validity of the origin AS and AS path of a prefix using an X.509-based certificate hierarchy. Secure Origin BGP (soBGP) [3], like S-BGP, relies on an X.509-based hierarchy. However, it only addresses the validity of the origin AS of a prefix and not the entire path. It authors believe it to be simpler to implement and deploy than S-BGP.

In addition, there have been several research efforts, which have attempted to examine Internet routing data for anomalies and inconsistencies. Merit Network developed a program to compare observed Internet routing data with registered routing policy data. This project was entitled Policy Analysis of Internet Routing (PAIR) [4]. The routing data was collected from Merit's Route Server Next Generation (RSNG) project. The PAIR project regularly posted data analysis results on it website. Though this project was able to provide a good example of analysis that could be performed on routing data., it had a number of limitations: 1)it was based on routing table snapshots rather than actual BGP update messages, hence, short-lived anomalous data could be missed, 2) there was no mechanism for notifying network owners of anomalous events, 3) it lacked the ability to dynamically generate reports based on particular criterion. The PAIR project was concluded with the cessation of the RSNG project in 2002.

Protocol misconfigurations are often responsible for vulnerable infrastructure. To quantify the scope of this problem Mahajan et. al [5] studied the cause and impact of BGP misconfigurations based on an analysis of BGP routing advertisements over a three week period. The study concluded that configuration errors are pervasive, with 200-1200 network prefixes erroneously configured each day. This once again highlights the important role that routing registries can play.

IV. Conclusions and Future Work

In this paper we have outlined how closer interaction between BGP and routing registries can enhance the security of the Internet. We briefly described how the routing registry databases are ideally suited to provide the information needed to detect malicious routing events. We summarized some of the more common attacks that have occurred or may occur on the routing infrastructure today, and then presented some simple ways in which routing registries can be extended via simple tools to harden the Internet against malicious attacks. Merit is able to offer a unique perspective on this topic by virtue of being a network service provider, a routing registry provider, and a coordinating body in the network operations community. It is possible to greatly improve the ability of the Internet to withstand malicious attack by enhancing the routing registries to include an authority model, ensuring the completeness of their data, and developing tools to not only generate filter lists based on this information, but to perform both passive and active correlation between routing events and the routing registry data.

References

[1] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel, A. Rubin. *W*orking Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing, *NDSS '03*, San Diego, 2003.

[2] C. Lynn, J. Mikkelson, K. Seo, Secure BGP (S-BGP), Internet Draft, draft-clynn-s-bgp-protocol-01, July 2003.

[3] J. Ng, Extensions to BGP to Support Secure Origin BGP (soBGP), Internet Draft, draft-ng-sobgp-bgp-extensions-01, June 2003.

[4] The PAIR project, http://www.rsng.net/pair

[5] R. Mahajan, D. Wetherall, T. Anderson. Understanding BGP Misconfiguration, *SIGCOMM '02*, Pittsburgh, 2002.

[6] B. Raveendran, BGPv4 Security Essentials, http://www.nanog.org/mtg-0206/ppt/BGP-Risk-Assesment-v.5.pdf, April 2004.

[7] C. Villamizer, et.al., RFC 2725: Routing Policy System Security, http://www.ietf.org/rfc/rfc2725.txt, December 1999.

[8] C. Villamizer, et.al, RFC 2769: Routing Policy System Replication, http://www.ietf.org/rfc/rfc2769.txt, February 2000.

[9] RADB: Routing Assets Database, http://www.radb.net

[10] 6bone Mailing List, AS1654/SICS Announces 178 Prefixes, http://dict.regex.info/ipv6/6bone/6bone.mail-2003-06/0010.html, June 2003

[11] S. Murphy, BGP Security Vulnerabilities Analysis, Internet Draft, draft-ietf-idr-bgp-vuln-00.txt, June 2003

[12] NANOG Mailing List: AS7007, http://www.merit.edu/mail.archives/nanog/1997-04/msg00340.html, 1997

[13] Hijacked IP Addresses: http://www.completedwhois.com/hijacked

[14] Route Views Project, http://www.routeviews.org