A Proposal to Improve MANRS Global Secure Internet Routing Policy Management Using Blockchain Technology

Version 1.1
June 6, 2020

William Favre Slater, III
slater@billslater.com
williamslater@gmail.com
Chicago, IL
United States of America
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>What We Learned in the ISOC MANRS Global Secure Routing Course</td>
<td>3</td>
</tr>
<tr>
<td>Introduction – Beginning at the Beginning</td>
<td>4</td>
</tr>
<tr>
<td>What Is MANRS?</td>
<td>13</td>
</tr>
<tr>
<td>What Problem Does MANRS Address?</td>
<td>14</td>
</tr>
<tr>
<td>What Is Secure Global Internet Routing?</td>
<td>14</td>
</tr>
<tr>
<td>Why Secure Global Internet Routing and Why Now?</td>
<td>17</td>
</tr>
<tr>
<td>What Is Blockchain and Why Is It Important?</td>
<td>18</td>
</tr>
<tr>
<td>How Can Blockchain Enhance Secure Global Routing?</td>
<td>20</td>
</tr>
<tr>
<td>Conclusion</td>
<td>21</td>
</tr>
<tr>
<td>Important Resources for Your Success</td>
<td>22</td>
</tr>
<tr>
<td><strong>Internet Routing Resources</strong></td>
<td>22</td>
</tr>
<tr>
<td><strong>Blockchain Resources</strong></td>
<td>22</td>
</tr>
<tr>
<td>References</td>
<td>23</td>
</tr>
</tbody>
</table>
Executive Summary

This blog will explain the highlights and the importance of what we learned in the ISOC MANRS Global Secure Routing Course, and then propose how Blockchain technologies can be used to further enhance the MANRS processes that have been established to provide secure Internet Routing.

What We Learned in the ISOC MANRS Global Secure Routing Course

This is the agenda for the ISOC MANRS Global Secure Routing Course:

- Routing Protocols with emphasis on BGP
- BPG and Global Routing Security
- Incidents Caused by Routing Errors
- What MANRS Is, How It Works and Why It Is Important
- Internet Routing Registries (IRR) and the Role They Play in Secure Internet Routing Infrastructure
- Internet Routing Registries (IRRs)
- Resource Public Key Infrastructure (RPK)
- PeeringDB
- Creation of a Network Policy
- Global Validation
- How Network Policies Work From a Practical Perspective
- Open Source Tools Used to Develop and Register Network Policies
- Filtering Techniques and Why We Use Them
- Anti-Spoofing Techniques and Why We Use Them
- Coordination and Techniques, Including Registration, Roles, and Responsibilities
Introduction – Beginning at the Beginning

The Internet began in 1969 as the ARPANET Project successfully used electronic communications to transmit messages between four centralized computers. The pictures below show the original ARPANET.

Scrawled on this paper in 1969 were the first four nodes of the ARPANET. Little did they realize these four nodes would grow to millions. (Image courtesy of The Computer History Museum, www.computerhistory.org)
The big color picture below from opte.org is a visualization of the Internet as it was in 2015.
A Proposal to Improve MANRS Global Secure Internet Routing Policy Management Using Blockchain Technology

Project Work Submitted to Mr. Tawanda Kembo, Chairman of the ISOC Blockchain SIG

William Favre Slater, III
June 6, 2020
The diagram below shows how people typically interacted with the Internet every 60 seconds in 2019.
The diagram below shows a high-level summary of how the Internet evolved from a conceptual idea to the time when it became an environment for e-commerce in the 1990s.
The rapid growth of e-commerce as well as the “dot-com” explosion from 1996 - 2000 made the Internet go “business critical” somewhere between 1997 to 1998. This not only meant that most organizations were adopting an online presence of their physical self, but that they were beginning to expect having Internet access on a 24 x 7 basis, including websites, e-mail, and e-commerce transactions. As these expectations continued, a transformation to a ‘Digital Economy” occurred, and downtime was not considered to be acceptable and in fact, it was considered to be a detriment to the viability of any organization that could not be up on the Internet on a 24 x 7 basis.
The Internet of the 21st Century has evolved into an environment that is heavily dependent on connected Cloud Data Centers, Cloud-based applications, and mobile applications. This requires a responsive, reliable, low-latency, network of networks to support these applications. Then with the onset of the global CoronaVirus Pandemic in March 2020, with social distancing requirements and the need for precautionary measures to slow the spread of this highly contagious virus, organizations started ordering their employees and contractors to work from home, in other words, to Telework as a standard business practice.

Whereas employees had formerly been used to going to work and connecting to their employer’s Internet connection, now they are relying on their home Internet Service Provider (ISP) to get out to the Internet to get their organization’s work accomplished. The Cloud and mobile applications are still very much in the picture, but the reality and ubiquity of telework for foreseeable has led ISPs to have to work with major Internet carriers to add new networking equipment and reconfigure their connections to optimize these new, unexpected Internet traffic patterns and usage loads.

It should be noted here that one of the biggest reasons for the successful evolution of the Internet as an environment/resource that most people in the civilized world depend on, is free, well-written standards and the organized framework for testing, evaluating, and publishing these standards. These are the RFCs (Request for Comments). The RFCs may be considered as the evolving “Constitution” of the Internet, and they are usually developed and approved by members of the Internet Engineering Task Force. The entire body of RFCs are located in these locations for public viewing:

- [www.rfc-editor.org](http://www.rfc-editor.org)
- [www.ietf.org](http://www.ietf.org)
- [www.faqs.org](http://www.faqs.org)
The diagram before shows the types of RFCs and how they get published.

Types of RFCs

![Diagram of RFC Publication Process]

The diagrams below should the organizations that influence the development of the Internet and Internet Standards. Note that in October 1998, IANA was replaced by ICANN. Also, in 2016, President Obama assigned ICANN as part of the United Nations, so it now operates independently from the authority of the Government of the United States.
For Completion of the The MANRS Secure Global Routing Course
A Proposal to Improve MANRS Global Secure Internet Routing Policy Management Using Blockchain Technology
Project Work Submitted to Mr. Tawanda Kembo, Chairman of the ISOC Blockchain SIG
William Favre Slater, III
June 6, 2020
What Is MANRS?

MANRS stands for the Mutually Agree Norms for Routing Security. It is a collective effort by Internet stakeholders (network operators, content distribution networks and IXPs) needed to achieve global routing security. MANRS has created and published the principles, standards, and procedures for Global Routing Security actions that will provide Routing Security for Global Internet Stakeholders if they are carefully followed. MANRS currently supported by a growing and visible community of more than 200 networks around the world that have adopted the MANRS guidelines for Global Security Internet Routing.

MANRS, is fostered by the Internet Society as a Global Strong Internet Project and it is currently led by Mr. Aftab Siddiqui, who works from Sydney, Australia. The screenshot below from May 5, 2020, shows the status of MANRS initiatives from January 2020 to May 2020, as well as their future plans.
The Internet Society wants more network operators, IXPs and other relevant internet stakeholders to join MANRS to help with the widespread adoption of Global Secure Routing Practice, which will lead to a more robust and secure Internet.

What Problem Does MANRS Address?

When the BPG Internet WAN Routing Protocol was architected, just like the TCP/IP protocol, it was created for accuracy, speed, and efficiency. That’s the good news. The bad news is that there are many security issues that BGP does not address. Without addressing Internet security, the raw implementation of BGP routing protocol is subject to many different types of attacks such as spoofing, Distributed Denial of Service (DDoS), reliability, threats to confidentiality of traffic, etc. So think of MANRS as the group of experts who are overseeing the principles, standards, and procedures that address the insecurities that naturally exist in BGP.

What Is Secure Global Internet Routing?

The idea of Secure Global Internet Routing was created to apply MANRS principles, standards, and procedures to carefully create Network Router Policy descriptor to enable the communication computers called Routers, that route packets on the Global Internet to perform this task as reliably and securely as possible. The diagram below shows the relationship of participant Internet routers that can added to a network infrastructure, with a summary the essential Network Router Policy descriptor objects.
Secure Global Internet Routing Policy Configurations related to the BGP Network Routing Policies defined at an Internet Routing Registry (IRR). The IRRs are shown below:

IRR stands for Internet Routing Registry and is a public database of Internet route objects. IRRs are used for determining and sharing route and other related information used for configuring routers.
Each IRR has a database that contain entries for the Network Routing Policy entry for each Router that is added into the Global Internet Infrastructure. Each Network Routing Policy comprised of the following objects:

<table>
<thead>
<tr>
<th>Objects</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>route or route6 object</td>
<td>Connects a prefix to an origin AS</td>
</tr>
<tr>
<td>aut-num object</td>
<td>Registration record of an AS Number Contains the routing policy</td>
</tr>
<tr>
<td>sets</td>
<td>Objects can be grouped in sets, i.e. as-set, route-set</td>
</tr>
<tr>
<td>keywords</td>
<td>“ANY” matches every route</td>
</tr>
</tbody>
</table>

Guidance Proving a 6-Step Summary of the Current Steps Required to Publish a Secure Internet Routing Policy Object.


1. Create a mntner object (equivalent of a user account) to give you the ability to create IRR objects in your selected IRR database
2. Create an aut-num to represent your autonomous system and describe its contact information (admin and technical) and your routing policy
3. Create an as-set to describe which autonomous system numbers your peers should expect to see from you (namely your own and your transit customers)
4. Create a route/route6 object for every prefix originated from your network
5. Update your peeringdb profile to include your IRR peering policy
6. Bask in the glory of enabling your peers to properly filter your peering sessions

Following the MANRS principles, standards and procedures, the creation and application of secure and verified Network Routing Policies and registering these with the IRR that is in the region where the router will reside, helps assure that the Global Internet Infrastructure will be secure, reliable, and continue to grow and evolve in an organized manner that is controllable, will provide the messages to stakeholders in the most efficient manner possible.

Why Secure Global Internet Routing and Why Now?

The importance of entering accurate Network Routing Policy configuration data is underscored by the scale and potential disastrous consequences of that can result from even a single flawed routing misconfiguration on the Global Internet Infrastructure. The paper located at this link: http://www.billslater.com/writing/2002_1107_Internet_Outage_and_Attacks_in_october_2002_by_William_Slater.pdf describes the events and results of what happened when a simple router misconfiguration at WorldCom on the East Coast of the United States led to a series of events that resulted in massive Internet services outages in October 2002. This debacle let to the denial of Internet service for over 40 million people. The root cause analysis of this unfortunate set of events led to improvements in quality controls for accuracy in entering Network Routing Policy Configurations, as well as a plan to increase the security of the Internet Domain Root Servers that existed at time on the Global Internet Infrastructure. In fact, in 2020, the security, reliability, and integrity of the complex global Internet Infrastructure is more important than ever because over 4.6 billion people use the Internet daily (https://www.internetworldstats.com/stats.htm), and 21st century workers and Internet Service consumers are more dependent on the Internet than ever due to events like the international COVID-19 Pandemic Crisis, and the increased universal needs for social distancing and teleworking. Quite simply put, as
described in the NASA Mission Control rescue of the Apollo 13 in April 1970, we now live in a world where “Failure is not an option”.

**What Is Blockchain and Why Is It Important?**

Blockchain is like a specialized Operating System that operates on top on Linux, Unix, and of Windows. It stores data in a distributed, decentralized ledger on a peer-to-peer network. All members of a given Blockchain network will have a consistent copy of the distributed ledger technology (DLT) data store. The data is stored in timestamped sequential “blocks” that are append-only, and each block contains the unique hash value of the block that preceded it. The idea of Blockchain was not exactly invented by Satoshi Nakamoto (Bitcoin inventor) but he popularized it in his 2009, 9-page paper about the creation of the digital currency known as Bitcoin. Below is a diagram from that paper:

![Blockchain Diagram](image-url)
In addition to hashing, Blockchain uses Public-Key Cryptography to secure the data in each block on the Blockchain DLT. Because of the way the Blockchain architecture works, new data can only be appended to the end of the Blockchain and there are no deletes of modifications allowed to the data. Data on Blockchain DLTs is said to be immutable because it cannot be changed. Two of the most common Blockchains, Bitcoin and Ethereum, are in Open Source Code and available on Github.

There are two types of Blockchain nodes on a peer-to-peer Blockchain network, clients and miners. Both of these are always supposed to have a current copy of the the DLT, but the miner nodes collect transaction data and assemble it into “blocks”. Blockchain is driven by a consensus protocol, which is a form of agreement. Two examples of consensus protocols are Proof of Work, and Proof of Stake.

Blockchain is important because it is being widely adopted for trusted computing, especially in the areas of supply chain management, financial industry, the legal industry, healthcare, business, education, and many other areas of the business world. In 2019, U.S. Congress introduced a Bill in July 2019, the Blockchain Promotion Act of 2019. Other key benefits are that Blockchain reduces risk of computer fraud, and this makes it a real business enabler.

**Note that Blockchain IS NOT Cryptocurrency, BUT Cryptocurrency uses Blockchain.**

The diagram below shows the comparison between a decentralized Blockchain Network and a Centralized Voting System Network.
How Can Blockchain Enhance Secure Global Routing?

Using Blockchain Distributed Ledger Technology to provide the storage of Network Routing Policy data in a Distributed Ledger that is both immutable and decentralized, will provide these advantages:

- Provide the important Network Routing Policy configuration data in the sequential, timestamped, immutable DLT data store.
- Create a history of Network Routing Policy configuration data that can be quickly accessed by any authorized engineer for troubleshooting purposes.
- Streamlining the efforts required to perform the current steps required for creating Network Routing Policy configuration.
• Have the possibility of providing this data or perhaps combining it for use with the other regional Internet Routing Registries.

Conclusion

Though this is an original idea for Secure Global Internet Routing Configuration with entering Network Router Policy information on an immutable, decentralized distributed ledger, this is not the first time that a Blockchain-based solution has been proposed to help secure the Internet Infrastructure. In July 2018, at Trinity College in Dublin, Ireland, Ms. Scarlett Gourley, a graduate student, and her Professor, Dr. Hitesh Tewari, co-authored their seminal study and paper on “Blockchain-based DNSSEC”. This paper is readily available for reference here at this link: https://www.researchgate.net/publication/326489781_Blockchain_Backed_DNSS EC.

The advantage of the proposed Blockchain DApp will be to provide rapid widespread secure access to immutable, decentralized data that will serve as an authoritative record of the time-stamped sequence of transactions made to update the Global Internet Infrastructure, and to document and provide a secure, decentralized single source of truth that can be used by multiple networking engineers and managers from geographically distributed locations to rapidly reconstruct Router Configurations related to Network Router Policy additions and changes (updates that supersede previously existing Network Router Policy data). Access to such data will help multiple technical stakeholders to rapidly collaborate to identify the Internet Infrastructure change history, and to pinpoint and hopefully resolve any possible errors that could result in outages and/or incorrectly routed Internet traffic.

It is unclear if the design ideas documented in my Project Blog will ever result in a real-life Ethereum Blockchain DApp that would be widely adopted by any or all of the IRRs, but the concepts discussed will serve to show the importance, viability, and advantages of such a solution.
Important Resources for Your Success

Internet Routing Resources

ARIN’s IRR User Guide
BGPStream by Cisco. https://bgpstream.com/
IRR Explorer - A remarkably handy tool for generating a dashboard of your current IRR status compared to what’s seen on BGP coming from your network
RFC2622 - “Routing Policy Specification Language (RPSL)” Describes the basic RPSL object syntax
RFC3704 - "Ingress Filtering For Multihomed Networks"
RFC4012 - “Routing Policy Specification Language next generation (RPSLng)” Describes useful additions to the RPSL language such as IPv6 route6 objects
RFC2650 - “Using RPSL in Practice”: A tutorial on generating RPSL objects
RFC7682 - “Considerations for Internet Routing Registries (IRRs) and Routing Policy Configuration: Some of the problems and lessons learned about the IRR system
RIPE’s Documentation on using PGP to authenticate mntner objects: In case you’d like to use more robust authentication.

Blockchain Resources

Several Presentations on Blockchain, Blockchain Security, and Blockchain Development: http://billslater.com/writing.
References


References


