Routing Security for Policymakers:
An Internet Society White Paper

October 2018

Although unseen to the average user, Internet Protocol (IP) routing underpins the Internet. By ensuring that packets[1] go where they are supposed to, routing[2] has a central role in the reliable function of the Internet. It ensures that emails reach the right recipients, e-commerce sites remain operational, and e-government services continue to serve citizens. The security of the global routing system is crucial to the Internet's continued growth and to safeguard the opportunities it provides for all users.

Every year, thousands of routing incidents[3] occur, each with the potential to harm user trust and handicap the Internet's potential.[4] These routing incidents can also create real economic harms. Key services may become unreachable, disrupting the ability of companies and users to participate in e-commerce.[5] Or packets may get diverted through malicious networks, providing an opportunity to spy on them.[6] While known security measures can address many of these routing incidents, misaligned incentives limit their use.

All stakeholders including policymakers, must take steps to strengthen the security of the global routing system.[7] This can only be done while also preserving the vital aspects of the routing system that have enabled the Internet to be so ubiquitous and improving their security. Through leading by example in their own networks, strengthening communication, and helping realign incentives to favor stronger security, policymakers can help improve the routing security ecosystem.

1 Network packets or "packets," are data sent over a network or networks.

2 Routing is the practice of determining the way to get data from one location to another location over a network or multiple networks.

3 Routing incidents are Border Gateway Protocol updates that have a negative impact.

4 https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

5 For example, in April 2017, a route leak caused a "large-scale internet disruption that slowed or blocked access to websites and online services for dozens of Japanese companies." https://bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

6 For several minutes in April of 2017, a network operator suspiciously hijacked the Internet traffic of several financial services. If intentional, the hijack could have been used to allow the network operator to read unencrypted financial information as it passed through its networks, or to attempt to decrypt encrypted financial information. https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/

7 While other forms of security (e.g. physical security or data security) are important for all stakeholders, including network operators, this policy brief is scoped to focus solely on improving routing security. For more information on securing the infrastructure of Internet service providers please see: https://www.rfc-editor.org/rfc/rfc3871.txt

Key Considerations

At its core, the routing system is built on trust among networks. The global routing system is a complex, decentralized system made up of tens of thousands of individual networks. Independent business decisions and trusted relationships between individual network operators implementing the Border Gateway Protocol (referred to as BGP in short) determine how the network operates.[8] The meshed system's architecture contributes to its resilience, scalability, and ease of adoption.

With no single point of failure or single controller, the routing system is difficult to break on a global level, easy to connect to and scales well. When a path becomes congested or fails, networks can choose to route traffic around the problem areas. The structure of the routing system also allows a great amount of flexibility for network operators to run their own networks. This allows network operators to develop novel network architectures and solutions to best fit the needs of their users. These qualities have made the Internet so successful and enabled its growth.

Challenges

While the routing system's qualities have enabled its overall success, these same attributes also contribute to some of its challenges. The system is based on chains of trust; each network relies on its neighboring networks (which in turn rely on their own neighbors, etc.) to act appropriately. There is no built-in verification and misrepresentation can be easy. This leads to ongoing **routing incidents**. The complexities and decentralization of the global routing system also bring **ecosystem challenges**, including misaligned incentives and externalized risks posed by routing insecurity. Solutions to address many routing incidents are known, but ecosystem challenges hamper their implementation. Any efforts to address these challenges must recognize the routing system's core technical functions and maintain the benefits provided by the routing system's architecture.

In 2017, there were close to 14,000 total routing incidents recorded.[9] Incidents affected over 10% of autonomous systems (AS's) on the Internet. There are three major types of routing incidents:

- **Route/prefix hijacking,** where a network operator or attacker impersonates another network operator, pretending that it is the correct path to the server or network being sought on the Internet.[10]

- **Route leaks,** are the propagation of routing announcements[11] beyond their intended scope (in violation of their policies).[12,13]

8 A *routing protocol* is the way in which a network determines the path a data packet is going to take. To route traffic between networks, most networks use the Border Gateway Protocol (BGP).

9 https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

10 In a route hijack, a network operator or attacker impersonates another network operator, pretending that it is the correct path to the server or network being sought on the Internet. This can cause packets to be forwarded to the wrong place, denial of service (DoS) attacks or traffic interception.

11 Networks make *announcements* to one another which detail the addresses reachable through or on their network or a customer's networks. Announcements help determine how routers decide to route traffic to a destination. *Announcement policies* determine what one network will announce to a neighbor.

12https://tools.ietf.org/html/rfc7908#section-2

13 For example, a network operator with more than one upstream provider announces to one upstream provider that is has a route to a destination through the other upstream provider (often due to accidental misconfiguration). Or a large network could unintentionally announce routes to all of its downstream networks. If malicious, a route leak can be used for traffic inspection and reconnaissance, or (often when accidental) can incur serious strain on infrastructure.

- **IP spoofing,** where someone creates IP packets with a false source IP address to hide the identity of the sender or impersonate another system.[14]

These incidents can create a serious strain on infrastructure, result in dropped traffic, provide the means for traffic inspection, or even be used to perform domain name server (DNS) amplification attacks,[15] or other reflective amplification (RA) attacks.[16]

Best practices in routing security are already available and are considered to be largely effective against these forms of routing incidents. For both route leaks and route hijacks, network operators can use stronger filtering policies[17] to determine when bad announcements are made by neighboring networks. IP source validation[18] can be used to find spoofed traffic as it moves to leave or enter a network. Spoofed traffic can then be filtered, preventing it from reaching its destination. There are ongoing efforts to develop even more effective tools, like Route Origin Validation (ROV),[19] and strengthen existing ones, like further defining a 'feasible path' in Unicast Reverse Path Forwarding (uRPF).[20]

The **Mutually Agreed Norms for Routing Security (MANRS)**[21] is a set of visible, baseline practices for network operators to improve the security of the global routing system. In 2014, a group of like-minded network operators developed MANRS as a voluntary initiative. It defines four simple but concrete actions for network operators to implement to greatly improve Internet security and reliability.[22] The first two improvements (filtering and IP source validation) address the root causes of common routing incidents. The second two, (coordination[23] and global validation[24]) help limit the impact of incidents and decrease the likelihood of future incidents.

Each of the MANRS actions prescribe outcomes, rather than specific methods. This allows implementation to change with technology. Alongside routing incidents, MANRS seeks to address ecosystem challenges in the global routing system. MANRS improves the economic incentives for routing security by allowing network operators to signal their routing security posture to customers, competitors and policymakers. It also provides metrics for measuring routing security. MANRS measurements can serve as a valuable 3rd party assessment of a network operator's security practices.[25]

Despite the availability of solutions to common routing incidents, ecosystem challenges limit their use.

---

14 In IP spoofing, someone creates IP packets with a false source IP address to hide the identity of the sender or impersonate another system. IP spoofing can be used to perform domain name server (DNS) amplification attacks.

15 A DNS amplification attack is executed by sending many requests to many DNS resolvers while spoofing the victim's IP address, an attacker can prompt many responses from the DNS resolvers to return to a target, while only using a single system to perform the attack.

16 https://www.us-cert.gov/ncas/alerts/TA14-017A

17 Each network determines what it will accept as an announcement from other networks, this is their *"filtering policy".*

18 IP source validation are techniques used to ensure that the IP address given by a packet came from a valid source address.

19 https://www.nccoe.nist.gov/sites/default/files/library/sp1800/sidr-piir-nist-sp1800-14-draft.pdf

20 https://tools.ietf.org/html/draft-sriram-opsec-urpf-improvements-03

21 https://www.manrs.org/

22 https://www.manrs.org/manrs/

23 Since routing incidents are best resolved close to their source, actions to improve coordination between network operators (which may be as simple as having publicly available and up to date contact information) is vital.

24 By publicly documenting their routing policy and what they intend to announce to external parties, others can validate their announcements.

25 An online portal for viewing these metrics, The MANRS Observatory, is in development and expected to be complete by the end of 2018.

- **Routing incidents are hard to address far from the source and must instead be addressed collectively.** Wherever a threat is coming from, the networks closest to its origin are best positioned to address the threat (e.g. adjacent networks can refuse to accept false announcements).[26] When a network is impacted further from the source of a routing incident, it can only attempt to mitigate the impact. It must rely on other networks closer to the source of the routing incident to fully address the problem.

- **Economic externalities.** Any network can be the source of an incident and the insecurity of one network can impact all other networks. However, even if a routing incident originates from one's own network, the impact is most likely to be felt on another network. Network operators are less likely to spend resources on better routing security since the benefits will mostly go to other networks, not their own.

- **Routing security is not a market differentiator.** Good routing security is currently not an effective marketing tool for network operators. It is difficult for network operators to communicate their level of routing security to their customers. Users have limited understanding of the global routing system and how their network's routing security practices will impact them.

Recommendations and Guiding Principles

Global collective action is the only way to address routing security threats and strengthen routing security. All stakeholders, including governments, have important roles to play in improving market incentives for better routing security, driving the development or adoption of best practices, and removing barriers and strengthening cooperation. However, any actions must be carefully crafted not to limit the strengths of the global routing system, including its overall resilience, ease of use, flexibility and scalability. To improve routing security, we should:

- **Lead by Example.** All stakeholders, including governments, should improve infrastructure reliability and security by adopting best practices in their own networks.

    - All networks providing internet connectivity, including enterprise or government networks, should use filtering, alongside IP source validation, to help prevent and mitigate the impact of incidents.

    - In addition, influential market players, such as large enterprises or governments, should, where feasible, require compliance with routing security baselines, such as the one documented by MANRS, for procurement contracts with Internet service providers. MANRS, through its MANRS Observatory, will provide measurements that can serve as a valuable 3rd party assessment of a network operator's security practices. These assessments can help inform procurement decisions.

- **Facilitate/encourage the adoption of common practices for routing security.** Industry associations, in close collaboration with governments and other stakeholders, should promote common baseline for routing security.

26 "In politics, such approach is called a Subsidiarity principle: Solutions should be defined and implemented by smallest, lowest or least centralized competent authority." https://www.internetsociety.org/collaborativesecurity/approach/#_ftnref5

  - Common baseline for network operators provide an industry standard for routing security and promote greater information sharing among network operators. They also provide a method for network operators to signal their level of security to prospective customers.

  - All stakeholders can contribute to the adoption and development of common baseline and industry practices for routing security by participating in the development process and, where feasible, through funding.

- **Support efforts to develop new, or strengthen existing, routing security tools.** To further improve the security of the global routing system partnerships with the research community could help develop the next generation of routing security tools and practices.

  - Where feasible, stakeholders, including governments and the private sector, can increase funding for research, development and experimental deployment of the next generation of Internet protocols, including those improving routing security.

  - Researchers can develop technical guidance on performing IP source validation, effective filtering, and global validation. Guidance should also encourage network operators to implement BGPSec[27] and RPKI.[28]

- **Encourage the use of security as a competitive differentiator.** To make routing security a competitive differentiator, stakeholders should support public awareness of the importance of routing security and encourage improved signaling of routing security between industry and customers.

  - For Internet service providers, routing security is a core component of their overall security posture. Signaling their attitude towards routing security reflects strongly on their overall posture, which can differentiate their services from competition.

  - Enterprises will pay more for better routing security, however they need ways to determine good routing security from bad routing security. In a 2017 survey, 94% of enterprises indicated that they would be willing to pay more for a vendor who was a MANRS member in a competitive situation.[29] The same research also found that awareness of MANRS was marginal among enterprises before the survey.

  - Industry, consumer groups, governments and other stakeholders should work together to promote the use of routing security baselines, such as MANRS, as a competitive differentiator. [30] In addition, they should support efforts to educate local enterprises about routing security and existing best practices.

---

27 BGPSec is an extension to the Border Gateway Protocol (BGP) that provides security for the path of Autonomous Systems (ASes) through which a BGP update message passes. https://tools.ietf.org/html/rfc8205

28 "With RPKI, Resource Public Key Infrastructure, Border Gateway Protocol (BGP) route announcements that are issued from a router are validated to make sure that the route is coming from the resource holder and that it is a valid route." https://www.arin.net/resources/rpki/

29 MANRS Project Study Report. 451 Research. https://www.routingmanifesto.org/wp-content/uploads/sites/14/2017/10/MANRS-451-Study-Report.pdf

30 MANRS, as a visible set of best practices and through its public measurements provided through the MANRS Observatory, has the potential to be a powerful marketing tool for Internet service providers.

- **Strengthen communication and cooperation between network operators and other stakeholders.** Stakeholders should support the development of better mechanisms for information sharing, engage in information sharing on routing security, and collaborate with stakeholders to address routing security threats.

    - The private sector, governments, civil society, academia and others can support the development or strengthen existing computer security incident response teams (CSIRTs). CSIRTs provide an important role in information sharing and coordination in response to routing incidents and threats.

- **Identify and address legal barriers to information sharing, the implementation of routing security technologies and research on routing incidents and threats.** Legal barriers can impede security researchers and disincentivize network operators from deploying routing security solutions and sharing information with one another.

    - Identifying and eliminating legal and regulatory barriers can improve information sharing and responses to routing incidents. Stakeholders, particularly security researchers, may worry that disclosing routing security incidents or threats could place them in legal jeopardy. Legal barriers can also impede the development and deployment of routing security technologies. In developing solutions to identified barriers, stakeholders must pay close attention to their potential impact on the privacy of individuals.

Conclusion

The global routing system is incredibly resilient. Its decentralized structure provides flexibility, scalability, and overall durability. While its structure has played a crucial role in the growth of the Internet, it has also enabled routing incidents to occur.

Best practices, like the Mutually Agreed Norms for Routing Security, provide a clear path for network operators to take towards addressing these routing threats. However, all stakeholders, need to take actions to address the ecosystem challenges preventing the widespread application of best practices. Only through collective action, can we address the challenges of routing security while maintaining the benefits of a decentralized routing system.