Policy Brief: Routing Security

Although unseen to the average user, Internet Protocol (IP) routing underpins the Internet. By ensuring that Internet packets go where they are supposed to, routing[1] has a central role in the smooth 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 its opportunities for all users.

Every year, thousands of routing incidents occur, each with the potential to harm user trust and handicap the Internet's potential.[2] These routing incidents also create real economic harm. Key services may become unreachable, disrupting the ability of companies and users to participate in e-commerce. 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. This can only be done by 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.

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 (commonly referred to as BGP in short) determine how the network works.[3] The meshed system's architecture contributes to its resilience, scalability, and ease of adoption.

---

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

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

[3] 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).

As there is no single point of failure, the global routing system is difficult to break. And with no single controller, the system is easy to connect to and to scale. 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. As the system is based on trust, there is no built in verification and misrepresentation can be easy, leading to ongoing **routing incidents**, both small and large. The complexities and decentralization of the global routing system also bring **ecosystem challenges**, including misaligned incentives and externalities posed by routing insecurity. Solutions to address routing incidents are well-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 immense benefits provided by the routing system's architecture.

In 2017, there were close to 14,000 total routing incidents recorded.[4] 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;[5]
- **Route leaks,** where 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);[6] and

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

[5] 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.

[6] In a route leak, 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

- **IP spoofing,** where someone creates IP packets with a false source IP address to hide the identity of the sender or impersonate another system. [7]

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.[8]

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[9] to determine when bad announcements[10] are made by neighboring networks. IP source validation[11] 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.

The **Mutually Agreed Norms for Routing Security (MANRS)**[12] 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.[13] The first two improvements (filtering and IP source validation) address the root causes of common

misconfiguration). This can be used for traffic inspection and reconnaissance, or incur serious strain on infrastructure.

[7] 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.

[8] 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.

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

[10] 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.

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

[12] https://www.manrs.org/

[13] https://www.manrs.org/manrs/

routing incidents. The second two, (coordination[14] and global validation[15]) help limit the impact of incidents and decrease the likelihood of future incidents.

Each of these 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.[16]

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

- **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). 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 impacts 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.

[14] 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.

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

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

- **Routing security is not a market differentiator.** Good routing security is 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 to strengthen the level of routing security is the only way to address routing security threats. Governments and policymakers have an important role 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. Governments and policymakers should:

- **Lead by Example.** Governments should improve infrastructure reliability and security by adopting best practices in their own networks.
    - Government networks providing internet connectivity should use filtering, alongside IP source validation, to help prevent and mitigate the impact of incidents. In addition, compliance with routing security baselines, such as the one documented by MANRS, should be a requirement for government 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 government procurement decisions.

- **Facilitate/encourage the adoption of best practices for routing security.** Governments should encourage industry associations to develop, or strengthen and promote existing voluntary codes of conduct for network operators.
    - Voluntary codes of conduct for network operators provide an industry standard for routing security and promote greater information sharing among network operators.[17] They also provide a method for network

[17] Australia's *Internet Service Providers (ISP) Voluntary Code of Practice for Industry Self-Regulation in the Area of Cyber Security* (2010) was funded by the Australian Government, while development was led by

operators to signal their level of security to prospective customers. However, new network operators may be unable to allocate the resources or have the experience necessary to quickly meet industry standards for routing security. Therefore codes of conduct must be voluntary to ensure barriers to entry for network operators are not increased.

- Governments can support the development of national network operator codes of conduct as participants in the development process and through funding.

- **Security as a competitive differentiator.** To make routing security a competitive differentiator, governments should support public awareness of the importance of routing security and encourage industry to better convey routing security to their 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 recent 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.[18] The same research also found that awareness of MANRS was marginal among enterprises before the survey.
  - Governments should work with industry, consumer groups and other stakeholders to promote the use of routing security baselines, such as MANRS, as a competitive differentiator. [19] In addition, governments

---

the Internet Industry Association of Australia. As of 2013, there are "34 ISP signatories to the [Code of Practice], representing approximately 90% of Australian home internet users." (https://www.communications.gov.au/sites/g/files/net301/f/icode-Review-Report_.pdf). The Mutually Agreed Norms for Routing Security can serve as both a baseline set of best practices and as a foundation to complimentary voluntary codes of conduct for network operators.

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

[19] 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.

should support efforts to educate local enterprises about routing security and existing best practices.

- **Strengthen communication and cooperation between network operators and other stakeholders.** Governments 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.
    - Governments 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.

- **Work with the private sector and civil society to identify and address legal barriers to information sharing and research on routing incidents and threats.** Legal barriers can impede security researchers and disincentivize network operators from sharing information with one another.
    - Identifying and eliminating legal and regulatory barriers can improve information sharing and responses to routing incidents. Stakeholders, in particular security researchers, may worry that disclosing routing security incidents or threats could place them in legal jeopardy. In developing solutions to identified barriers, governments should 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, including governments, 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.