Resilience of the commons: routing security

Andrei Robachevsky

robachevsky@isoc.org

Internet Society

Security of the global Internet routing infrastructure is to some extent no one's concern and everyone's concern at the same time. How can improvements be stimulated in this area – an area, where traditional market forces, the main drivers of the development of the Internet, do not work, where regulation may not be effective, where one's actions may benefit competitors more than one's own customers?

Technology building blocks and solutions are one aspect, but people are what ultimately holds the Internet together. The Internet development has been based on voluntary cooperation and collaboration and we believe that is still one of the essential factors of its prosperity.

Internet history contains examples of such cooperation and its efficacy. A prime example is the Conficker Working Group[1], created to fight the Internet borne attack carried out by malicious software known as Conficker. A multitude of regional and national network operators groups (NOGs) and their role is resolving operational problems, often spanning multiple networks, is another example.

In this paper we seek to motivate an approach to tackle a difficult collective action problem based on our work with the impacted community of network operators. Our approach is focused on building consensus around an understanding of the problem space, shared understanding of the potential offered by different solutions, building a culture of collective responsibility based on an understanding of collective and individual benefits, and focusing on a positive end goal.

Global inter-domain routing

The Internet infrastructure is made up of tens of thousands of independently owned, managed and operated networks that interconnect with one another in a sparse mesh. The interconnection between these networks is generally shaped by economic factors and comes in one of two basic forms, either transit or peering. Transit links are most common at the edge of the network where one network pays another for access to 'the Internet'. In this case the transit provider routes traffic destined to and received from all other Internet hosts. On the other hand, peering links allow networks to exchange traffic destined for each other, but nowhere else. Peering provides network operators with a way to reduce the amount of traffic for which they have to buy[2].

Networks exchange reachability information about other networks, or IP-address prefixes, among each other. The wide-area routing protocol, used to exchange reachability information in the Internet is BGP (Border Gateway Protocol, Version 4)[3].

[1] Conficker Working group, http://www.confickerworkinggroup.org/wiki/

[2] An Introduction to Internet Interconnection Concepts and Actors. Briefing Paper, Internet Society, http://www.internetsociety.org/introduction-internet-interconnection, 2009

[3] A Border Gateway Protocol 4 (BGP-4). RFC4271, http://tools.ietf.org/html/rfc4271

To be more precise, this reachability information is exchanged between so-called autonomous systems (ASes) that comprise the global routing infrastructure. An AS is administered by a single entity, and implements a set of policies in deciding how to route its packets to the rest of the Internet, and what reachability information to send to other ASes. Such a set of policies is often called an AS routing policy. Routing policies vary among ASes, but are based on the same principles: hot-potato routing[4], preference of customer routes, "valley-free" routing[5]. In practice it is only partly possible to infer the exact policies an AS uses, as only the outcomes of the decision are communicated in the form of routes exported to neighboring ASes, and not the complete decision process itself.

A routing policy is defined and implemented by an AS independently, and has only local significance as there is little way for the AS to control how its intent is handled by other networks. For example, it has been shown that interaction of independently implemented policies may lead to policy disputes and cause BGP to oscillate indefinitely[6,7]. The valley-free routing rule is often violated, for instance by customers beginning to provide transit to their providers or peering networks becoming transit providers for their peers[8]. This type of policy violation is sometimes called a "route leak". A "route hijack", when an AS accidentally or maliciously announces a prefix belonging to another AS, is yet another example of violation of routing policy.

Routing policy violations may not only affect service availability, but also confidentiality and integrity of communications, opening them up to man-in-the-middle (MITM) attacks.

It is worth mentioning in this context that sending reachability information to a neighbor indicates an AS commitment to pass traffic to that destination. Cases when this assumption is violated cause "black-holing" of the traffic – a sort of a denial of service attack.

To a great degree routing between ASes is based on trust, assuming that a neighbor is doing the right thing, and varying levels of policy checks that rarely go beyond the immediate neighbors of an AS.

One of the Internet Commons

The Internet global infrastructure, its "core", is frequently compared with the commons, especially in the context of the "tragedy of the commons". Indeed driven to a great extent by economic incentives there is a tendency for individual organizations to neglect the characteristic properties of the interconnecting core that we all ultimately depend on.

This analogy limps, of course. As there is no core in the Internet, there is no commons - the "Internet commons" is a collection of other networks or resources that are not ours, that we do depend on, but do not control. Our network and our resources are also part of the commons, just not from our own perspective.

When analyzing the efficacy of various approaches that facilitate improvements in the area of routing security we found it useful to look at the global inter-domain routing through the prism of the concept of the commons.

---

[4] http://en.wikipedia.org/wiki/Hot-potato_and_cold-potato_routing

[5] Valley-Free rule is defined as follows: after traversing a provider-to-customer or peer-to-peer edge, the AS path cannot traverse a customer-to-provider or peer-to-peer edge.

[6] K. Varadhan, R. Govindan, and D. Estrin, "Persistent route oscillations in Inter-domain routing," Computer Networks, 32:1-16, 2000

[7] T. Griffin, F. Shepherd, and G. Wilfong, "The stable paths problem and Inter-domain routing," IEEE/ACM Trans. Networking, 10:232-243, 2002

[8] V. Giotsas, S. Zhou. "Valley-free violation in Internet routing - Analysis based on BGP Community data, " IEEE ICC, 2012.

The commons or, more precisely, a common pool resource (CPR), in this case is a globally distributed BGP routing database, which contain reachability information of all IP-address prefixes, or networks. The database content is compiled and distributed using BGP, with networks (or ASes) passing select (i.e. conforming to their policy rules) reachability records to their neighbors and every network compiling their own copy of the database, again shaped by the routing policy rules. This way the global routing database is replicated and is only loosely consistent as every AS maintains its own more or less complete copy of the database, modified by its own routing policy rules.

So what is the main threat to the BGP commons that leads to its deterioration? The main threat comes from actions (or absence of actions) of network operators that can generally be characterized as pollution.

One of the cases of such pollution is when redundant information is injected and propagated. For instance, the announcement of more specific prefixes for a destination when a covering prefix, an aggregate, exists. A CIDR report[9] shows that for some ASes more than 90% of the information they contribute to the global BGP database is redundant and can be cleaned up. Overall, the size of the global routing table can be reduced by 42%. This type of pollution puts the burden of maintaining a bigger than necessary database on all ISPs, and may result in degrading the performance of the global system in terms of the BGP convergence time.

Another type of pollution, which is directly related to the scope of the activities of the Internet Society, is the injection and propagation of incorrect information. This information ranges from asserting reachability that doesn't exist (prefix hijack), or that contradicts the intent of another ISP (e.g. route leaks).

As with any other type of the commons, investing in it is problematic, as individual costs by far outweigh individual benefits, unless everyone, or at least a critical mass, participates. In the area of routing we observe a situation where participating networks are reluctant to invest in the maintenance of the commons – sanitizing own input, cleaning up and not further propagating incorrect reachability information. Needless to say, such events cause routing disruptions and may result in service outages of different scales and security impacts.

In his "The Tragedy of the Commons"[10] Garrett Hardin wrote:"[T]he commons […] is justifiable only under conditions of low-population density. As the human population has increased, the commons has had to be abandoned in one aspect after another". If we continue to extend this concept to the inter-domain routing system, the future looks bleak.

The problem is aggravated by the fact that many attempts to apply technology and technical solutions alone have met with mixed success. As Ross Anderson argued in his paper "Why Information Security is Hard", contrary to one common view that information security comes down to technical measures, "[m]any of the problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons."[11]

What is the way out?

Hardin offers two main solutions. The tragedy of the commons can be averted by turning it into private property, or by the introduction of "coercive laws or taxing devices that make it cheaper for the polluter to treat his pollutants than to discharge them untreated"[10]. He also notes that both solutions haven't worked well, especially in this particular case: the concept of private property "favors pollution" and laws are always behind the times and require "elaborate stitching and fitting" to adapt them to new circumstances. We could add that governmental regulation of the Internet commons is especially difficult due to its global and cross-border nature.

[9] http://www.cidr-report.org

[10] Hardin, G. "The Tragedy of the Commons". Science 162 (3859): 1243–1248, 1968.

[11] Anderson, R. "Why Information Security is Hard - An Economic Perspective". Proceedings of the 17th Annual Computer Security Applications Conference, 2001.

However, Elinor Ostrom in her work "Revisiting the Commons: Local Lessons, Global Challenges"[12] suggests that there might be other ways to get out of the seeming inevitability of commons degradation. Through empirical studies she demonstrated that community-driven, bottom-up self-regulation may yield better and more effective results. We note that the model of bottom-up self regulation worked exceptionally well as a governance model for many important Internet areas – from the development of open standards to the distribution of Internet number resources – IP address blocks and AS numbers.

While technology is certainly an essential component in supporting Internet routing security, and laws and compliance requirements when applied appropriately can stimulate improvements, an approach based on collective responsibility and self-regulation seems to be most able to produce good and lasting results in this case, too. But for this several conditions have to be met.

Prerequisites

Back in 2009 the Internet Society started systematically looking at ways to foster improvements in security and resiliency of the Internet routing system. Initially our work was aimed at the promotion of the existing best operational practices and technologies that are being developed in the Internet Engineering Task Force (IETF), but we soon realized that technology is only one aspect and that even more challenging issues lie in the social and business planes. What are the drivers that will ultimately get these technologies deployed and used? What are the missing pieces that can help in fostering the improvements?

These were the underlying questions that formed agendas of several meetings that the Internet Society organized with network operators and researchers: Operator Roundtables on Routing Security[13,14] and a Routing Resiliency Measurements Workshop[15].

The objectives of these events varied but the overarching goal was to bring people that run networks and make decisions on the ground together and start an open dialog about issues related to routing security and resilience in order to develop a common understanding of what good looks like and what adequate responses could be instigated in the spirit of collective responsibility.

Through these discussions the challenges of routing security were better understood. The issues and associated challenges and opportunities fall into four main areas. In our opinion, making progress in each of these areas is a prerequisite for a positive impact:

1. Common understanding of the problem
2. Common understanding of solutions
3. Understanding of common and individual benefits
4. Ability to assess risks

In the rest of the paper we will discuss the challenges and opportunities related to these areas in more detail.

---

[12] E. Ostrom, et.al. "Revisiting the Commons: Local Lessons, Global Challenges", Science 284 (5412): pp. 278–282, 1999.

[13] http://www.internetsociety.org/routing-security-report-2nd-internet-society-operator-roundtable

[14] http://www.internetsociety.org/routing-security-report-3rd-internet-society-operator-roundtable

[15] http://www.internetsociety.org/doc/report-routing-resiliency-measurements-workshop

Common understanding of the problem

Can we agree on a problem (or a set of problems) that we, as operators and as a technical community, collectively need to solve? Earlier in the paper we mentioned that in inter-domain routing the ISP policy only has local significance. If we define routing policy as the desired way packets from source A, passing intermediate networks, reach destination B, then routing resilience is the ability to resist deviation from that routing policy, and is the ultimate goal. Subsequently, lack thereof is the ultimate routing problem. In one of our roundtable meetings[13] participants named network stability, resilience and performance as the main priorities for operators. Security is important to the extent it helps in reaching these goals.

One set of routing security problems is directly related to vulnerabilities of the inter-domain routing protocol - BGP. Faulty, misconfigured, or deliberately malicious sources can disrupt overall Internet behavior by injecting bogus routing information into the BGP-distributed routing database (by modifying, forging, or replaying BGP packets). These vulnerabilities are well understood and documented[16]. Some high-profile examples of exploits of these vulnerabilities are the hijacking of the YouTube prefix[17] and China's deflection of the Internet traffic[18].

There are, however, problems beyond vulnerabilities of BGP that are related to limitations of the protocol itself. One of them is a route leak. Another set of problems that may affect routing comes from the way BGP handles malformed attributes. For example, attendees of one of the Operator Roundtables perceived it as one of the most important problems that can seriously impact network resilience[13].

Coming back to the initial question, there is a general agreement about the abovementioned problems. At the same time there is a wide range of opinions regarding their severity and priority of their resolution.

Common understanding of solutions

The challenge here is there is a whole array of possible solutions and each of them solves only part, or one set of the problems. For example, there is work underway in the Secure Inter-Domain Routing (SIDR) WG in the IETF aimed at hardening BGP security and fixing its vulnerabilities[19]. Even if fully deployed, this solution allows for certain violations of the routing policy. For example, it does not protect against route leaks that present a significant threat to security and stability of a network. Also, this technology relies on a significantly populated and well-maintained RPKI (Resource Public Key Infrastructure) repository, containing digitally signed assertions of what legitimate routes are[20].

Another set of solutions focuses on "securing the borders" of an ISP resulting in the increased scrutiny on what routes the ISP gets from its neighbors. In practice, this approach is mostly applied to an ISP's direct customers, where it is easier to define what networks belong to a customer and what routes can be legitimately announced. Extending this approach beyond one's own customers is difficult mainly due to lack of reliable data about legitimate routes[14].

In all these solutions there is a challenge that the execution of an ISP routing policy on a global scale, outside own network depends on third parties – other ISPs, several hops away, which makes it impossible to fully enforce. It also depends on information from third parties – network's peers and customers, which is difficult or cumbersome to validate[13].

---

[16] S. Murphy. "BGP Security Vulnerabilities Analysis", RFC4272, http://datatracker.ietf.org/doc/rfc4272.txt.

[17] "YouTube Hijacking: A RIPE NCC RIS case study ", http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study, RIPE NCC, 2008.

[18] J. Cowie. "China's 18-Minute Mystery", http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml, Renesys Blog, 2010

[19] http://datatracker.ietf.org/wg/sidr/charter/

[20] M. Lepinski, S. Kent. "An Infrastructure to Support Secure Internet Routing", RFC6480, http://datatracker.ietf.org/doc/rfc6480/

There is also another dimension of the solution space: proactive vs. reactive. The two sets of solutions described above belong to the first category. They are aimed at preventing incidents from happening. Reactive measures come into play when "bad things" happen and their effectiveness depends on the availability of detection and monitoring tools as well as disaster recovery planning, an important component of which is the personal network among network operators. An active operators community facilitates communication and faster resolution of incidents. For example, NANOG (http://www.nanog.org/mailinglist/) and Outages (http://puck.nether.net/mailman/listinfo/outages) mailing lists are frequently used by network operators to report problems, as was shown at the Routing Resiliency Measurements Workshop[15].

None of these approaches provide a full solution to the routing-related problems. They are just building blocks that can be used in building an ISP's own solution. These building blocks vary in the costs and the benefits they bring to an ISP individually and the common good of the global routing infrastructure. Understanding these factors and how they are aligned with the business objectives of network operators is crucial for sustained improvements in routing security.

Understanding of common and individual benefits

It is important that people making decisions and running networks agree on what good looks like. It is an inverse of, and is tightly related to the problem space. But instead of forcing us to look for solutions, sets a positive common goal.

In the context of the commons analogy we want pollution to be minimized. Pollution of the routing system, and in particular injecting and propagating incorrect routing paths affects routing resiliency and is a security risk.

Understanding this and agreeing within the operational community is very important as it sets the foundation for a cultural change.

Individual actions, based on some of the mentioned building blocks, contribute to this goal, although the degree of contribution varies. The benefit of the action to the individual operator will also vary.

For example, applying extra scrutiny to routing announcements received from a customer provides direct benefits to the ISP, preventing, for instance a "transformation" of a customer into a provider of transit. These actions might be easier to justify with a business case. And it also somewhat improves the hygiene of the overall routing system.

On another hand, theoretically, the ability of a large transit provider to prevent pollution is much higher. But the costs are also higher and it is difficult to find a business case to justify the expenses. Also, effectiveness of this ability is constrained by lack of trusted data.

Focusing on cases that have business utility and yet contribute to the overall goal seems to be a sensible approach.

Ability to assess risks

"Unmaintained" routing commons is a risk to the global Internet ecosystem. Its potential ranges from disrupting traffic flow, resulting in a DoS attack, to eavesdropping of traffic and mounting MITM attacks for immediate impact or as a preparatory phase for future attacks.

Nonetheless, the global routing system worked reasonably well so far. Research data shows a relatively small, on the order of tens, number of incidents – routing misconfigurations that propagate globally – annually, which corresponds to operators experience. At the same time it is unclear how much goes unnoticed. There is a lack of agreement on metrics that can represent the resiliency of the global routing system, and no systematic long-term monitoring or measurement. Coming back to the analogy of the commons, this means that the commons "capacity" is unknown and we don't know how much of it has already been exhausted.

One of the conclusions of the Routing Resiliency Measurements Workshop[15] was that network operators lack factual data and a good understanding of what is going on in the ecosystem outside their own networks. A mini-survey that the Internet Society conducted showed that many operators do not even know how many incidents affect their network as they have no

capability to detect, and their NOCs don't classify the tickets in a way that would allow for such analysis.

But this is essential information, needed for a risk assessment and a selection of adequate tools and approaches. It is also important to measure the effect of such tools once they are deployed and monitor the changing dynamics of the environment. And because the inter-domain routing system is globally interdependent, such monitoring and measurements should be long-term and be done on a global scale.

Building critical mass through strengthening of collaboration and communication

Speaking about the four areas of impact, one cannot assume universal agreement of the underlying issues, or a coherent plan of action adopted globally. But, as Ostrom noted, "[u]sers of a CPR include (i) those who always behave in a narrow, selfinterested way and never cooperate in dilemma situations (free-riders); (ii) those who are unwilling to cooperate with others unless assured that they will not be exploited by freeriders; **(iii) those who are willing to initiate reciprocal cooperation in the hopes that others will return their trust (**emph. mine**)**; and (iv) perhaps a few genuine altruists who always try to achieve higher returns for a group[12]."

In her work, Ostrom demonstrated that the ability to communicate, sanction one another, or make new rules, is essential to overcome the tragedy of the commons. The good news is that the essential ingredients necessary for sustained improvements in the area of routing security exist.

One of the drivers of improvements is the culture of intolerance towards "routing pollution". Communication and collaboration play an important role here. They help create peer pressure, or, as Garrett Hardin named it, "mutual coercion, mutually agreed by the majority of the people affected"[10]. Collaborative responsibility and open communication lines are also crucial for effective response and reactive measures to mitigate routing security incidents.

A community is the place where communication happens and rules are agreed upon. There are numerous operator communities of a national and regional scale. Some of the examples of regional ones are NANOG, RIPE, LACNOG.

There are processes for the development and modification of the rules. These are commonly called Best Operational Practices, and may be developed by an operator's community, or other bodies, for example IETF.

Extra scrutiny and filtering out of incorrect routing announcements is one of the sanctions that operators apply following BCPs. Another common sanction is terminating a BGP session with a neighboring network if the number of prefixes received exceeds a certain threshold.

If group (iii) is big enough and is able to grow the impacts will be amplified. So the goal is to reach a common understanding of the challenge and possible actions in group (iii) (and (iv)) and build critical mass by growing this group in size.

Security in general is a difficult area when it comes to searching for incentives. Security of the global Internet Infrastructure, be it DNS or routing, brings additional challenges: the utility of security measures depends on actions of many other parties. Technology solutions are an essential element here, but technology alone is not sufficient. In order to expect visible improvements in this area there must be a better articulation of the problem in terms of risks, based on metrics and trends, and, more importantly, a cultural change promoting collective responsibility. These areas are the main focus of the program of routing security of the Internet Society.