From routing security to secure routing

Report on 3rd Operator Roundtable on Routing Security

31 May 2012, ISOC office, Reston, USA

Introduction

Network operator's business is heavily dependent on the stability and performance of the global routing system. The critical element of the interdomain routing is BGP - a single inter-domain routing protocol that has provided interdomain routing services for the Internet's disparate component networks since the late 1980's. One of the major concerns related to BGP is its lack of effective security measures, and as a result the routing infrastructure of the Internet is vulnerable to various forms of attack.

The issue of routing security was an object of constant attention by the industry for more than a decade. A set of best practices has been developed. Several technology components and systems have been developed and used with varying level of success. Development of new technologies and solutions is underway. Yet the proliferation of these best practices, technologies and their integration with the ISP provisioning infrastructure has been slow and having little effect on the state of the global routing security.

One of the challenges is that if used by an ISP in isolation these measures bring relatively little benefits. On the opposite, if being deployed in collaborative manner they can reach the critical mass and open the real potential.

The participants were invited to discuss concrete steps and measures that should be taken for incremental improvements in the security of inter-domain routing. The main focus was on the existing best practices and approaches, including securing the network boundary interfacing customers and peers, which provide a foundation for future deployment of technologies being developed by the IETF.

Agenda

1. Welcome, introductions and goal setting
2. Brief overview of the problem space and existing best practices, focus on BGP security
3. Roundtable discussion of security problems pertaining to interdomain routing
4. Roundtable discussion of best practices and possible solutions
5. Roundtable discussion of possible solutions

Discussion

The roundtable meeting consisted of three discussions sessions, preceded with an overview of the problem space and best practices in the area of routing security.

Discussion of security problems pertaining to inter-domain routing

When discussing BGP vulnerabilities two additional classes were mentioned in addition to the ones discussed in RFC4272: policy violations, valid from a protocol point of view; and invalid (malformed) attributes. Both present security risks. The latter presents an interesting dilemma: whether an operator only accepts known good BGP attributes from peers and/or customers in order to protect the protocol better, or whether they pass such attributes along because it becomes more difficult for the Internet as a whole to innovate (roll out new attributes). Getting vendors to handle unknown attributes more gracefully is really hard.

The participants agreed that security problems in this space exist, but it is hard to quantify them beyond a few high-profile cases and anecdotal evidence. There is absence of longitudinal study on frequency and types of BGP attacks, making it impossible to separate threats from risks. In opinion of the participants such data and its analysis could provide vital information for creating a more founded business case for operators as well as inform a range of solutions that will apply depending on the range of threats and the relative importance of the infrastructure being protected. Also, there is no trend analysis - are things getting better or worse, and where? Would be great to be able to do that as well as able to classify types of attack, and what parties were impacted, geographies, targets, ISPs.

It was noted that getting empirical data is challenging - the intent is unknown in many cases, data is incomplete, not always clear what to look for. There were several suggestions on how/where additional data can be collected:

- Centrally collecting anonymized NOC reports of events related to BGP security - e.g. route hijacks. Need to agree on classification of events, actual data collected, issues related to privacy and confidentiality as well as who can play a role of the collector (Internet Society was suggested as a possible clearinghouse).
- Getting data from services like BGPmon, MyASN, etc., that can give us data on number of alerts (i.e. when documented intent differed from the observed reality via RouteViews and RIS).

Some of the participants proposed that we look at threats and related risks from a business relationship point of view. Whether there is a business relationship with the entity experiencing or causing problems will determine certain types of solutions, their efficacy, reaction times, etc.

It was acknowledged that the governments are increasingly concerned with BGP vulnerabilities and a perceived state of security of the global routing system. Lack of demonstrated positive improvements taken collectively by ISPs only contributes to these concerns.
Participants agreed that the quality of registration data is important for establishing the truth as well as for reducing the reaction time when dealing with incidents (contact data) and needs to be improved. Many acknowledged that also data pertaining to their own networks could be improved.

Discussion of best practices and possible solutions

The following classes of best practices were discussed:

a) Session protection

Usually not a big issue (low volume sessions), neighbors that consider this a security issue are protected (this amounts up to 10%)

b) Maximum prefixes on a peering

Most participants apply this recommendation. Some consider this to be an effective protection on customer links, even if only this recommendation is applied. This is a low hanging fruit.

c) Prefix filtering with customers

Most participants apply this recommendation. The data is usually received from a customer and rarely validated. This is considered as adequate protection against misconfiguration.

d) Prefix filtering with peers

No one of participants applies filtering on session with Peers beyond static filters. This is considered unnecessary, since peering implies a trusted relationship. Also, risks of incorrect filtering are perceived bigger than the ones from received "garbage" from a peer. Another reason that was mentioned is that the reaction time to the latter events may be much shorter than to filtering misconfiguration.

e) Detection, coordination and reaction

Some of the participants considered this set of practices as important as the other ones. Moreover, reactive actions might be much more effective (and less costly) when dealing with certain type of events. Unfortunately this set of practices is much less documented and formalized.

f) Keeping “whois” data clean and up to date

Many agreed that accuracy of whois data is important and should be improved, increasing responsibility of the data “owners” (e.g. network operators) for supplying correct information.

Discussion of concrete actions and coordination activities

When discussing further improvements most of the participants felt that they already perform adequate protection and although improvements are always possible, closing the loop completely will cost disproportionally more. It was also felt that they were in minority and that majority of the Internet networks doesn't follow these practices.

Education and stimulating the network operators, and also making it easier to adopt the BCPs was considered an important direction. It was suggested that the Internet Society Deploy 360 program might be a locus of such activities.

Sharing of data was another avenue that people thought should be explored. That should improve coordination and result in better reaction times, more effective reactive approaches, provide empirical data.

The idea of creating "safe islands" and providing incentives to other to join by building a critical mass of a culture of security needs further elaboration and discussion.

Attendees

- Shane Amante, Level3
- Wes George, TW Cable
- Ted Seely, Sprint
- Heather Schiller, Verizon
- Duncan Sparrel, AT&T

- Leslies Daigle, Internet Society
- Matthew Ford, Internet Society
- Phil Roberts, Internet Society
- Andrei Robachevsky, Internet Society