Poster: Resilience of the Internet: the Case of the BGP Backbone

Sylvain Frey, Awais Rashid, Yehia Elkhatib, Karolina Follis,
John Vidler, Nick Race, Chris Edwards
Lancaster University
{s.frey,a.rashid,y.elkhatib,k.follis,j.vidler,n.race,c.edwards}@lancaster.ac.uk

***Abstract*—The Internet has become a critical infrastructure. This multi-disciplinary study evaluates the resilience of one of its cornerstone assets: the Border Gateway Protocol (BGP) infrastructure, that constitutes the backbone of the network of networks. The study combines three complementary approaches: a Systematic Literature Review (SLR) established an exhaustive threat model for BGP systems; a qualitative analysis, based on a series of interviews with major stakeholders of the Internet, identified key specificities of the operation and governance of backbone networks; and large scale attacks were simulated based on a detailed study of the logical and physical topologies of the backbone. Our first conclusions challenge the idea that the Internet's built-in resilience guarantees against large-scale failures: important changes in the way the backbone is operated and governed may be necessary to address new threats arising in a near future.**

I. Goals and Approaches

In this study, we assess the current state, governance and management model of BGP infrastructures. We evaluate the resilience capabilities of these infrastructures during hypothetical major security events, assess existing protection and recovery solutions and investigate technical and policy improvements.

Our analysis is based on three complementary approaches:

- We conducted a Systematic Literature Review (SLR) [1] on the topic and we established an exhaustive threat model for BGP systems.
- We conducted a series of interviews with major Internet stakeholders, to grasp their perception of the backbone and identify the key specificities of the operation and governance of such a *system of systems*.
- We studied the physical and logical infrastructure through different public data sources and constructed several complementary models of its topology. We simulated several attack scenarios inspired from the threat model we established, and determined that large-scale disruptions of the backbone are possible.

II. Overview of the Backbone

BGP is the highest-level routing protocol, used to route traffic between major Internet networks: international carriers, Internet Service Providers (ISP), hosting platforms, cloud providers, Content Delivery Networks (CDN) and so on. These networks – called Autonomous Systems (AS) – exchange routing information via BGP by advertising IP prefixes (e.g. "1.2.[0-255].[0.255]") identifying the range of public IPs in a given AS. Routing information is propagated between neighbouring ASes by building AS paths via a gossip-like propagation – e.g. AS1 advertises its own prefix, its neighbour AS2 advertises the same prefix with path AS2→ AS1, AS2's neighbour AS3 advertises path AS3→ AS2→ AS1 and so on.

ASes can be broadly classified into two categories:

- "Stub" ASes sit at the periphery of the routing table, producing or consuming traffic while not providing transit to any other AS.
- "Core" ASes provide connectivity to other ASes: international carriers, Internet Service Providers. These are therefore critical to the rest of the infrastructure : they are the focus of the following security study.

III. Threat Model

BGP was designed to be as open and simple as possible, with little security concerns. It lacks elementary security features such as authentication (BGP routers communicate via unsecured TCP sockets) and path validation (the protocol does not check the consistency of announcements). A number of attacks are possible:

- **BGP hijacks**: any router can announce any prefix and reroute traffic from its legitimate target [2].
- **BGP death ray**: sophisticated route announcements can exhaust the resources of a victim router [3].

In addition to these BGP-specific attack, a number of generic threats against the backbone must be considered:

- **(D)DoS**: (Distributed) Denial of Service attacks disrupt a victim infrastructure via request saturation [4].
- **Packet of Death**: some routers can be taken down by specific packets exploiting OS vulnerabilities [5].
- **Physical attacks**: geographical asset concentration in the backbone makes it vulnerable to localised physical attacks, as described in the following section.

IV. Infrastructure Mapping & Attack Scenarios

We constructed a series of maps:

- **physical** maps of backbone assets: routers, landlines, undersea cables, colocation centres[1].

[1]Central platforms dedicated to exchanging BGP traffic, concentrating high numbers of routers and links.

- **logical** maps of the routing table showing the interconnection between ASes and potential traffic paths.

The maps reveal a number of serious pinch points of the infrastructure at both physical and logical levels. The geographical concentration of assets in colocation centres and the convergence of landlines and undersea cables to the same physical hubs is such that a single physical attack could take down a number of core systems at the same time. The logical reliance on limited numbers of core ASes (an example is shown in Fig. 1) providing most of the transit to the rest of the AS eco-system also make the backbone vulnerable: a single successful attack (hijack, DDoS, etc.) taking down a core AS could affect the entire infrastructure significantly.

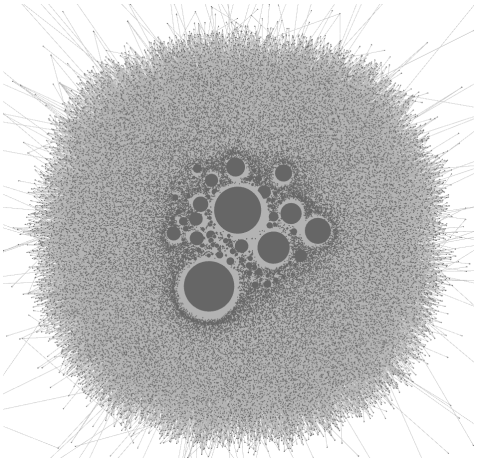

Fig. 1. Example routing table at an international colocation centre. Each node represents an AS, with its size proportional to the AS's degree.

We developed attack simulations based on actual AS routing tables [6], [7] representing significant portions of the backbone in Europe. These simulations estimate the knock-on effect of the death of a core AS by computing how many routes would have to be re-routed through other core ASes. This is a very rough estimate of the actual traffic the knock-on effect would represent[2] that gives an indication of the order of magnitude of the traffic surge such an attack would create.

Victim:	Effect on:					
	AS-A	AS-B	AS-C	AS-D	AS-E	AS-F
AS-A		15.3 22.3%	21.4 31.7%	10.9 15.7%	8.4 13.2%	7.5 19.1%
AS-B	15.2 18.3%		12.7 18.8%	9.6 13.8%	6.5 10.2%	5.6 14.3%
AS-C	21.8 26.2%	12.7 18.5%		8.6 12.4%	5.8 9.1%	5.9 15.1%
AS-D	11.1 13.3%	9.8 14.3%	8.8 13.1%		11.0 17.4%	5.8 14.8%
AS-E	8.6 10.4%	6.5 9.5%	6.0 8.9%	10.5 15.2%		4.2 10.7%
AS-F	7.6 9.1%	5.8 8.4%	6.0 8.9%	5.7 8.3%	4.3 6.7%	

Fig. 2. Effect of taking down a single core AS (left column) on other core ASes (top row): load surge is measured in absolute traffic (top number) and relative to the usual traffic (bottom percentage). Only top core AS are shown.

Sample results in Fig. 2 show that the death of a core AS would indeed result in a sizeable number of link redirections for the rest of the backbone. For instance, the death of AS-A (first line) would create a traffic surge from 13.2% (on AS-E*) to 31.7% (on AS-C). Several simulations run on different data sets show similar orders of magnitude, with many traffic surges above 10% and up to to 50%, depending on the topology. The reaction of the backbone to such an event is hard to predict. In case the traffic surge proved too much for another core AS to handle, this AS could in turn be taken down and a cascading failure could follow, with a theoretical potential for major disruption to the Internet eco-system. Despite the incompleteness of the data, one must therefore conclude that the risk of cascading failures in the backbone cannot be ruled out as improbable a priori, and more investigations are necessary to establish a sound evaluation of that risk.

[2]A better approach would be based on actual traffic data, which is not publicly available.

V. Broader perspectives

The demonstration that cascading failures in the backbone are theoretically possible is not the only crucial conclusion of this study of the resilience of the Internet. It must be appreciated in the context of the following findings:

- The Internet is mostly an uncharted territory: operators report unanimously that grey areas in their own infrastructures – BGP and beyond – cover unexpected behaviours and hidden dependencies. This perception is confirmed by the limits of the publicly available routing data used in this study. A significant mapping and assessment effort is necessary to understand the state and the fragilities of the backbone.
- Secure extensions of the BGP protocol – meant to address its weaknesses by providing authentication and path validation features – are impractical: they introduce known additional security issues, and their limited deployment makes them inefficient.

Beyond technical issues, governance considerations are also essential to securing the backbone – and in such a global system of systems, governance is an international challenge. Balancing regulatory (static) approaches against cooperative open models currently in use for backbone operation and regulation will be key to achieving a sound governance of the Internet.

References

[1] T. Dyba, B. Kitchenham, and M. Jorgensen, "Evidence-based software engineering for practitioners," *Software, IEEE*, vol. 22, no. 1, pp. 58–65, Jan 2005.

[2] J. Gersch and D. Massey, "Characterizing vulnerability to ip hijack attempts," in *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, Nov 2013, pp. 328–333.

[3] M. Schuchard, C. Thompson, N. Hopper, and Y. Kim, "Peer pressure: Exerting malicious influence on routers at a distance," in *Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on*, July 2013, pp. 571–580.

[4] N. Hoque, M. H. Bhuyan, R. Baishya, D. Bhattacharyya, and J. Kalita, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications*, vol. 40, pp. 307–324, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804513001756

[5] K. Kielhofner, "Packets of Death," http://blog.krisk.org/2013/02/packets-of-death.html, 2013, [Online; accessed 25-Feb-2014].

[6] "CAIDA," http://www.caida.org, 2014, [Online; accessed 15-Jul-2014].

[7] "RIS Raw Data," http://www.ripe.net/data-tools/stats/ris/ris-raw-data, 2014, [Online; accessed 30-Apr-2014].