Measuring Internet resilience

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Measuring Internet resilience

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Internet resilience

The ability to work even under strain (failure, dDoS. . .)

A very necessary property, now that the Internet is used for a lot of important things (love letters, banking, process control, e-government, sending ICANN applications for a new gTLD. . .)

The report

`http://www.ssi.gouv.fr/NOT-YET-PUBLISHED-BUT-SOON`

« Résilience de l'Internet français 2011 : état des lieux »

or

"Resilience of the French Internet 2011: an assessment"

Actual measurements

The report focuses on **data**, not theoretical analysis or feelings. 55 pages. Publically available but no actual name given (no domain name, no AS number).
This first version analyses only BGP and DNS. Uses almost only public information. The result is "not bad" but things can be improved.

The authors

1. ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information, the national cyber-security agency, under the Prime Minister `http://www.ssi.gouv.fr/`),
2. AFNIC (Association Française pour le Nommage Internet en Coopération, the `.fr` registry `http://www.afnic.fr/`)

[BGP] The indicators

- Consistency between Internet Routing Registries and the reality
- Level of connectivity

[BGP] The method

1. Four big French operators selected,
2. BGP announcements from a RIS route collector during the year,
3. Routing registry data from RIPE-NCC,
4. Analysis by a home-made program. OCaml ruLeZ.

Two views:

- BGP announcements compared with registry data (“Is there a route object for this announcement?”)
- and registry data compared with announcements (“Is this route object present in the BGProuting table?”)

afnic

[BGP] The results

1. Consistency between the announcements and the registry varies from “perfect” (100 % match) to “better than nothing” (as low as 33 % match for route objects vs. BGP and 13 % for BGP vs. route objects).
2. Five transit operators provide most of international connectivity of the Big Four.
3. BGP severe inconsistencies are common (average 10 % for one operator) but typically mistakes, not deliberate hijackings. Nevertheless, we can guess that deploying RPKI will be hard. Operators have trouble managing their address space.

afnic

[DNS] The indicators

- Number and diversity (AS, country) of name servers per zone
- Source Port Randomization of resolvers
- Usage of IPv6, DNSSEC, SPF, in the zones

[DNS] The method

1. Active query of domains under `.fr` with DNSwitness `http://www.dnswitness.net/`
2. Find out IP addresses, AS numbers, countries for the name servers,
3. Check if signed with DNSSEC, if IPv6 announced,
4. Passive measurements of incoming requests: Source Port Randomization, IPv6 transport and query type.

[DNS] The results

1. Not enough name servers per zone: 2.2 in average (recordman at 8, the maximum allowed by AFNIC),
2. Insufficient variety of AS per zone: 1.2 in average (recordman at 7), 80 % of the zones have only one AS, ← **Biggest weakness**
3. Concentration: one AS has 36 % of the name servers,
4. Big majority of name servers inside France,
5. Still 10 % of resolvers without SPR, four years after Kaminsky,
6. Very little DNSSEC (∼100 signed zones) or IPv6 (40 % of zones with at least one IPv6 name server but less than 1 % with an IPv6 Web server, 2 % of incoming requests over IPv6).

Future work

- RPKI deployment
- Testing quality of DNS configuration (Zonecheck)
- More BGP collectors

Prospective:

- Analysis through distributed DNS resolvers (Varuna project)

Similar work

- IIS.se does a comprehensive DNS analysis `http://www.iis.se/docs/Healthcheck2011-Reachability.pdf`
- Kim Davies analyzes the resilience of TLDs, for instance "AS diversity" `http://svsf40.icann.org/meetings/siliconvalley2011/presentation-update-root-zone-management-15mar11-en.pdf`