AT-LARGE ADVISORY COMMITTEE

AL.ALAC/ST.0309/5
ORIGINAL: English
DATE: 16th May 2009
STATUS: FINAL

Statement on DNS Security Issues

At-Large Advisory Committee Statement

Introductory Statement
By the Staff of ICANN

This statement is the result of a process begun when representatives of eighty-eight (88) At-Large Structures ("ALSes") from five Regional At-Large Organizations ("RALOs") representing ICANN's global At-Large community met in the At-Large Summit (ATLAS) as a part of the 34th International ICANN meeting in Mexico City.

Amongst the various activities of the Summit were five working groups on issues of concern to the At-Large community. One of the five was devoted to ICANN Transparency and Accountability.

The final statements of all five working groups was compiled into the Declaration of the At-Large Summit, presented to the Board of ICANN at the Public Board Meeting in Mexico City.

In order to ensure that the entire At-Large community had the opportunity to review the five statements, and for their perspectives to be taken into account, the ALAC resolved upon a process of consultation and amendment for the statements by resolution at its 24th March 2009 teleconference. As a result, the Summit Working Group statement was opened for public comments by the At-Large community on 1st April, closing on 1st May. The Chair of the ALAC then requested the Staff to open a vote on the document, said vote opening on 8th May and closing on 15th May.

The results were announced on 16th May by the Staff, said result being that the Statement was endorsed by a vote of 10-1-0. The result may be verified under the following URL: https://www.bigpulse.com/pollresults?code=jQmtJVrePkpDYQELXHg9

Internet users want all reasonable steps taken for a more secure internet

We recognize that there is no “silver bullet” technology or policy that will make the Internet entirely secure. We also recognise that ICANN is not the only organisation that deals with securing the Internet. But we are concerned with the role ICANN should play to better secure the Internet for Internet users.

Recently, ICANN's constituent communities have begun to ask how ICANN could work within its remit and have a positive impact to reduce activities which use the DNS in criminal, malicious or fraudulent ways.

For its part, ICANN's mission includes as a core component ensuring the stability and security of the DNS, which is in its remit. We believe that there are actions that ICANN can and should take that will mitigate and possibly stop such malicious or criminal activities.

We believe ICANN should act in the following areas:

- DNSSEC
  - Signing the root
  - Requirements for Registries and Registrars
- Fighting exploitation of the DNS
  - Accuracy and verifiability of registration data
- Registration abuse

DNSSEC

The introduction of DNSSEC, especially signing the root, might harm the some network implementations i.e. WIFI hotspots. Several authentication systems are likely to fail. ICANN should initiate a study of such possible impacts.

ICANN should support industry efforts to accommodate DNSSEC and its provision in more secure environment.

Signing the root

We urge ICANN to proceed in the process of having the root signed in a way that provides integrity and is globally accepted. We believe international accountability for generating the signatures to be the most acceptable solution.

Until the root is signed, third party trust anchor repositories (especially ITAR) should be used.

Requirements for Registries and Registrars

All TLDs should be signed as soon as possible, to establish a valid trust chain. Trust anchor repositories do not scale at that level due to domain explosion. Therefore, we urge all new TLDs to be signed from their inception. DNSSEC should be a technical requirement for new registries and new TLDs.

ICANN should modify the registry and registrar contracts to include provisions that would allow registrants to deploy DNSSEC in a convenient way. (See Annex A for details).

Fighting exploitation of the DNS

Currently the most prominent example of exploitation of the DNS is Fast-Flux hosting as described in the following documents:
http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf,
http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf

We support the APWG Best Practices and urge all stakeholders to implement the proposed steps as soon as possible. There is no need for further studies; it is time to act.

We urge ICANN to support the following points:

• Encourage a stricter registration process to minimize fraudulent registrations.
• Enforce technical methods to restrict fast-flux as defined by the APWG at the registry level.
• Adopt a clearly defined, universal process for accelerated suspension of misused domains.
• Promote improvement of data sharing and analysis regarding criminal or malicious ctivities among registry, registrar, law enforcement and anticrime communities. Data protection and privacy issues must be considered.
• Collect and promote best practices for registries and registrars to protect their customers from fraudulent activities. Provide the information translated to the native languages of the end users, i.e. http://www.identidadrobada.com/

Registration abuse

For the Internet user and domain registrant, the following issues are important:

• Domain Name Hijacking
• Registrant impersonation by social engineering
• Domain transfer pitfalls
• Erroneous delete

We strongly encourage ICANN to promote the prompt implementation of the recommendations from the 2005 Hijacking report:
http://www.icann.org/en/announcements/hijacking-report-12jul05.pdf

The working group recognizes that the recommendations therein have been implemented to varying degrees, however, full implementation will go a long way to addressing all of the issues above.

Typo squatting is registering a domain name which can be easily confused with an existing one. The issue becomes more widespread and difficult to solve with the introduction of IDN. Together with other fraudulent look-alike domain presentations such registrations should not be allowed in the first place. These techniques are used in the distribution of malware and for purposes of PII theft, as well for search engine result gaming. We recommend applying the existing detection algorithm to all registries and encourage a study on the new issues with IDNs.

Conclusion

In order to deploy DNSSEC in a wide scale, the registry and registrar contracts should be amended to include provisions relative to DNSSEC. Existing TLDs should be signed as soon as possible. New TLDs should be signed from the start. The root should be signed as soon as possible.

There could be some issues for the Internet users to be able to effectively benefit from the added security introduced by DNSSEC. It is also crucial that mechanisms are put in place at registry and registrar level to allow domain name registrants to deploy DNSSEC in a convenient way.

A number of malicious and criminal activities involving domain name registration could be mitigated by stricter registration processes and monitoring of unusual registration activities.

Summary of recommendations

• ICANN should initiate a study of such possible impacts of the introduction of DNSSEC on the installed base.
• ICANN should proceed in the process of having the root signed in a way that provides integrity and is globally accepted.
• ICANN should modify the registry and registrar contracts to include provisions that would allow registrants to deploy DNSSEC in a convenient way.
• ICANN should encourage a stricter registration process to minimize fraudulent and criminal registrations.
• ICANN should proceed further with implementing the proposals from the 2005 Hijacking report.

Annex A

From the Internet user perspective, an effective DNSSEC solution should address the following points:

• Domain management through the reseller chain has to include all DNSSEC features. Registrants need a single entity to deal with.
• Publish escalation matrix for DNSSEC failure: Wrong or expired signatures render the zone unusable. Key loss due to operational error is expected to be the most common error and will only noticed, when the first signatures times out. Quick reaction is important. Otherwise DNSSEC will be disabled.
• Require minimal DNSSEC capabilities at every point in the reseller chain: Removing key material by authorized people to deal with transferring signed domains.
• Extend holder change policies to a seamless key rollover as the default change procedure even with unwilling parties. Zones should be kept signed during this process.
• Unauthorized or malicious people must not be able to disturb the DNSSEC.