Trustworthy Transfers

Quantifying structural difficulties in maintaining the DNSSEC path of trust during domain transfers for domains hosted on registrar-operated nameservers

JOE ABLEY, WESTERN UNIVERSITY, JABLEY@UWO.CA

Domain registration through the Shared Registry System is fundamentally a database service. The products of those services are reflected in the DNS infrastructure, but they are not a priori DNS services. However, DNS hosting services are frequently bundled with domain registration services by organisations that provide registrar functions. Consequently, these functions are frequently conflated; anecdotally, registrants expect DNS services to be part of the domain registration they are paying for. DNSSEC signing is another example of a separate service that is frequently bundled.

The Shared Registry System accommodates domain transfers between registrars with no interruption to registration systems. However, continuity of bundled DNS hosting or DNSSEC signing services is not assured by the system and there has been concern expressed for over ten years that the lack of such assurance causes operational problems that ultimately may act as barriers to improved DNSSEC adoption.

The ultimate goal of this work is to validate concerns about whether there is a structural incompatibility between DNSSEC and domain transfers of the kind alluded to above using measurements of the DNS and corresponding Shared Registry System.

A natural prerequisite to answering that problem is to know whether a domain transfer has occurred, whether a change of nameservers indicative of the imagined bundling scenario accompanied the transfer, whether the transferred domain was signed with DNSSEC and whether this combination of circumstances is observed to have presented an operational problem.

Some well-known source data that could provide insight into these questions are readily available and well-known. However, some of the source data are not required to be made available contractually by registry operators, are not generally published and can only be inferred. The accuracy of those inferences is difficult to assess without some ground truth. A secondary goal of this work is to train an inference model that can identify domain transfers based on changes visible in the DNS, without reference to registry data and identify a source of ground truth that can be used to test it.

We will acquire datasets that will allow the frequency of the domain transfer scenario of concern to be measured accurately over a representative, recent sample period in the ORG registry. ORG is a so-called legacy gTLD, having been in continuous operation since 1985. It was the first gTLD to support DNSSEC, and has an active registry that with over ten million domains under management. It is also a gTLD for which most registrars are accredited. We will use the domain transfer dataset to quantify the rarity of the scenario and to identify trends.

We will acquire DNS zone data for ORG and other gTLDs. The DNS zone data for ORG will be used to design, train and test an inference model that allows the insights in the ORG gTLD to be identified without reference to registry data. This model will then be used to provide equivalent (estimated) insights into other gTLDs solely by reference to DNS zone data.

Together, the transactional registry data from the ORG registry together with inferred equivalent insights into other gTLDs will provide a measure of how frequently the domain transfer scenario of concern occurs, and whether its frequency is trending up over time.