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

Agenda

- For the purposes of this study:
  - we are only concerned with domains registered in gTLD registries, although quite possibly some findings here will be applicable to others;
  - we are only concerned with secure delegations, although some of the byproducts of the approach might be more generally useful.
- In this brief presentation we will cover:
  - the ultimate goal of this work to provide context;
  - source data acquisition;
  - the planned approach to infer data that we can't obtain directly

Anatomy of a Domain Transfer

- A change in the sponsoring registrar for a particular domain name
- The choreography of a domain name can be a little involved (time-outs, registrant confirmations, auth codes)
- Domain Transfers are database transactions
  - a change in the stored metadata for a domain name
  - a change in sponsoring registrar has implications for billing and for authorisation for subsequent changes to the domain name
  - the transfer operation in and of itself does not result in a change in the DNS

DNS Hosting is not a Registrar Service

Except that everybody assumes it is

- Normal people don't go to ICANN meetings
  - instead they live happy and productive lives
- Most people who register a domain just want their web page to work
  - they don't know or care about the DNS
  - they don't know or care about DNS hosting
- The registrar business is competitive, low-margin and sensitive to support costs
  - you give people exactly what they expect or they will find someone else to do it
  - you bundle DNS hosting with domain name registration, usually for free

Scenario 1

Transfer Trouble

- EXAMPLE.ORG registered through Registrar A
- EXAMPLE.ORG hosted for free on nameservers operated by Registrar A, something that the registrant is largely oblivious to
- Registrant decides that they like Registrar B's Superbowl commercial that told them to move their domain name there for a Special Low Price (Act Now! Superbowl Special!)
- EXAMPLE.ORG transfer initiated by Registrar B at registrant's request
- Registrar A has no reason to continue the free DNS hosting service and drops the domain immediately, which causes the domain to stop working (lame delegation)
- EXAMPLE.ORG transfer completes (this might take some time)
- Domain is repaired by Registrar B, either automatically or at the registrant's request

Scenario 2

Transfer Trouble with a side order of DNSSEC

- EXAMPLE.ORG registered through Registrar A
- EXAMPLE.ORG hosted for free on nameservers operated by Registrar A, something that the registrant is largely oblivious to
- **EXAMPLE.ORG is signed by Registrar A**
- EXAMPLE.ORG transfer initiated by Registrar B at registrant's request
- EXAMPLE.ORG transfer completes (this might take some time)
- Domain is repaired by Registrar B, either automatically or at the registrant's request
    - **EXAMPLE.ORG either goes unsigned or is signed by Registrar B, in which case the domain just experienced a really poor and abrupt KSK rollover**

Anecdotes and Supposition

- These scenarios have been discussed at sporadic intervals over the past decade
  - people keep threatening to design new policy around these problems
  - people keep saying things like "domain transfers don't work with DNSSEC"
  - people are designing technical mechanisms to try and manage smooth transfers of the DNSSEC signing function between different operators
- Nobody seems to have spent much time looking to see whether these problems are actually real
  - let's try and do something about that

Source Data

Registry Data

- Public Interest Registry (operators of the .ORG registry) have a relatively new programme for data sharing for research
  - they have an internal approval process and template data access agreements that are very reasonable
  - separate processes for datasets that contain PII and those that do not
  - the details are not very well-publicised
- I asked PIR for a list of transfer operations over a sample period and they said yes
- Most other large legacy gTLD operators do not make data available in this way as far as I know
  - need another approach if we want to find transfers in other gTLDs

Finding Transfers in Zone Data

- Transfer operations don't involve DNS changes, in theory
- However, if scenarios like those described are real, and if people want their domains to work they will need to update nameservers after domains are transferred
- Look for correlations between changes in zone data in the ORG zone and transfer transaction data shared by PIR
  - build and test a classifier to identify transfer operations
  - build and test a classifier to map domain names to registrars
- If scenarios like those described are not real, and we can't find a useful correlation, then that probably also tells us something

Source Data

Zone Data

- CZDS gives access to gTLD zone data for research
  - obtaining a history of zone data over a non-trivial sample period takes a little more work
  - getting registry operators to give you access even when your request is entirely legitimate also takes a little more work
  - spin up the tiniest, cheapest VM you can on AWS and run daily jobs to pull zone data and throw the results into cold storage until you have enough to sift through
- Zone data provides nameservers and DS RRs for domains

Testing the Classifiers

- We can use training and test data from PIR to test the model for the ORG registry
- We can use the nameserver/registrar classifier to try and map domain names to registrars in other gTLDs
  - we can test the accuracy using whois
- We can use the nameserver/transfer classifier to try to find transfers in other gTLDs
- There is some hope that we can build classifiers that are accurate enough to use, and also that the accuracy can be quantified well enough to draw downstream conclusions

Checkpoint

- At this point in the story we will hopefully have:
  - Access to zone data history for most gTLDs
  - An ability to find transfers for domains hosted on registrar-operated nameservers
  - Knowledge of which domains were signed with DNSSEC at the time they were transferred
- Or we will fail to find transfer footprints in zone data, in which case we will regroup and imagine that this part-time Masters programme might never end

Questions?