

A Universally Unique Registrant ID

Gavin Brown gavin.brown@centralnic.com

ROW, May 2018

Problem

- Registrant info coming out of public Whois.
- Anti-abuse researchers unable to correlate domain registrations to identify patterns in registrations, e.g. for DGA botnet takedown.
- Anti-abuse researchers don't care about the email address itself, they just use it as a unique key to correlate registrations. They also do this using nameservers.

Proposal

- For each domain, publish an opaque token derived from the registrant's email address: $H(e, k)$.
- This means that domains registered to the same registrant will have the same token.
- Even if different domains have a different registrant *objects*, the token will be the same if the email address is the same.
- Anti-abuse people can then correlate registration activity as before.
- Provide a private API allowing vetted persons, given a known email address, to find out what token that email address corresponds to.

Issues

- Email addresses may require “normalisation”, e.g.: case folding, handling internationalised email addresses, known domains that do things with “+” and “.” characters.
- Easy to deploy on a single registry system, but value in deploying across many registries.
- Can we design a solution that allows different registries to generate the same token for an email address?
 - A shared secret key?
 - A central registry?
 - A blockchain?
- Would such a token be PII?