WHOAMI – a decentralised alternative to WHOIS

Gavin Brown <gavin.brown@centralnic.com>

IETF 101, London
WHOAMI – agenda

• Origin story
• Status quo
• Description of protocol
• Impact on various parties
• Potential issues
• Future work
WHOAMI – origin story

Fabricio makes some good points. WHOIS is an important tool to keep the Internet working properly. There needs to be ways to contact people responsible for websites and more.

Gavin Brown
There is. Every domain owner could publish their contact information in a vcard at https://www.example.com/well-known/whois.vcf. No less likely to be accurate, but no massive database required.

404 - Not Found
example.com
4 m Like Reply
WHOAMI – origin story

Internet Engineering Task Force
Internet-Draft
Intended status: Experimental
Expires: June 22, 2018

G. Brown
CentralNic Group plc
December 19, 2017

title

A Method For Identifying a Domain Operator's Point of Contact (WHOAMI)
draft-brown-whoami-00

Abstract

This document proposes a decentralised alternative to traditional
WHOIS directories.
WHOAMI – status quo – RDDS (Whois/RDAP)

• Registries collect contact information (sometimes via registrars) and store it in a centralised database

• Freely available to anyone who wants it (for good or evil) via WHOIS/RDAP

• Low-level PII – but lots of it

• Zone files/passive DNS are an index allowing data mining, resulting in spam, phishing, ID theft, scams, etc

• Zero transparency for data subjects on who is processing their data

• No differentiated access (even though RDAP supports it)

• No incentive for data subjects to provide accurate information
WHOAMI – basic principles

• No centralised database

• Domain owners/operators publish their own contact information as vCard

• WHOAMI protocol provides a way for consumers to locate this information for a given domain

• Self-publication gives domain owners/operators transparency on access/processing

• Easy to delegate to third parties

• No worse than the Status Quo
WHOAMI – protocol – URI record

_nicname._tcp.example.com. IN URI ( 
    10 ; priority 
    1 ; weight 
    https://example.com/whoami/whoami.vcf ; target 
)
WHOAMI – protocol – data: URI record

_nicname._tcp.example.com. IN URI (  
  10  
  1  
  
    data:text/vcard;charset=utf-8;base64,QkVHSU46VkNBUkQNC1ZF...  
)

WHOAMI – protocol – well-known URI

http://example.com/.well-known/whoami/whoami.vcf
WHOAMI – for domain owners

• Publish their own vCard
  • Many already publish same information (e.g. as “Impressum”) due to local regulation

• Redirect to third party agent/proxy

• Delegate to host/registrar/DNS operator

• Require authentication for access

• Log requests to access WHOAMI information

• Provide different information to different requestors
WHOAMI – for registrars, web/DNS hosts

• Easy to act as an agent/proxy for customer by intercepting WHOAMI queries
• Value-added service to manage WHOAMI for customers
WHOAMI – for registries

• No need to maintain large databases
  • Whois/RDAP becomes “thin”
  • GDPR

• Can still validate contact information at <create>/<update>/<renew>

• Still easy to monitor and review compliance
WHOAMI – for consumers

• Still possible to data mine
• Can integrate into applications (e.g. browsers) without risk of hitting registry rate limits
• May need to handle domains which require authentication
• Can still report domains with missing/bogus WHOAMI data to registries to be suspended
WHOAMI – potential issues

• WHOAMI could be abused/misused
• But in no worse ways than Status Quo is abused/misused
WHOAMI – future work

• Authentication of access requests
• Multiple contact types (admin/tech/billing/abuse)?
• How could WHOAMI work for domains on clientHold/serverHold?
• Security Considerations – formal analysis
• Privacy Considerations – formal analysis
• WG adoption?
• Deployment
Questions?

gavin.brown@centralnic.com

@GavinBrown