WHOIS RIGHT?
AN ANALYSIS OF WHOIS AND RDAP CONSISTENCY

Simon Fernandez[1], **Olivier Hureau**[1], Andrzej Duda[1], Maciej Korczyński[1]

[1]Université Grenoble Alpes, CNRS, Grenoble INP, LIG, 38000 Grenoble, France

Public registration information on domain names, such as the accredited registrar, the domain name expiration date, or the abuse contact is crucial for many security tasks, from automated abuse notifications to botnet or phishing detection and classification systems. Various domain registration data is usually accessible through the WHOIS or RDAP protocols—*a priori* they provide the same data but use distinct formats and communication protocols. We examine the core assumption that WHOIS and RDAP offer the same data and that users can query them interchangeably.

WHOIS

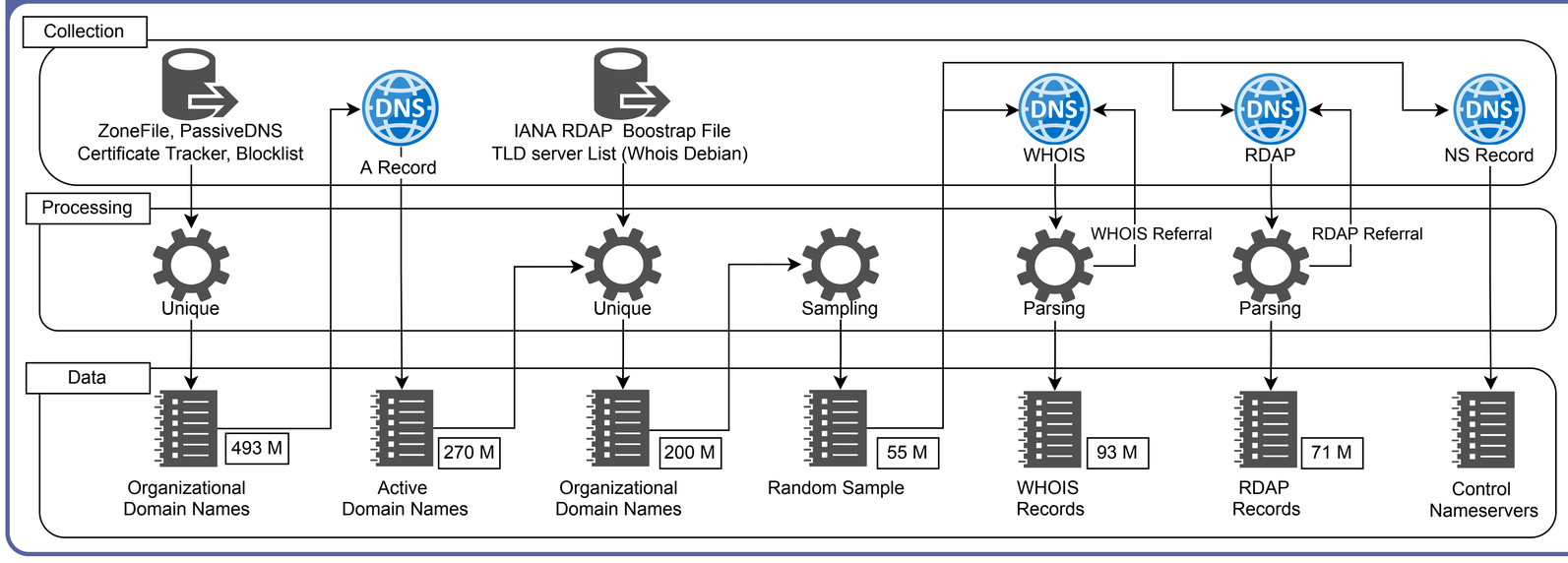
```
hureauo@fiji:~$ whois hureau.com
   Domain Name: HUREAU.COM
   Registry Domain ID: 142356035_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.ovh.com
   Registrar URL: http://www.ovh.com
   Updated Date: 2024-02-01T06:48:42Z
   Creation Date: 2005-02-13T19:04:29Z
   Registry Expiry Date: 2025-02-13T19:04:29Z
   Registrar: OVH sas
   Registrar IANA ID: 433
   Registrar Abuse Contact Email: abuse@ovh.net
   Registrar Abuse Contact Phone: +33.972101007
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: DNS108.OVH.NET
   Name Server: NS108.OVH.NET
   DNSSEC: signedDelegation
   DNSSEC DS Data: 48475 8 2 7E77E427C18E5F39A198C39D169186B760B2C3C14F46FAADBB086B16F280F61F
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-18T14:54:03Z <<<
```

RDAP

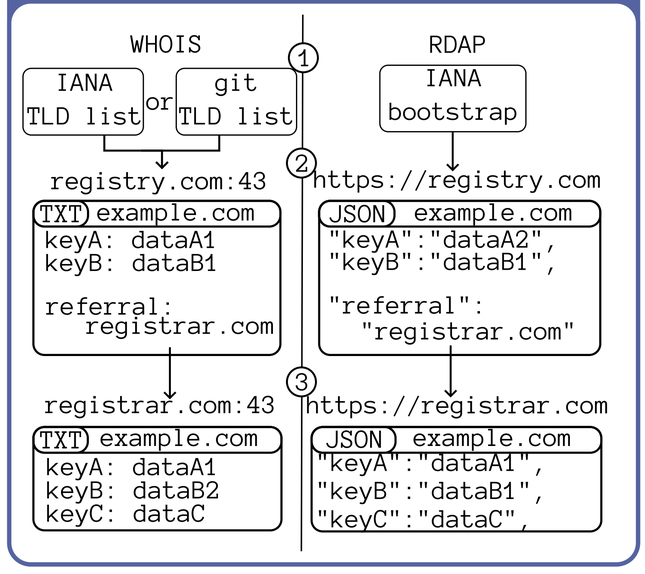
```
hureauo@fiji:~$ curl https://rdap.verisign.com/com/v1/domain/hureau.com
{"objectClassName":"domain","handle":"142356035_DOMAIN_COM-VRSN","ldhName":"HUREAU.COM","links":[{"v
alue":"https:\/\/rdap.verisign.com\/com\/v1\/domain\/HUREAU.COM","rel":"self","href":"https:\/\/rdap
.verisign.com\/com\/v1\/domain\/HUREAU.COM","type":"application\/rdap+json"},{"value":"https:\/\/rda
p.ovh.com\/domain\/HUREAU.COM","rel":"related","href":"https:\/\/rdap.ovh.com\/domain\/HUREAU.COM","
type":"application\/rdap+json"}],"status":["client delete prohibited","client transfer prohibited"],
"entities":[{"objectClassName":"entity","handle":"433","roles":["registrar"],"publicIds":[{"type":"I
ANA Registrar ID","identifier":"433"}],"vcardArray":["vcard",[["version",{},"text","4.0"],["fn",{},"
text","OVH sas"]]],"entities":[{"objectClassName":"entity","roles":["abuse"],"vcardArray":["vcard",[
["version",{},"text","4.0"],["fn",{},"text",""],["tel",{"type":"voice"},"uri","tel:+33.972101007"],[
"email",{},"text","abuse@ovh.net"]]]}]}],"events":[{"eventAction":"registration","eventDate":"2005-0
2-13T19:04:29Z"},{"eventAction":"expiration","eventDate":"2025-02-13T19:04:29Z"},{"eventAction":"las
t changed","eventDate":"2024-02-01T06:48:42Z"},{"eventAction":"last update of RDAP database","eventD
ate":"2024-04-18T15:18:42Z"}],"secureDNS":{"delegationSigned":true,"dsData":[{"keyTag":48475,"algori
thm":8,"digestType":2,"digest":"7E77E427C18E5F39A198C39D169186B760B2C3C14F46FAADBB086B16F280F61F"}]}
,"nameservers":[{"objectClassName":"nameserver","ldhName":"DNS108.OVH.NET"},{"objectClassName":"name
server","ldhName":"NS108.OVH.NET"}],"rdapConformance":["rdap_level_0","icann_rdap_technical_implemen
tation_guide_0","icann_rdap_response_profile_0"],"notices":[{"title":"Terms of Use","description":["
Service subject to Terms of Use."],"links":[{"href":"https:\/\/www.verisign.com\/domain-names\/regis
tration-data-access-protocol\/terms-service\/index.xhtml","type":"text\/html"}]},{"title":"Status Co
des","description":["For more information on domain status codes, please visit https:\/\/icann.org\/
epp"],"links":[{"href":"https:\/\/icann.org\/epp","type":"text\/html"}]},{"title":"RDDS Inaccuracy C
omplaint Form","description":["URL of the ICANN RDDS Inaccuracy Complaint Form: https:\/\/icann.org\
/wicf"],"links":[{"href":"https:\/\/icann.org\/wicf","type":"text\/html"}]}]}
```

Measurements

Domain Data Collection and Filtering



Referral system



Results

Field	Missing rate (domain)	Domain inconsistency
Nameserver	6.6%	573,790 (1%)
IANA ID	13.7%	106,83 (0.2%)
Creation Date	2.2%	3,138,024 (5.7%)
Expiration Date	2.7%	2,424,951 (4.4%)
Emails	14.8%	18,958,821 (34.5%)

Nameservers and Emails Mismatches

Domain mismatches	Nameservers	Emails*
Inclusion	224,833	14.5 M
Intersection	23,934	0.23 M
Disjoint	343,994	2 M

* After removing the local part of the address.

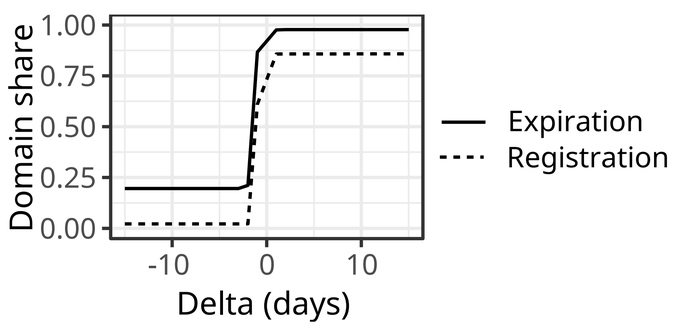
Inclusion. $A \subset B$ or $A \supset B$: one set is a subset of the other one.

Intersection. No inclusion but $A \cap B \neq \emptyset$: A and B do not match but they have at least one common server.

Disjoint. $A \cap B = \emptyset$: A and B do not have common nameservers.

Mismatching Dates

Cumulative distribution of creation and expiration date mismatches



Conclusion

Our analysis of 164 million entries from 55 million domains highlighted that even if the majority of the information available through WHOIS and RDAP stays consistent across servers and protocols, 7.6% of all studied domains had mismatching entries.

The additional analysis highlighted that these mismatches vary a lot in form, severity, and the number of the concerned domains but also underlines that for the fields where we could determine which entry is right by collecting data from another source, RDAP entries are right in 78% of the cases when mismatching with a WHOIS entry.

This work has been partially supported by the French Ministry of Research projects PERSYVAL-Lab under contract ANR-11-LABX-0025-01 and DiNS under contract ANR-19-CE25-0009-01.

References

[1] Aruna Prem Bianzino et al. "Who is whois? An analysis of results consistence". In: *2014 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, Sept. 2014.

[2] Carlos Ganan. "WHOIS Sunset? A Primer in Registration Data Access Protocol (RDAP) Performance". In: *TMA* (2021), p. 8.

[3] Chaoyi Lu et al. "From WHOIS to WHOWAS: A Large-Scale Measurement Study of Domain Registration Privacy under the GDPR". In: *Proceedings 2021 Network and Distributed System Security Symposium*. NDSS 2021. Internet Society, 2021.