Registro.it

THE REGISTRY OF .IT DOMAINS

REGISTRO .IT IS MANAGED BY

Consiglio Nazionale delle Ricerche

ISTITUTO DI INFORMATICA E TELEMATICA

IETF 110 Online RegExt Session, Mar. 9, 2021

Review of draft-ietf-regext-rdap-reverse-search

Mario Loffredo
Registro.IT/IIT-CNR

Feedback from IETF 109

- Technical issues
  - **Alex**: We need a scalable AAA infrastructure for that
- Privacy concerns
  - **Alex**: no need to say “follow the law”, but there should be a MUST consider implications for implementors
  - **Ulrich**: We should point our where exactly the privacy problems are! Follow the law is not enough
  - **Antoin**: HRPC WG opposed this document. Their work was about not publish it at all

Technical issues

- **We do need a scalable AAA infrastructure for all the searches!**
- Measures:
  - Making searches available only to some users
  - Limiting rate of search requests
  - Applying restrictions to search paths and patterns (e.g. use of wildcard)
  - Implementing RFC 8977 and RFC 8982 capabilities

Privacy concerns (1)

- Generic threats from RFC 6973
  - **Disclosure**: the revelation of information about an individual
  - **Secondary use**: the use of collected information about an individual without the individual's consent for a purpose different from that for which the information was collected
  - **Mis-use**: the use of information about an individual for a purpose different from that for which the use was requested and approved

Privacy concerns (2)

- Specific threats
  - **PII in REST API query**: the delivery of PII as a query parameter in a GET request
  - **Detecting facts**: the ability to infer facts about an individual starting from a PII
  - **Anything else?**

Recall of GDPR principles

- In order to treat personal data you must have a lawful basis to do so:

1. the consent of the individual
2. performance of a contract
3. compliance with a legal obligation
4. necessary to protect the vital interests of a person
5. necessary for the performance of a task carried out in the public interest
6. in the legitimate interests of company/organization (except where those interests are overridden by the interests or rights and freedoms of the data subject)

- In RDAP context, RDAP servers MUST collect information and provide users with query capabilities and response contents in compliance with GDPR (or other privacy protection regulations in force).

Disclosure - Mitigations

- Providing query capabilities and response contents according to user profiles
  - “…The most common way for protocols to limit disclosure is by providing access control mechanisms....” (RFC 6973)
- Minimizing functionalities and data within Identity Management (i.e. Role-Based Access Control)
  - Can be implemented through OpenID ”scope” claim
- Ensuring that the endpoint of a communication is the one that is intended
- Keeping data opaque to unauthorized users

Secondary use - Mitigations

- Asking the contact for specific consent about the use of private information
  - “…Protecting against secondary use is typically outside the scope of IETF protocols....” (RFC 6973)
- In the context of RDDSs:
  - There are registries asking the individual for a generic consent for publishing (GDPR LB 1)
  - Should an RDAP provider implementing reverse search ask for a specific consent?
    - No, if the reverse search is accessible only to accredited users
    - Anyway, if we should, it should be done for standard seaches as well

Mis-use mitigations

- Requiring the user to declare the purpose of the request (i.e. Purpose-Based Access Control)
- Two possible models:
  - Full Trust: the registry trusts the fairness of an accredited user (e.g. police officer, authority). The requestor is always legitimated to submit a given request for a legal purpose
    - Can be implemented by using the RDAP specific OpenID “purpose“ claim
  - Zero Trust: the registry requires documents assessing that the requestor is legitimated to submit a given request no matter the declared purpose
    - Can be implemented by assigning the requestor with temporary OpenID credentials linked to the given request (i.e. Time-Based & Attribute-Based Access Control)

PII in REST API query - Mitigations

- Controlling the access to reverse search capability
- Securing the transport channel (i.e. HTTPS)
- If this is not considered sufficient, what about the following ?

```
/entities?fn=Mario%20Loffredo
```

Detecting facts - Mitigations

- Permitting a usage of reverse search compliant with GDPR (or other privacy protection regulations in force):
  - Allowing registrars to search only their own contacts (GDPR LB 2)
  - Allowing a public officer to request information in the performance of a task set out in a law (GDPR LB 5)
  - Allowing UDRP service providers to request information in defense of the legitimate interests of complainants (GDPR LB 6)
- **Note**: Reverse search is not the only way to detect facts in RDAP

Summarizing

- All of the privacy concerns about reverse search in RDAP are common to standard searches
- To mitigate privacy threats, RDAP providers MUST set up an AAA infrastructure operating in compliance with regulations about privacy protection in force in their countries
- Consequently, RDAP providers SHALL implement authorization rules increasingly stringent: from a policy based merely on roles, to requiring the request purpose, till to assigning the user with temporary credentials and related grants that are scope limited
- Even if searches on contacts' information might be made publicly available on those contacts who gave the consent for publishing, RDAP providers are RECOMMENDED to allow those searches only to authorized users

About HRPC’s opinion and engagement

- There are some requirements from legal stakeholders to open reverse search to accredited users for abuse and cyber crimes investigations:
  - GNSO IPC and BC
  - CENTR L&R discussion on EU E-Evidence and cooperation between Registries and local authorities
  - Lots of web articles about brand enforcement in GDPR era
- I would suggest to have a review from people having a legal background

Thanks for the attention!

Q & A