Open Questions on Security Issues for RDAP

Ning Kong

IETF 86, WEIRDS

Index

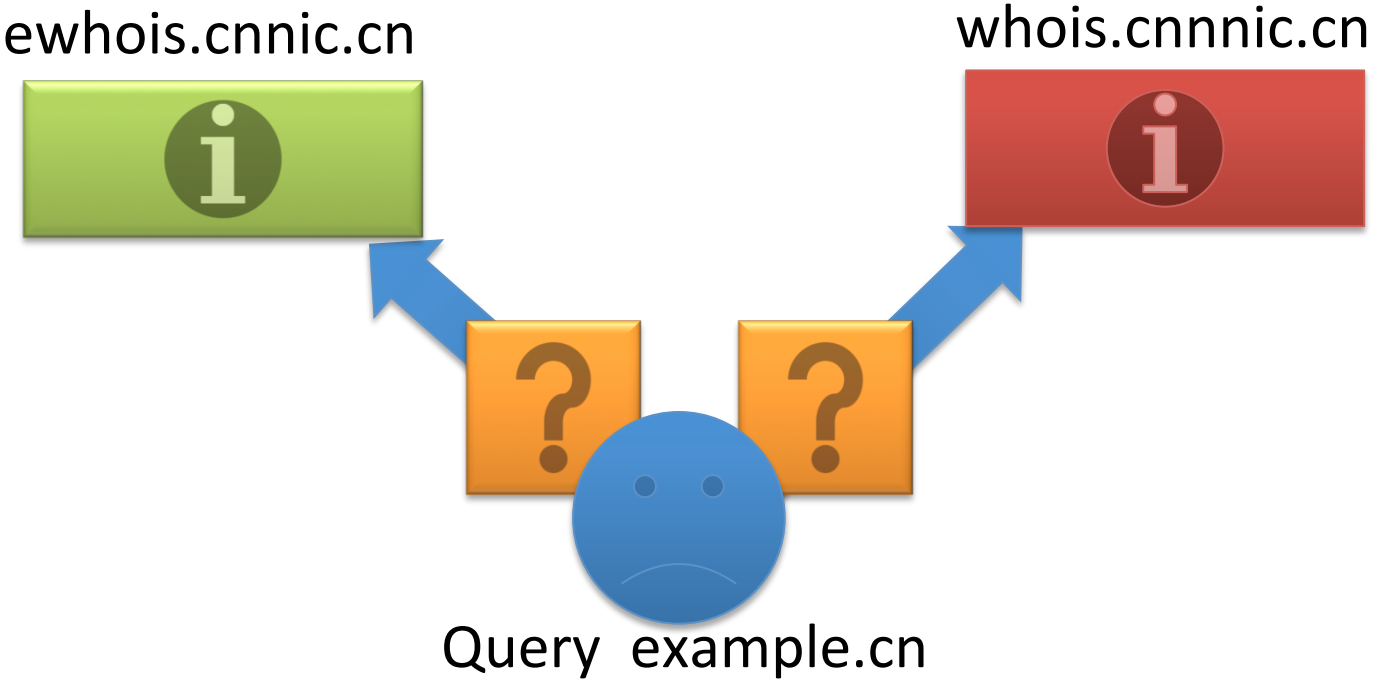
- #1 Federated Authentication
- #2 Server Authentication
- #3 Updated Authentication Approach
- #4 Data Integrity for Redirection Service
- #5 Data Abuse on Searchable RDAP

#1 Federated Authentication

- Is Federated Authentication only a policy issue?
- Do we need to identify technical approaches to develop Federated Authentication?
  - Oauth 2.0?
  - OpenID?
  - CA?
  - Others?

#2 Server Authentication

- Do we need to identify the approach to enable users to authenticate the identity of a WHOIS server or a redirect server?



#3 Updated Authentication Approach

- **Background:**
  - Basic and digest authentication mechanisms defined in RFC 2617 are not perfect, HTTPAUTH is planning to update them.
- Should RDAP follow the updated authentication mechanisms by HTTPAUTH?
- Should RDAP include some customized and form-based authentication methods?

#4 Data Integrity for Redirection Service

- **Background:**
  - Insure the redirection URL data must not be able to modify URL in data transmission process. See security considerations in draft-ietf-weirds-redirects-01
- Do we need to detail the approach for insuring data integrity of RDAP?

#5 Data Abuse on Searchable RDAP

- How to avoid abuse of searchable RDAP?
- Is this only a policy issue?
- Do we need to identify some technical approaches to avoid data abuse?

Any Comments?

Thanks!