Domain Registration Data - Use Case Exposition

LE/Anti-abuse/Registration Process/General commercial use

Determine “Reputation” of domain name and/or elements associated with domain name registrations

Goal/Scenario

Domain names, nameservers, registrants, and other attributes associated with registering domain names are often related to each other. Such relations can be used to create “reputation” for these attributes. Several organizations and services (e.g. Alexa, SURBL) use these relations and attributes of domain names to create a reputation “score” for domain names and their attributes. For this document, we’ll collectively call such entities, “reputation assessors”.

A reputation is typically expressed as either a scalar value like 0-100 to indicate confidence in a certain type of behavior, or a designation like “malicious”, “parking”, “enterprise”, “government”, etc. In some cases, reputation designations are provided along with scalar confidence levels. When a reputation assessor comes across a new domain name or domain name attribute, they will gather several data points to build their reputation data, including associated domains or domain registration attributes via common registration elements like registrant, nameservers, or contact e-mail addresses, along with a host of other information like a domain’s age, registration status, hosting location, nameserver configuration (e.g. fast-flux, corporate hosting, CDN), content of website, content of associated e-mail, etc. Typically new domains or elements will tend to cluster around certain parameters, allowing reputation to be determined transitively across such clusters.

Using the information provided by a reputation assessor, organizations can make decisions on subsequent actions. Typical uses include grey or black-listing domains for e-mail delivery or website resolution, allowing a domain registration to proceed or not (or be further scrutinized), informing legal actions like UDRP efforts or criminal investigations, determining search-engine rankings, or providing other services like CERTs or hosting.

NOTE: This is a use-case based on current practices that involves both today’s “regular” whois system directly, along with universal whois databases collected by outside organizations, including “whowas” type services.

Brief Format Use Case

Use Case: Determine “Reputation” of domain name and/or elements associated with domain name registrations.

Main Use Case – Domain name (element) reputation creation/update process: Automated reputation system (process) receives domain name or

domain name components to evaluate or update. Process accesses the RDS via established access methodology and authentication credentials. Process queries about one or more domain names to retrieve full information about the domain name(s) entered. If the starting point is a particular domain attribute like a nameserver or e-mail address, the RDS will create a list of domains with those attributes. Based on the results obtained, the RDS returns a list of domain names and potentially other information the process is entitled to given its credentials. The process then applies algorithms typically based on stored reputation data to assign reputation values/scores to the domain name or domain name attributes being scrutinized. The process will likely iterate on this case many times based on the information various searches reveal.

Casual Format Use Case

Title: Determine "Reputation" of domain name and/or elements associated with domain name registrations.

Primary Actor: Automated process running on system(s) of an authenticated user of the RDS system that is obtaining information related to domain name(s) or domain name attributes.

Other stakeholders: Operator of the RDS, registrant of queried domains, any listed contacts returned by querying the system, registrar/reseller of queried domains, providers for Internet services (web/e-mail/messaging/etc.) for the domain name.

Scope: Interacting with Domain Name Directory Service

Level: User Task

Data Elements:
Nameservers assigned to the domain names identified
e-mail addresses used to control the domain(s)
registrar(s)/reseller(s) of domain names identified
Domain registration/renewal date
Domain status
contact info associated with the domain name
- Name/Org Name
- e-mail address
- phone
- physical address

Story: Automated reputation system (process) receives domain name or domain name components to evaluate or update.
Process accesses the RDS via established electronic access methodology (API or other means) and authentication credentials.

The process queries about one or more domain names and/or data related to domain names that being scored and requests any domain names or other information tied to that input via a search capability.

Optional step: If the starting point is a particular domain attribute like a nameserver or e-mail address, the RDS will create a list of domains with those attributes.

Based on the results obtained, the RDS returns a list of domain names and potentially other information the process is entitled to given its credentials. Information that would likely be stored by the RDS that could be useful for scoring includes lists of related domains along with the full contact information (proxy and non-proxy) for the listed registrant, the e-mail addresses used to control the domain name, nameservers utilized by the domain name, registration status and dates of the domain(s) and the relevant registrar (and reseller), and service providers associate with the domain name(s).

The process then applies algorithms typically based on stored reputation data to assign reputation values/scores to the domain name or domain name attributes being scrutinized. The process will likely iterate on this case many times based on the information various searches reveal.

This process will be repeated on a regular basis – perhaps in near real-time, or in "batches" (e.g. when new zone files are published), and when new reputation scoring algorithms or weights are determined.

Reputation scores are then used for other processes including:
Creating and updating grey or black-listing domains for e-mail delivery or website resolution.
Determining whether to allowing a domain registration to proceed or not (or be further scrutinized)
Informing legal actions like UDRP efforts or criminal investigations
Improving search-engine rankings and/or warnings
Providing input into a CERT issuance process
Providing consumer confidence scores for a website
Alerting providers of potentially harmful presences on their networks/services
Providing input into sign-up processes for online services such as web hosting, online advertising, or e-mail marketing