The Registry of the Future

Cristian Hesselman¹, Giovane C. M. Moura¹, Ricardo de O. Schmidt², and Cees Toet¹

1: SIDN, the Netherlands
2: University of Twente, the Netherlands
Key Concept: TLD Control Plane

• Modular system that enables a registry to further increase the operational security and stability of its TLD by leveraging its key datasets (registrations, zone file, DNS queries)

• Motivation: protect TLD users from increasing number of attacks (such as phishing, DDoS, and malware), thus increasing added value of the TLD

• Approach: automatically share threat info with other players in the TLD (collaborative security) and adapt registry’s DNS anycast services more dynamically

• Today: overview and illustrate what it takes to run a control plane, using .nl (the Netherlands) as a use case
Required Functions
Required Functions

Function 1: DNS traffic import, storage, and retrieval

UNIVERSITY OF TWENTE.
Required Functions

Function 2: threat detection and automatic sharing

UNIVERSITY OF TWENTE.
Required Functions

UNIVERSITY OF TWENTE.
Required Functions

Function 4: TLD-level security and stability visualization

UNIVERSITY OF TWENTE.
Required Functions

Function 5: Privacy protection

TLD players such as:
- Access providers,
- Hosting providers,
- Registrars

---

TLD operator

Privacy Board

privacy policies

---

Standard text (24 pt.)

Level up

Level down

---

[Diagram of DNS services and threat detection]

- Traditional DNS Services
- Domain registration transactions (e.g., EPP)
- Zone file
- DNS anycast network
- DNS stats
- DNS traffic
- DNS Reconfiguration Module (DRCM)
- Threat Detection Modules (TDMs)
- ENTRADA (multi-node cluster)
- Dashboard
- Reconfig Commands
- Registration updates
- DNS stats
- DNS traffic
- DNS Reconfig Module
- DNS Stats
- DNS Traffic

---

[Diagram of roles and responsibilities]

- Registrant
- Registrar
- Access Provider
- Hosting Provider
- Resolver
- End-user
- www.example.nl
- Hosting Provider

---

Required Functions

- TLD operator
- Traditional DNS Services
- Control Plane
- TLD players such as:
  - Access providers,
  - Hosting providers,
  - Registrars

---

UNIVERSITY OF TWENTE.
Function 1: ENTRADA (entrada.sidnlabs.nl)
Function 2: Collaborative Security

User

Report Classifier

Judicial Authorities

Site Operator

Registrar

Registrant

Hosting Provider

Resolver Operator

Domain Classifier

DNS queries and responses (ENTRADA)

DNS Name Servers

domain name lookup (DNS)

JTIE interacties (index = domeinnaam)

DNS/EPP interaction

Threat intelligence flow

Domain Name Server

Criminal investigation

Technical operations

user reports

notifications

investigation

notifications

registration updates

notifications

registration updates

notifications

UNIVERSITY OF TWENTE.
Function 4: .nl Security Dashboard

Filter

Registrar
Registrar has Anomaly
Submit

Registrant ID
Anomaly Threshold

Registrations / 30 Minutes

From Feb 10, 2017 To Feb 17, 2017
Next Steps

• Flesh out TLD control plane functions through various collaborative research projects

• Incrementally transition the control plane into production

• Continue to share and discuss with the (technical) community

• Longer term: fully distributed control plane
  • Running at different DNS operators
  • Distributed threat detection/analysis
  • Sharing threat info using standard formats
  • Taking different privacy regulations into account
Q&A

Presentation based on:


URL: https://www.sidnlabs.nl/downloads/papers-reports/sidnlabs-commag.pdf