The Registry of the Future

Cristian Hesselman[1], Giovane C. M. Moura[1], Ricardo de O. Schmidt[2], and Cees Toet[1]

1: SIDN, the Netherlands
2: University of Twente, the Netherlands

Key Concept: TLD Control Plane

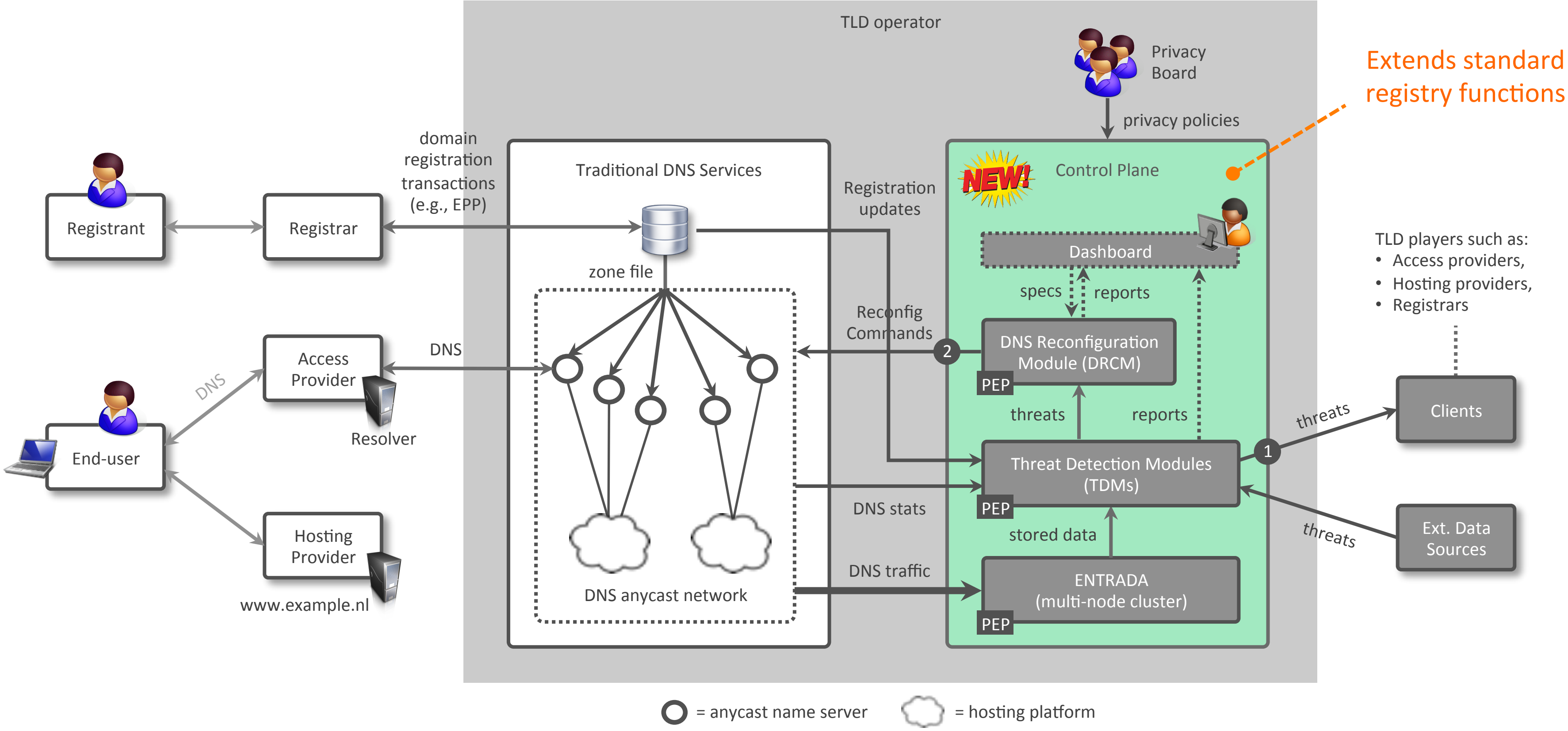
- Modular system that enables a registry to further increase the operational security and stability of its TLD by leveraging its key datasets (registrations, zone file, DNS queries)

- 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

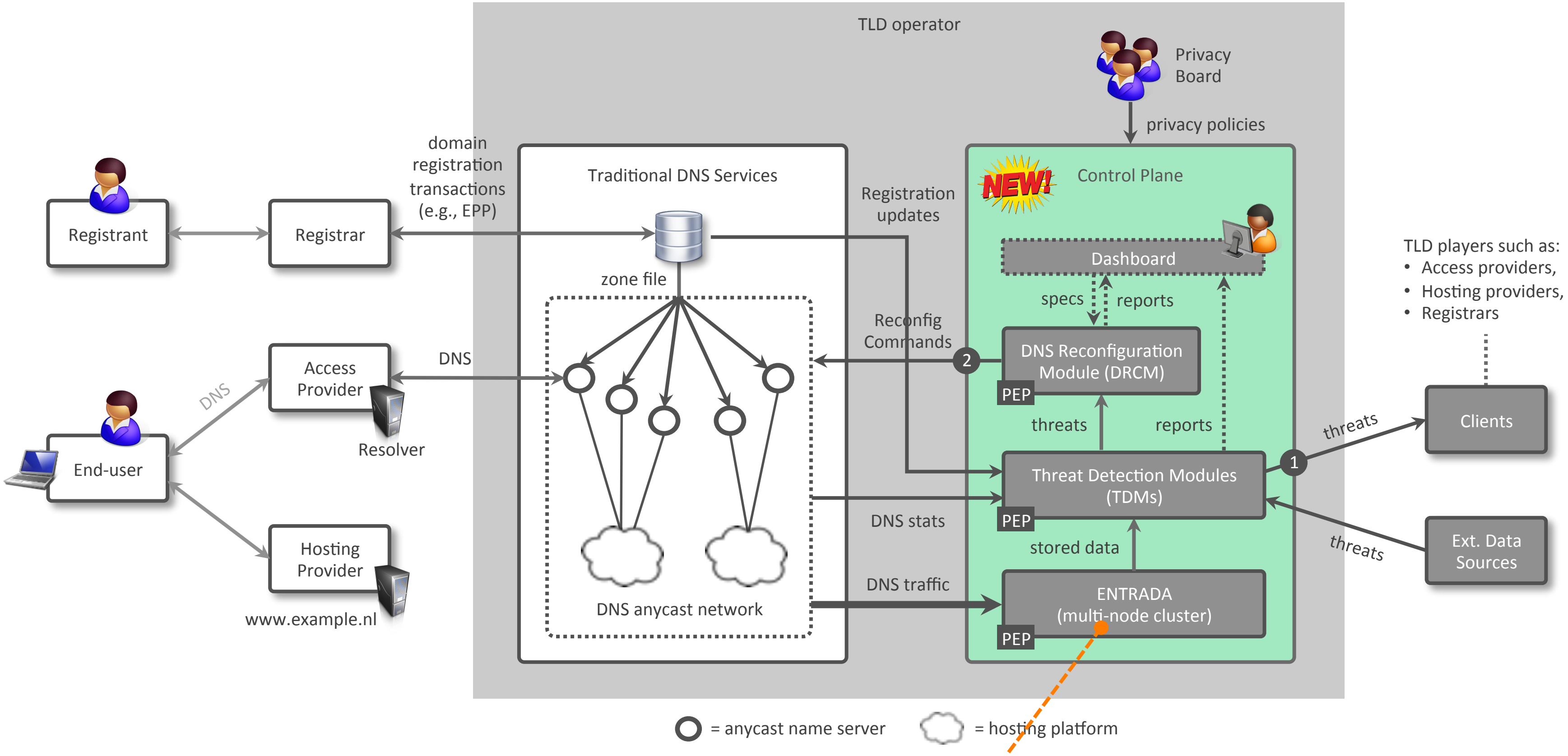
Required Functions



UNIVERSITY OF TWENTE.

SIDN LABS

Required Functions

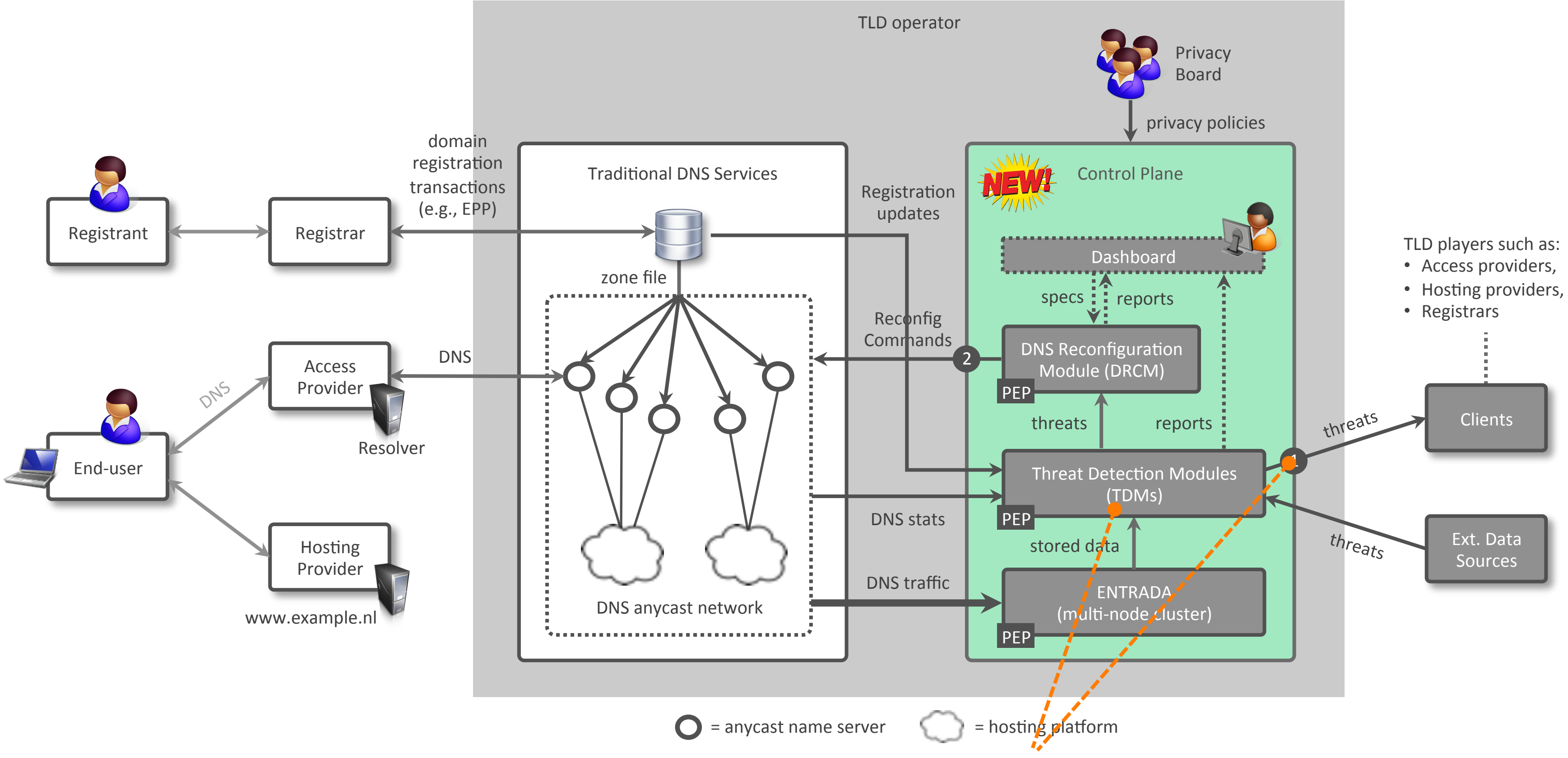


Function 1: DNS traffic import, storage, and retrieval

UNIVERSITY OF TWENTE.

SIDN LABS

Required Functions

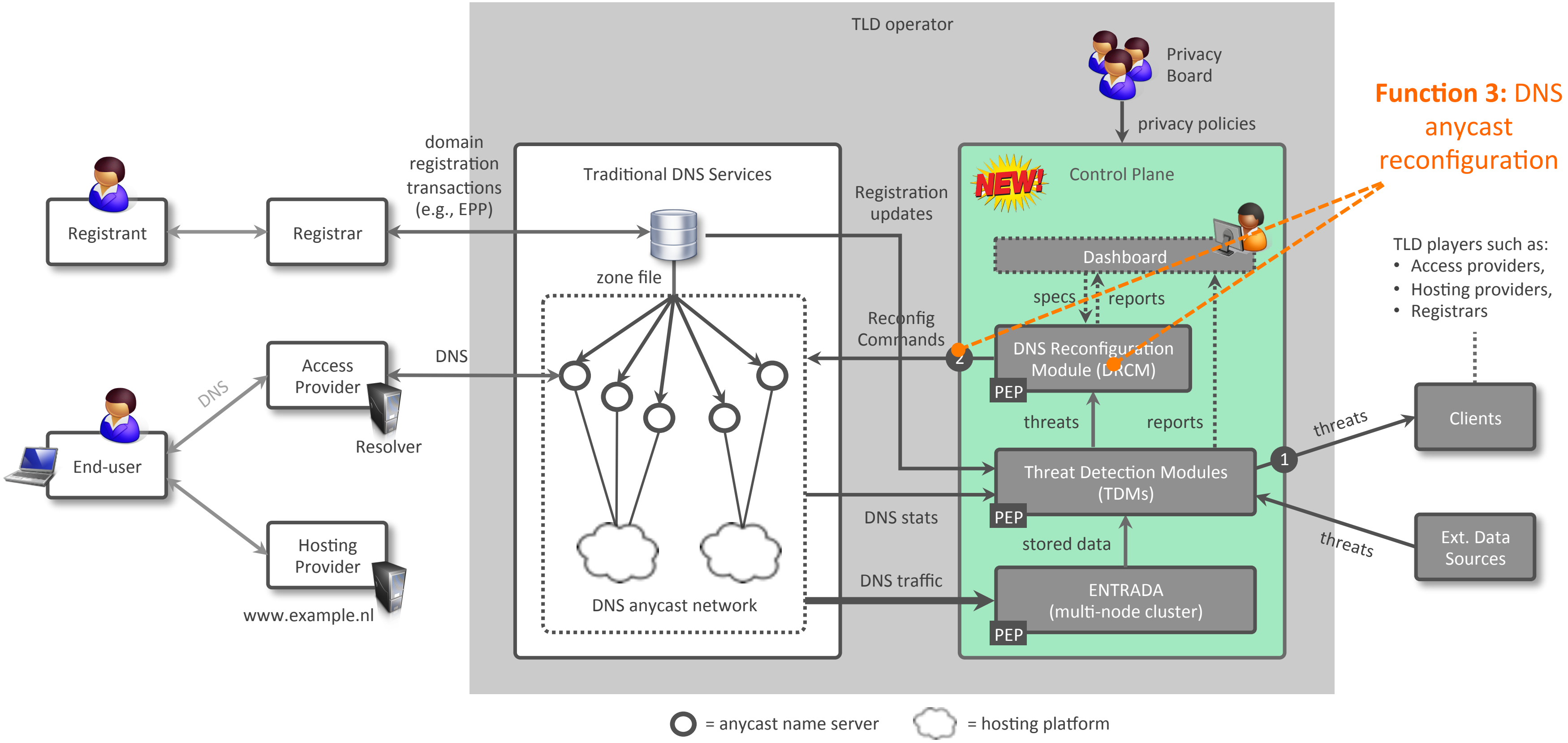


Function 2: threat detection and automatic sharing

UNIVERSITY OF TWENTE.

SIDN LABS

Required Functions

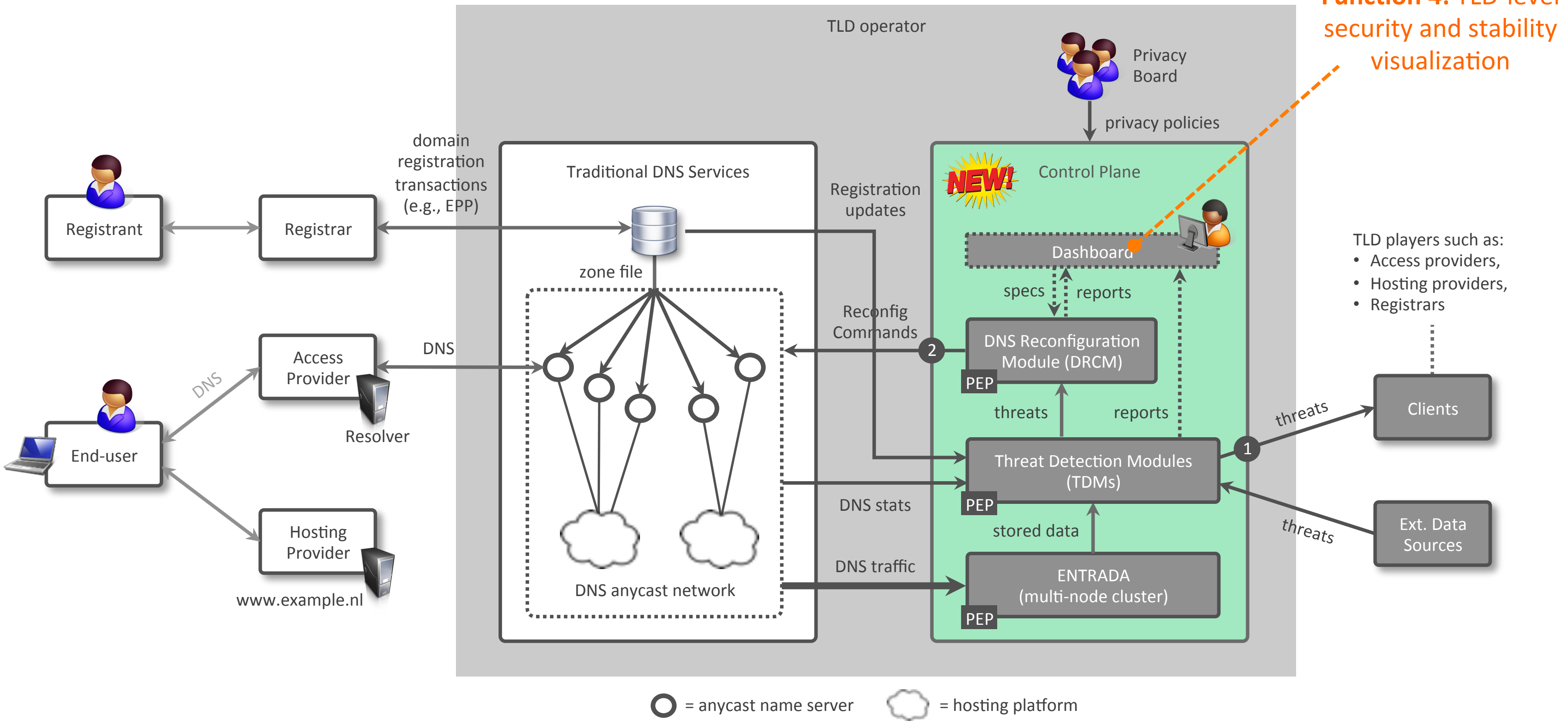


Function 3: DNS anycast reconfiguration

UNIVERSITY OF TWENTE.

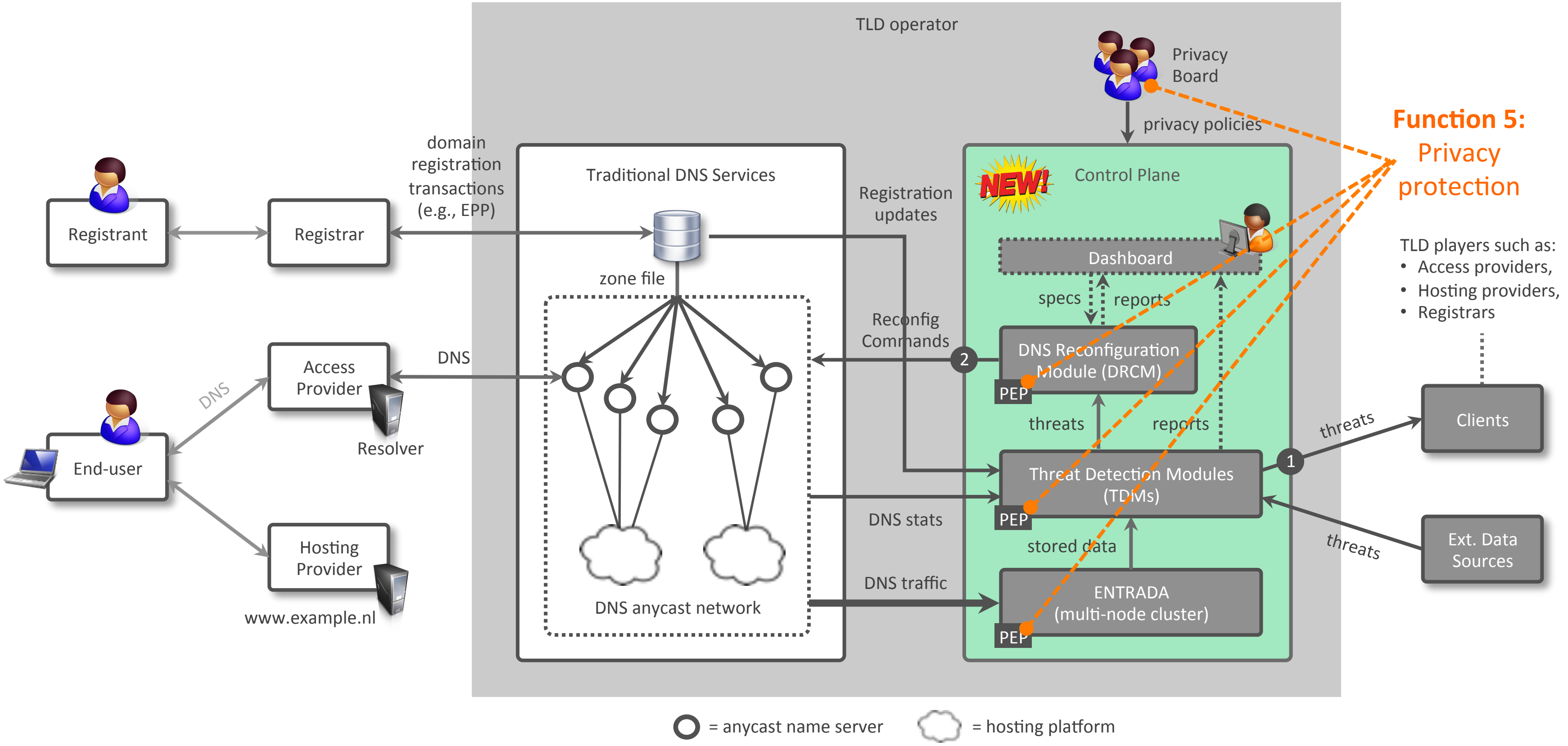
SIDN LABS

Required Functions



Function 4: TLD-level security and stability visualization

Required Functions



TLD operator

Privacy Board

privacy policies

Function 5: Privacy protection

Control Plane

NEW!

Registrant

Registrar

domain registration transactions (e.g., EPP)

Traditional DNS Services

zone file

Registration updates

Dashboard

specs

reports

Reconfig Commands

2

DNS Reconfiguration Module (DRCM)

PEP

TLD players such as:

- Access providers,
- Hosting providers,
- Registrars

DNS

Access Provider

Resolver

End-user

Hosting Provider

www.example.nl

threats

reports

Threat Detection Modules (TDMs)

PEP

1

threats

Clients

DNS stats

stored data

threats

Ext. Data Sources

DNS traffic

ENTRADA (multi-node cluster)

PEP

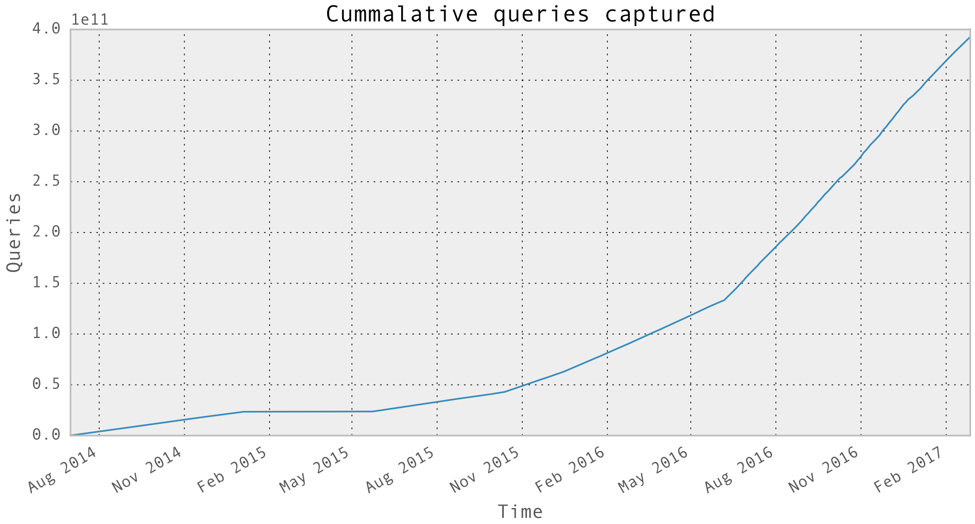
DNS anycast network

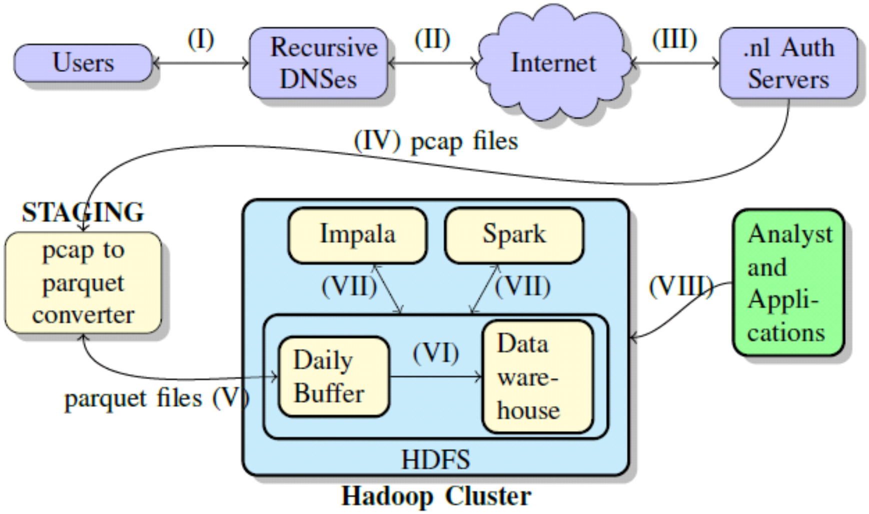
○ = anycast name server ☁ = hosting platform

Function 1: ENTRADA (entrada.sidnlabs.nl)

Maarten Wullink @Wulliak · 9 Dec 2016

Expanding our #entrada #hadoop cluster with 108TB storage. entrada.sidnlabs.nl pic.twitter.com/8UfggXiXcL

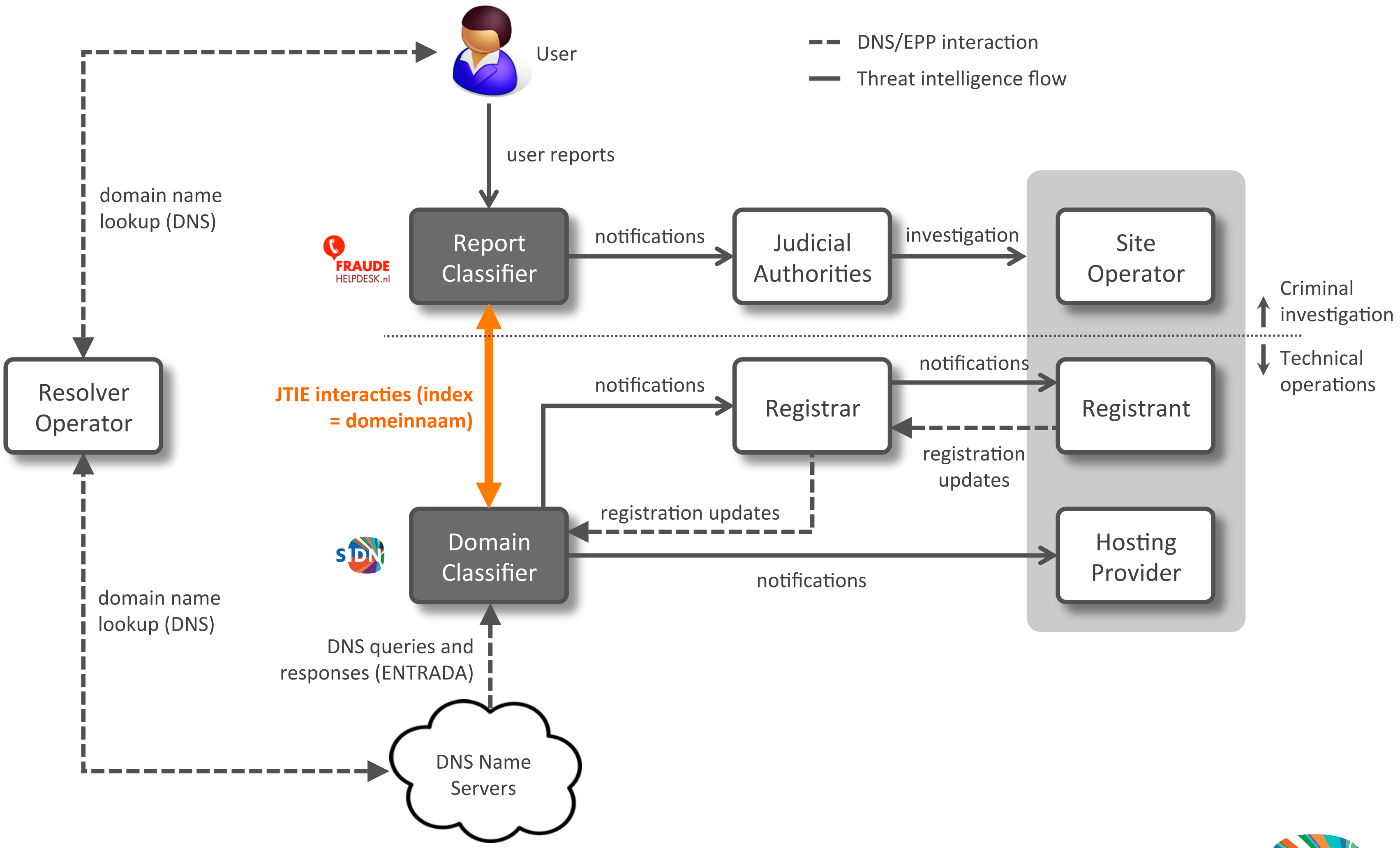




UNIVERSITY OF TWENTE.

SIDN LABS

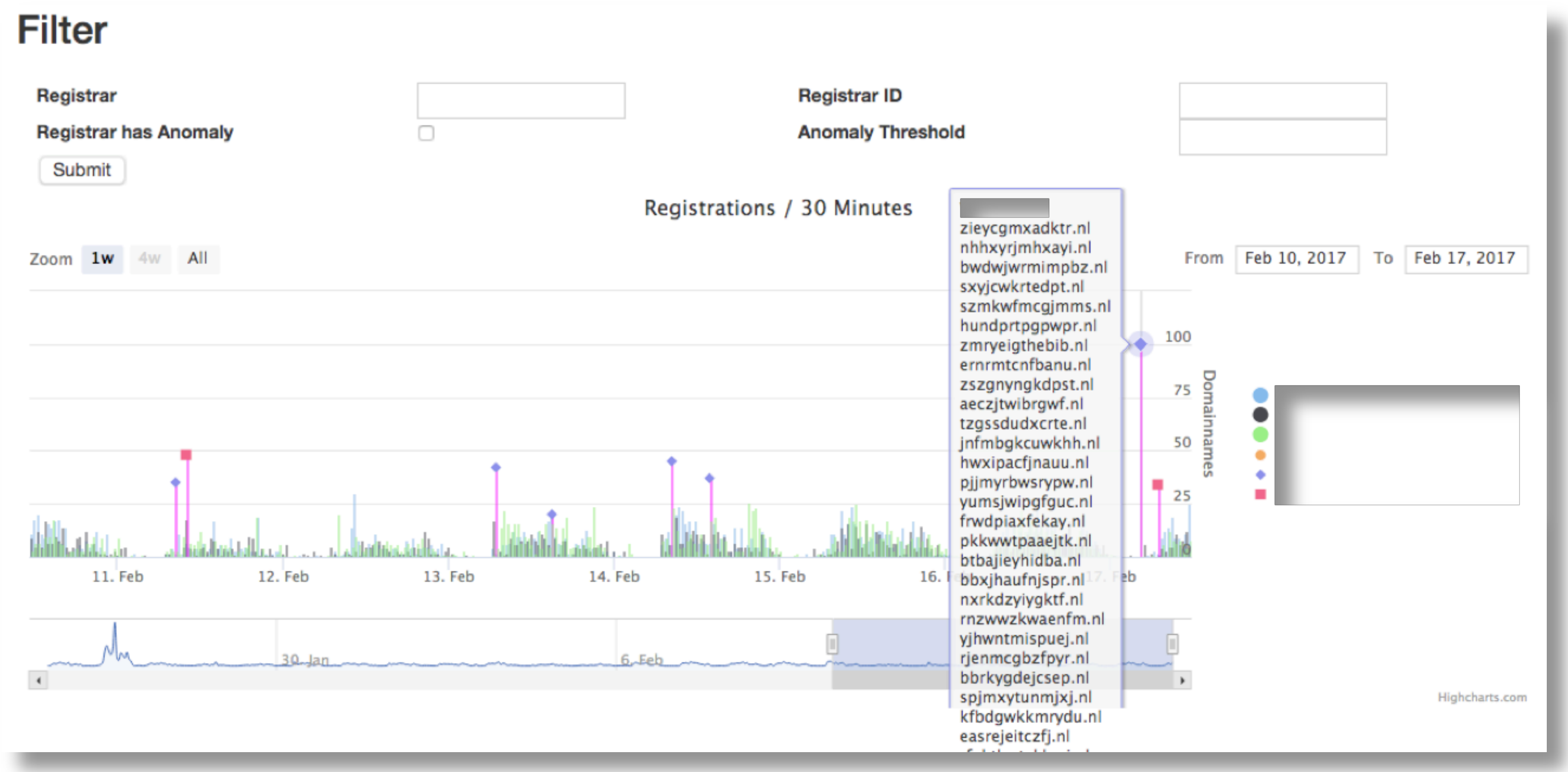
Function 2: Collaborative Security



UNIVERSITY OF TWENTE.

SIDN LABS

Function 4: .nl Security Dashboard



Filter

Registrar		Registrar ID	
Registrar has Anomaly	□	Anomaly Threshold	

Submit

Registrations / 30 Minutes

Zoom 1w 4w All

From Feb 10, 2017 To Feb 17, 2017

[redacted]

zieycgmxadktr.nl
nhhxyrjmhxayi.nl
bwdwjwrmimpbz.nl
sxyjcwkrtedpt.nl
szmkwfmcgjmms.nl
hundprtpgpwpr.nl
zmryeigthebib.nl
ernrmtcnfbanu.nl
zszgnyngkdpst.nl
aeczjtwibrgwf.nl
tzgssdudxcrte.nl
jnfmbgkcuwkhh.nl
hwxipacfjnauu.nl
pjjmyrbwsrypw.nl
yumsjwipgfguc.nl
frwdpiaxfekay.nl
pkkwwtpaaejtk.nl
btbajieyhidba.nl
bbxjhaufnjspr.nl
nxrkdzyiygktf.nl
rnzwwzkwaenfm.nl
yjhwntmispuej.nl
rjenmcgbzfpyr.nl
bbrkygdejcsep.nl
spjmxytunmjxj.nl
kfbdgwkkmrydu.nl
easrejeitczfj.nl

[redacted]

UNIVERSITY OF TWENTE.

SIDN LABS

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

Follow us

.nl SIDN.nl

@SIDN

in SIDN

Q&A

Presentation based on:

C. Hesselman, G. Moura, R. de O. Schmidt, and C. Toet, *"Increasing DNS Security and Stability through a Control Plane for Top-level Domain Operators"*, IEEE Communications Magazine, Network and Service Management Series, January 2017

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

UNIVERSITY OF TWENTE. SIDN LABS