SECURING THE ROOT: A CONTROL PLANE APPROACH FOR TLD STABILITY

Sunčica Rosić

NextGen@ICANNN

THE CRITICAL ROLE OF DNS

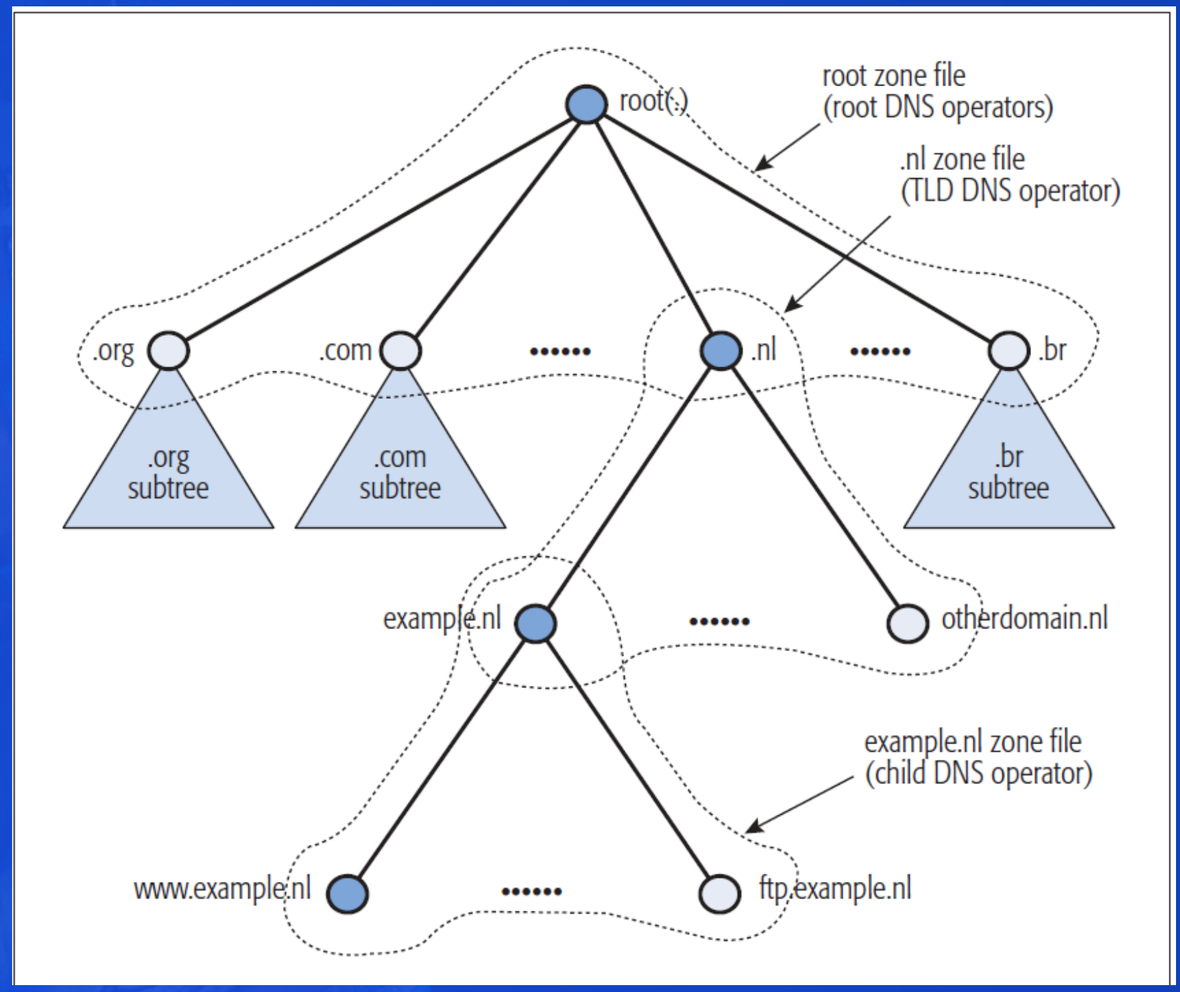
DNS is a critical part of the Internet infrastructure.

DNS replaced earlier methods (HOSTS.TXT) to provide scalable domain name to IP address mappings.

The DNS uses a hierarchical, tree-like structure with authoritative name servers at each level.

Top-Level Domains (TLDs) are the second level in this hierarchy (e.g., .org, .nl).

TLD operators manage the authoritative name servers and the database of registered second-level domains.



DNS Naming Hierarchy

A NEED FOR A CONTROL PLANE

Goal: Leverage TLD operator data to detect potential threats and automatically reconfigure name servers.

Existing threat detection and DNS reconfiguration are often manual and ad hoc tasks.

A novel system, a "control plane," is proposed to extend traditional services.

This system automatically derives potential threats and makes information available to other TLD players (hosting/access providers, registrars).

INTRODUCING CONTROL PLANE

> **A system built on a set of open source modules on a Hadoop-based data storage cluster**

Key datasets leveraged:

Large amounts of DNS traffic handled by authoritative servers.

The TLD's database of registered domain names.

These datasets offer a real-time centralized view that lower-level operators lack, aiding detection of coordinated malicious activity across registrars.

The control plane includes policies to protect the privacy of TLD users.

CORE FUNCTIONS

1

Threat Detection

Purpose Automatically detect potential threats (e.g., phishing domains, name server unavailability)

2

On-Demand DNS Reconfiguration

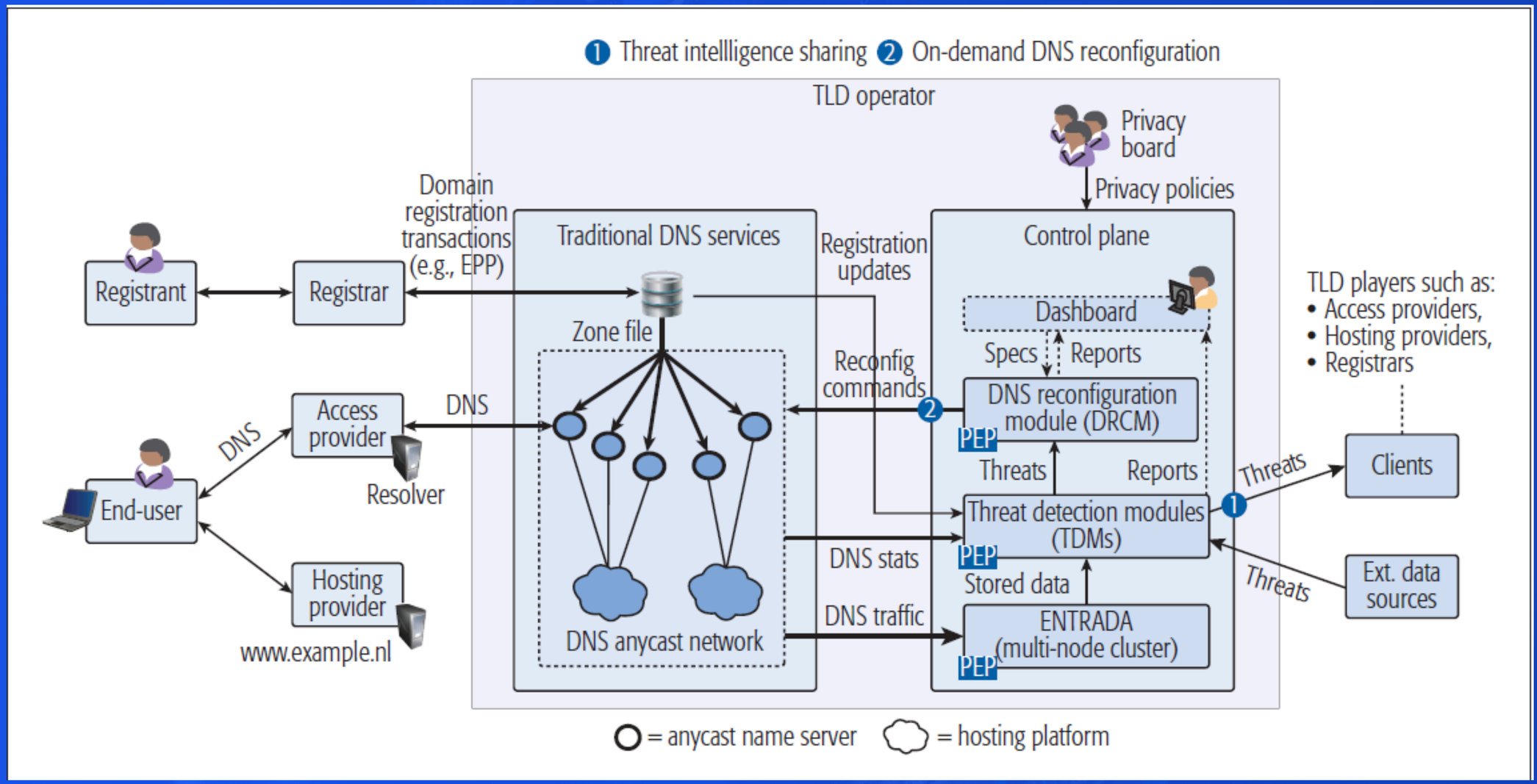
Purpose Dynamically adapt the TLD operator's DNS anycast infrastructure

3

Privacy Protection

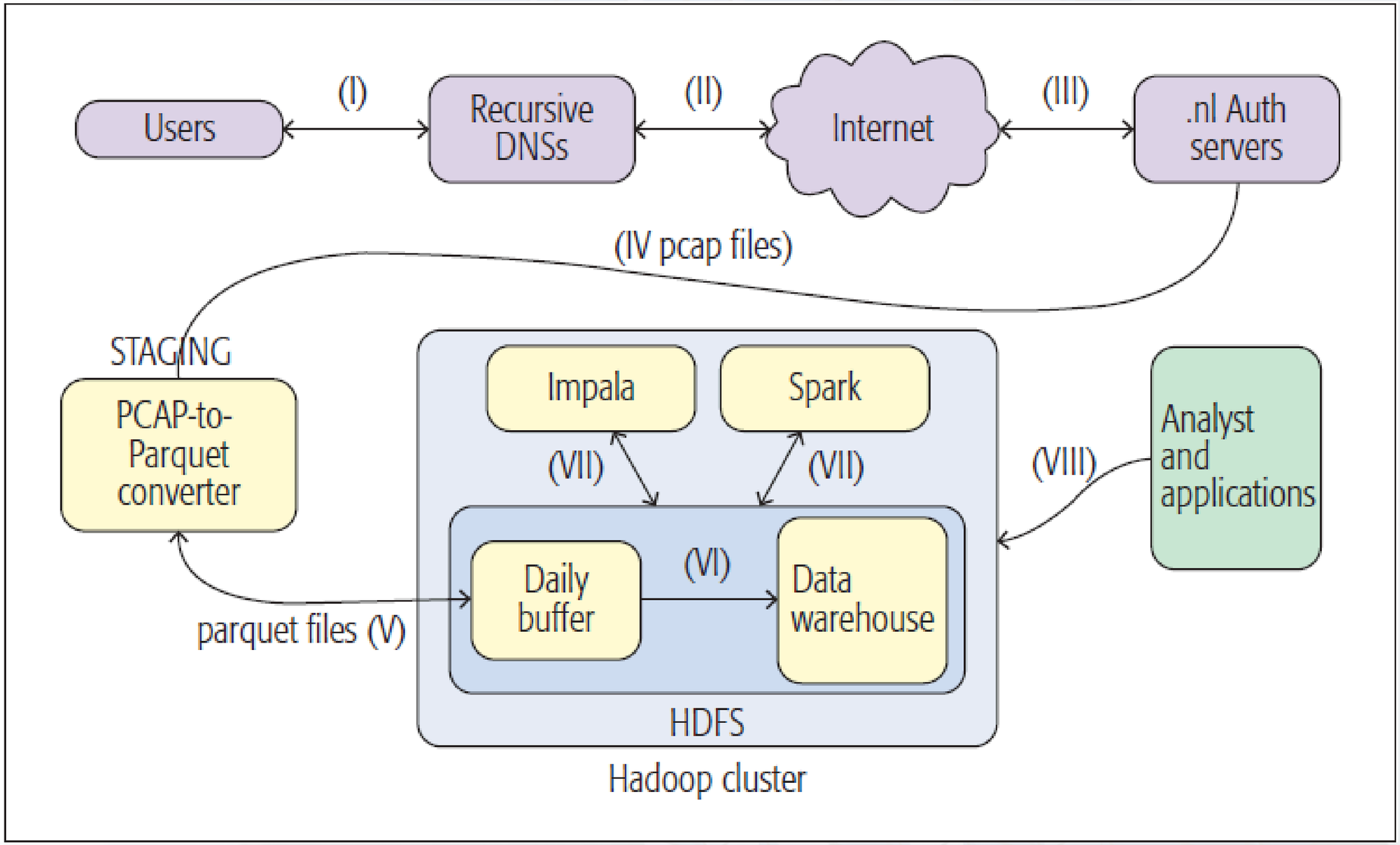
Purpose Systematically balance user privacy and increased TLD security/stability

CONTROL PLANE ARCHITECTURE



A TLD operator’s traditional DNS services (left) and its control plane (right).

ENTRADA - THE DATA ENGINE



ENTRADA overview.

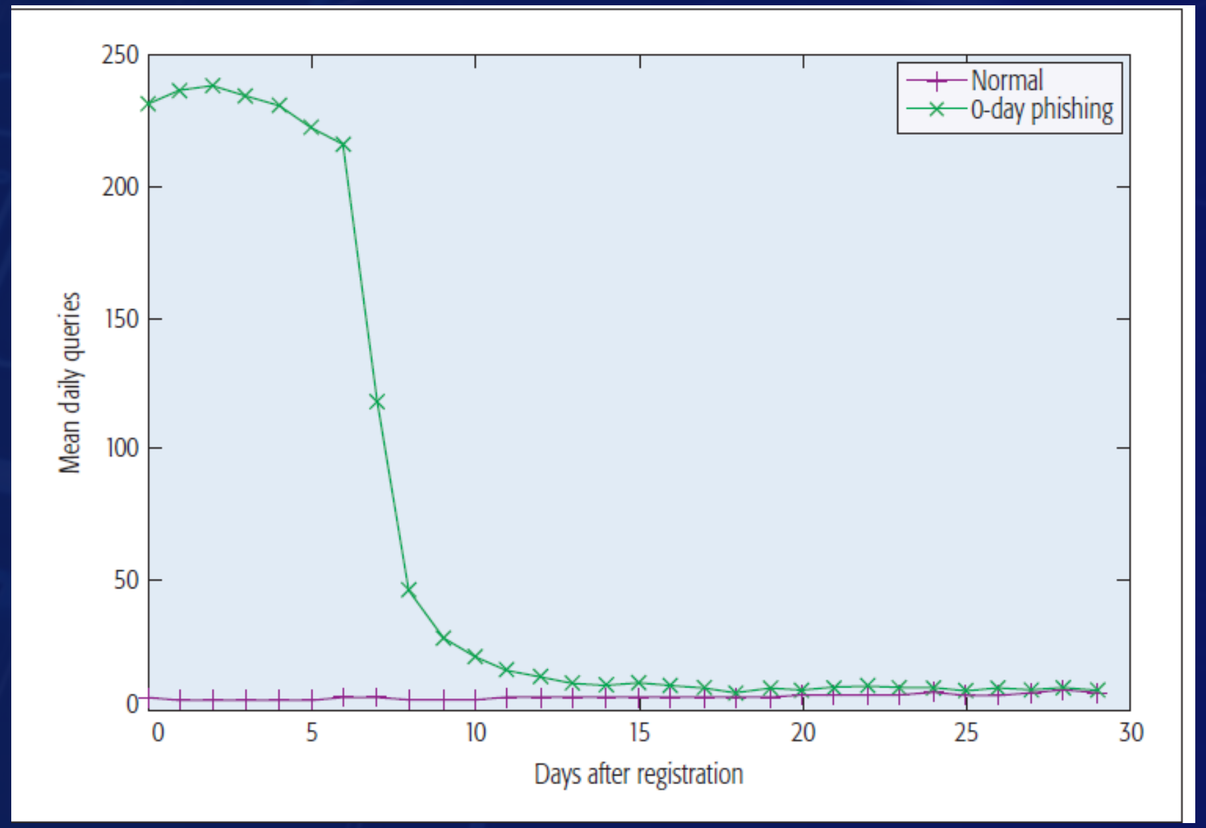
THREAT DETECTION MODULES (TDMS)

Applications running on ENTRADA that discover potential threats.

Combine TLD data (traffic, database) with external feeds (e.g., ShadowServer).

Examples:

- nDEWS (New Domains Early-Warning System)
- Botnet Detection



Queries to normal and phishing domains.

DNS RECONFIGURATION MODULE (DRCM)

Purpose: Dynamically adapt the DNS anycast infrastructure.

Handles threats like DDoS attacks (name server unavailability).

Involves starting and stopping virtualized DNS name servers at hosting platforms.

Manages a dynamic set of name servers, unlike today's mostly static networks.

Requires interfacing with name servers to send commands.

Gathers statistics (resource usage, EDNS Client-Subnet - ECS) to inform decisions. ECS can map query demand to client location.

Research suggests connectivity is more important than the sheer number of anycast sites for performance and stability.

CONLUSION

The control plane enables TLD operators to enhance security and stability by becoming threat intelligence providers.

It extends traditional services by leveraging and analyzing DNS traffic and registration data.

Automatically detects threats and shares information with other TLD ecosystem players.

Can also dynamically scale DNS infrastructure for increased robustness.

Built on the open source ENTRADA software (Hadoop-based).

ENTRADA is being used by at least six country code TLD operators.

REFERENCES

C. Hesselman, G. C. M. Moura, R. De Oliveira Schmidt and C. Toet, "Increasing DNS Security and Stability through a Control Plane for Top-Level Domain Operators," in IEEE Communications Magazine, vol. 55, no. 1, pp. 197-203, January 2017, doi: 10.1109/MCOM.2017.1600521CM. keywords: {Servers;Databases;IP networks;Internet;Computer crime;Stability analysis;Telecommunication network management},