DNSAttackStream Prototype

Introduction

In the frame of the MADDVIPR project, studying the impact of Distributed Denial of Service (DDoS) attacks against DNS infrastructure represent a pillar of our research.
DDoS attacks, with their rising firepower, can cause serious issues to DNS infrastructure and the global internet. To understand how DDoS attacks affect DNS infrastructure, we developed the prototype of DNSAttackStream, which enabled us to provide a live overview of the impact of these attacks on the global DNS ecosystem.

Architecture

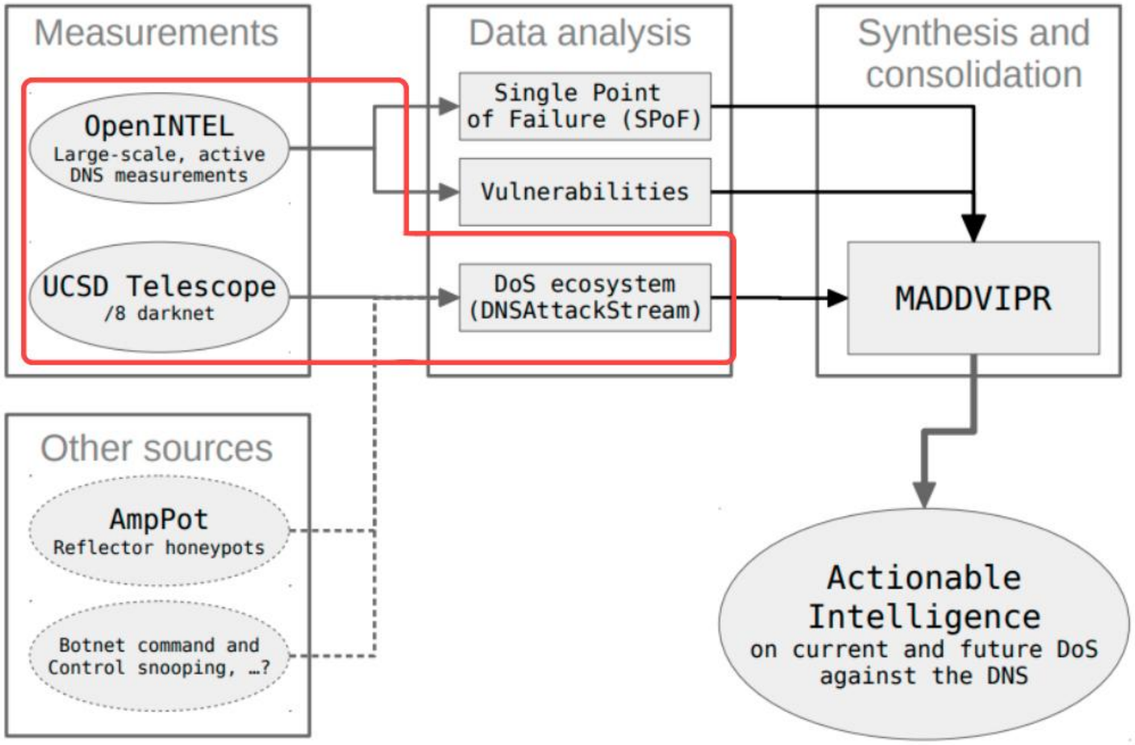
Measurements
OpenINTEL
Large-scale, active DNS measurements
UCSD Telescope
/8 darknet
Data analysis
Single Point of Failure (SPoF)
Vulnerabilities
DoS ecosystem (DNSAttackStream)
Synthesis and consolidation
MADDVIPR
Other sources
AmpPot
Reflector honeypots
Botnet command and Control snooping, …?
Actionable Intelligence
on current and future DoS against the DNS

Figure 1. MADDVIPR Architecture

DNSAttackStream represents the first step in integrating different data sources into the MADDVIPR framework. We started with RS-DoS (Reflected Spoofed Denial of Service) attack information, collected by the UCSD STARDUST project, and joined it with OpenINTEL live measurements. DNSAttackStream merges the obtained information of IP addresses inferred to be under attack based on the STARDUST (UCSD Network Telescope) data every 5 minutes with the list of IP addresses of authoritative nameservers measured by OpenINTEL.
This mechanism allows us to provide insights into the number of authoritative nameservers and related Second Level Domains (SLDs) affected by attacks.

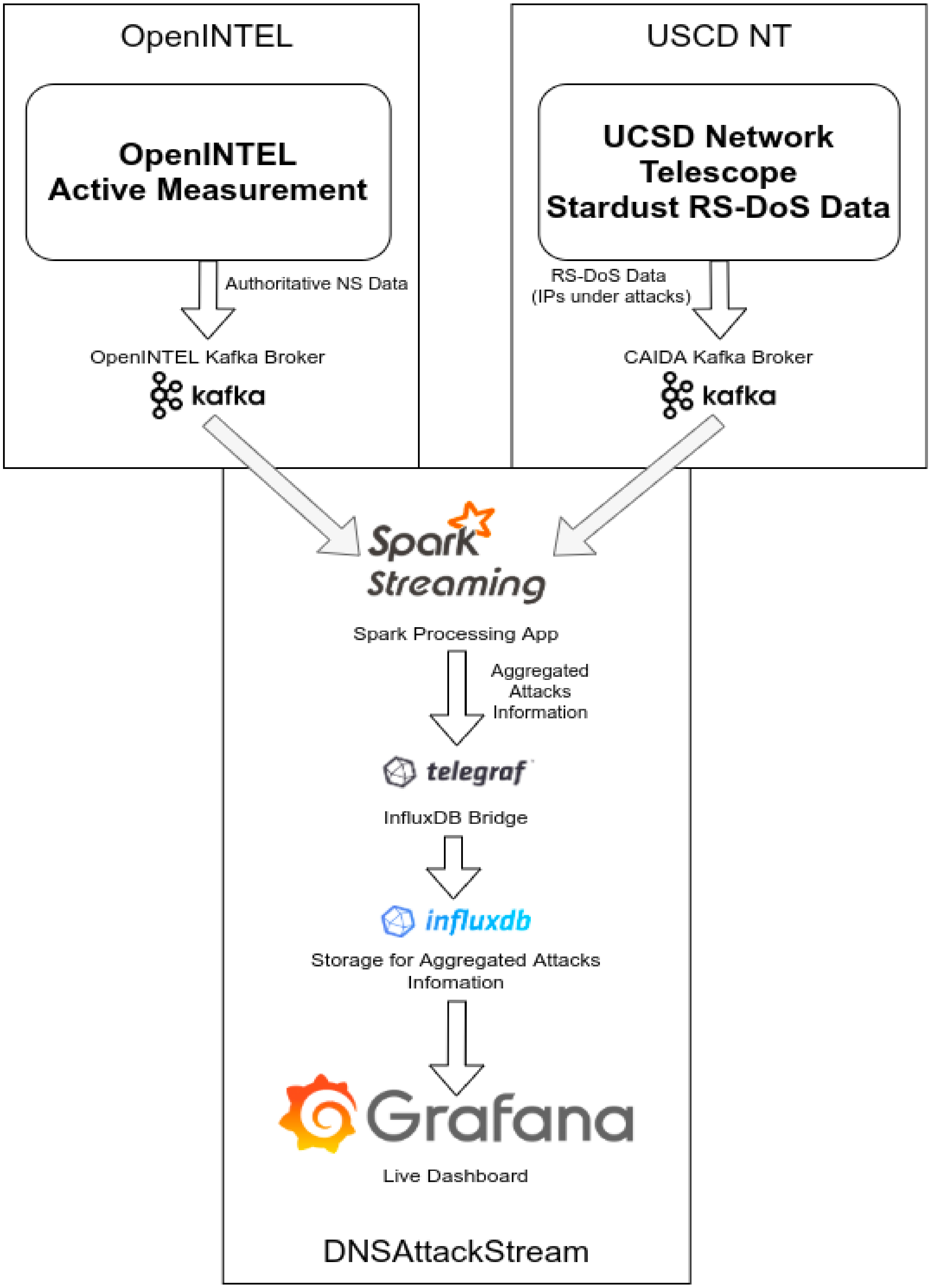

Figure 2. DNSAttackStream overview

To integrate these two sources of information, we implement a streaming pipeline, using Kafka as a message broker for retrieving live data, a Spark streaming application for joining the two live datasets, Telegraf as middleware for InfluxDB, InfluxDB for storing time series of aggregated attacks information, and finally Grafana for the implementation of a live dashboard.

Live Dashboard

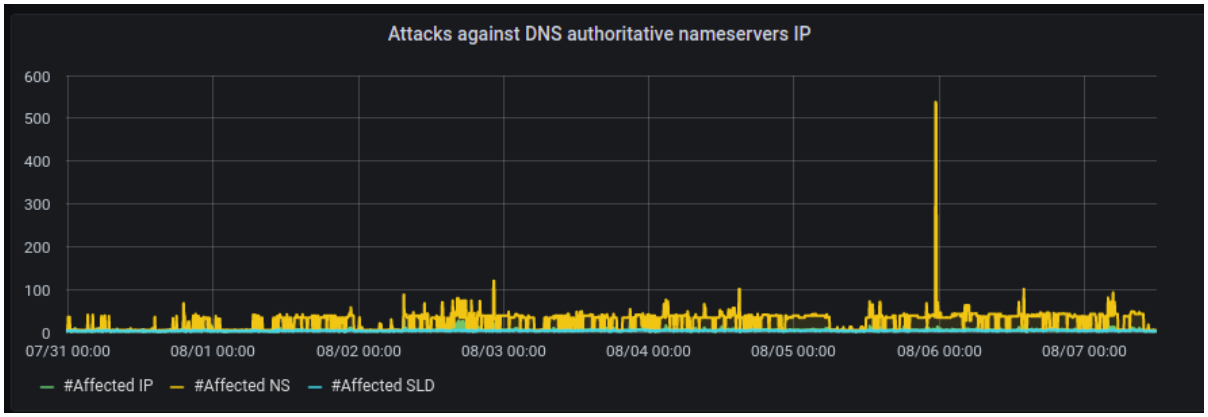

Figure 3. Cumulative impact of attacks against DNS infrastructure

The Dashboard provides live and historical insights on attacks against DNS and offers the possibility to filter out data by IP under attack, nameserver, and TLDs of the target SLDs.

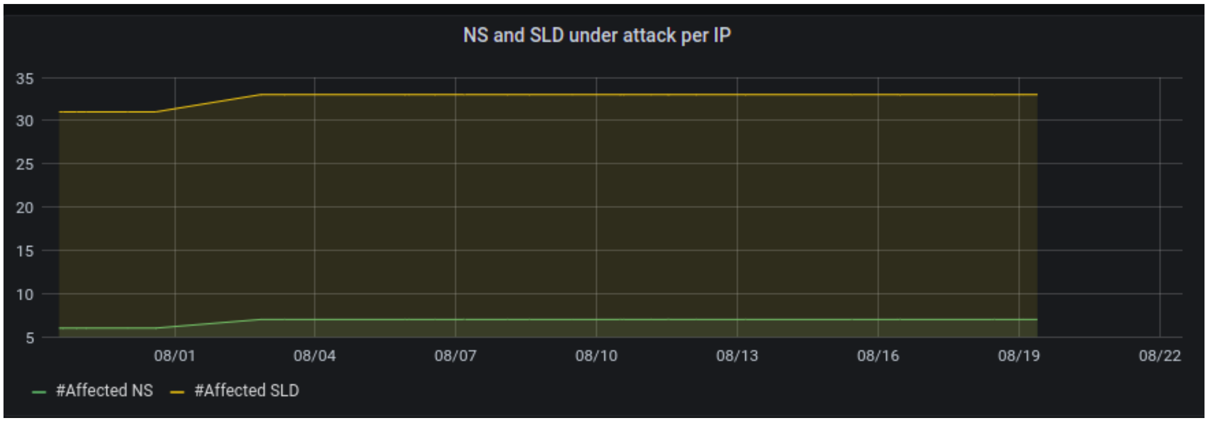

Figure 4. Impact on SLDs and NSes for a single IP under attack.

This granularity enables us to present the data in different ways to facilitate exploration and analysis of each attack.

Please note that the dashboard will be subject to architectural changes in the future to expand the platform and enrich the data provided. We are also engaged in active development of the OpenINTEL cluster.