
Relazione sullo stato del progetto:

DyNE

(Dynamic Network Enumeration)

Antony Chiossi • 04/06/2019

Overview

Introduction

- Context and main problem
- Start point
- Network reconnaissance
- The DyNE project
- Road map

-
- Introduction
 - **Context and Main Problem**
 - Network reconnaissance

Context and Main Problem

Companies/Agencies/Institutions

- Huge networks with an increasing amount of connected devices
 - Legacy system
 - Policies like bring your own device
 - What is running on these devices
-

-
- Introduction
 - **Context and Main Problem**
 - Network reconnaissance

Context and Main Problem

Solutions:

- Active and passive reconnaissance
 - Situation awareness tools
-

Network reconnaissance

- Context and Main Problem
- **Network reconnaissance**
- Starting point

Active

- Actively collects informations by to probing all devices connected to the target network

Passive

- Passively collects and infers informations about devices and their communications protocols.

The main purpose of these two methodologies is to collect as much information as possible about the targeted network.

-
- Starting point
 - Network reconnaissance
 - DyNE

Start point

Open-source project:

- Censys (censys.io)
- Ivre (ivre.rocks)

Side notes: Ivre is very poorly documented and lacks of engineeristic approach to the implementation of the system software.

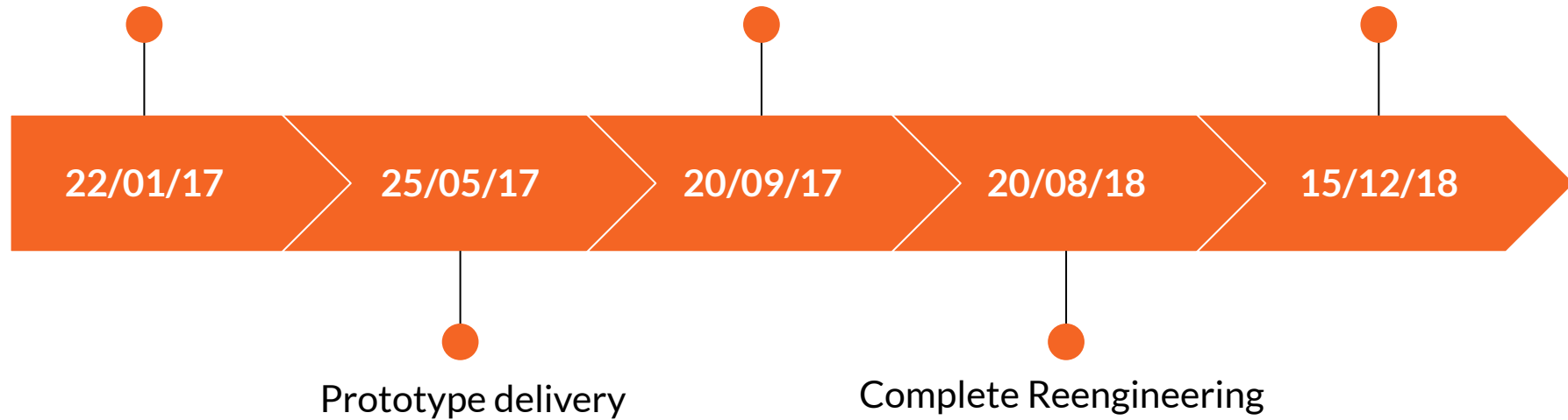
DyNE

(Dynamic Network Enumeration)

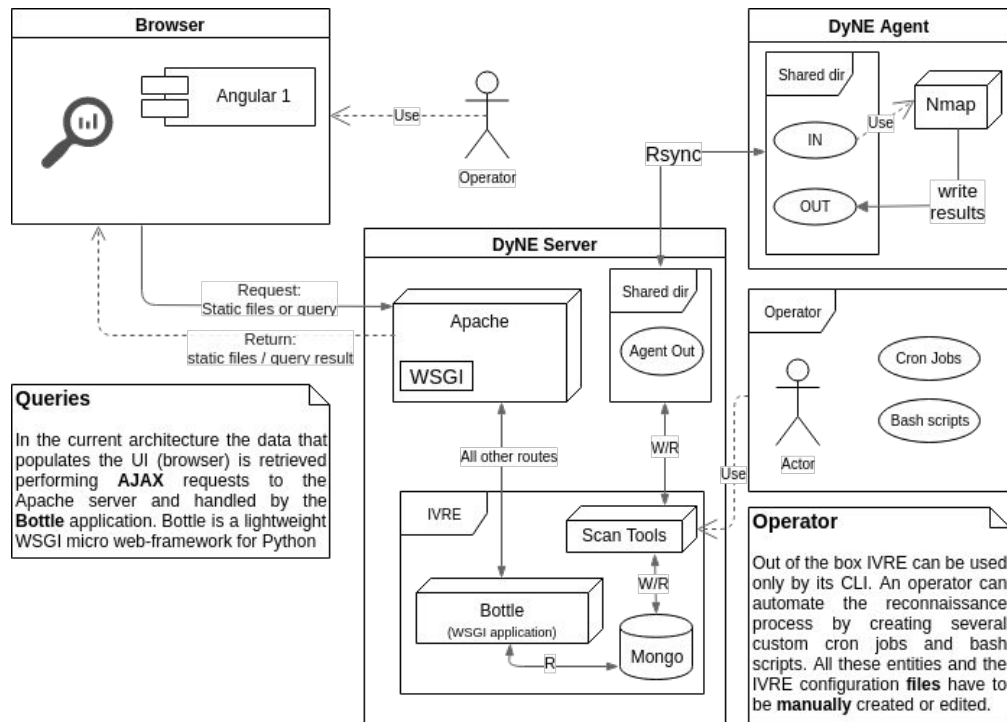
Internship starts

Enhancements

Contribution to IVRE



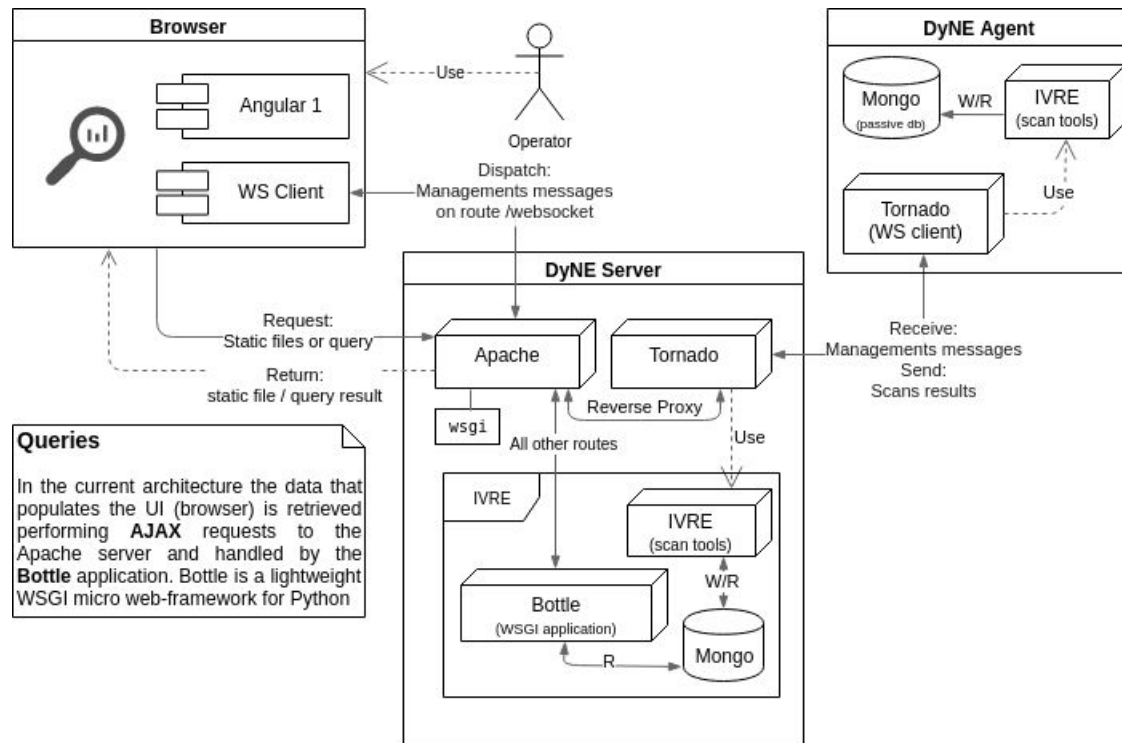
IVRE Architecture



IVRE

1. Hard to install and use
2. Hard to manage and maintain
3. Can be automated

DyNE Architecture (modern approach - 1/2)

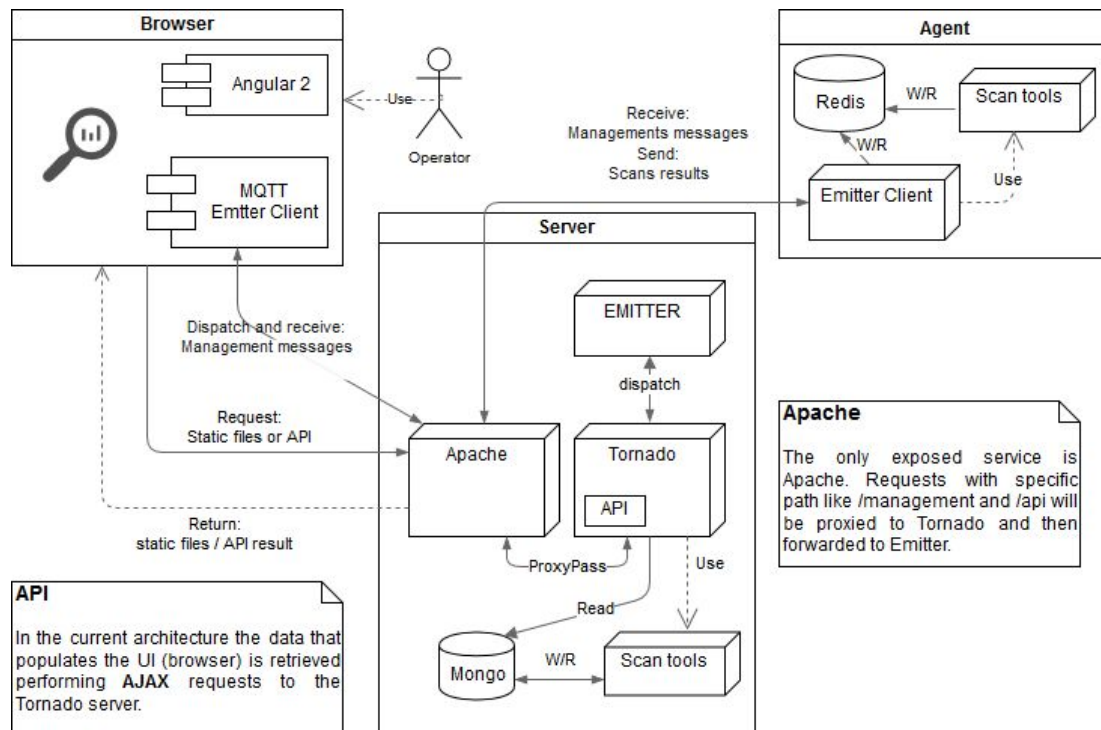


DyNE

(modern approach - first attempt)

1. New Communication Protocol
2. Real-Time
3. Single Point of Access
4. Automated main processes
5. Easy to use and maintain
6. Not fault tolerant

DyNE Architecture (modern approach - 2/2)



DyNE

(modern approach - second attempt)

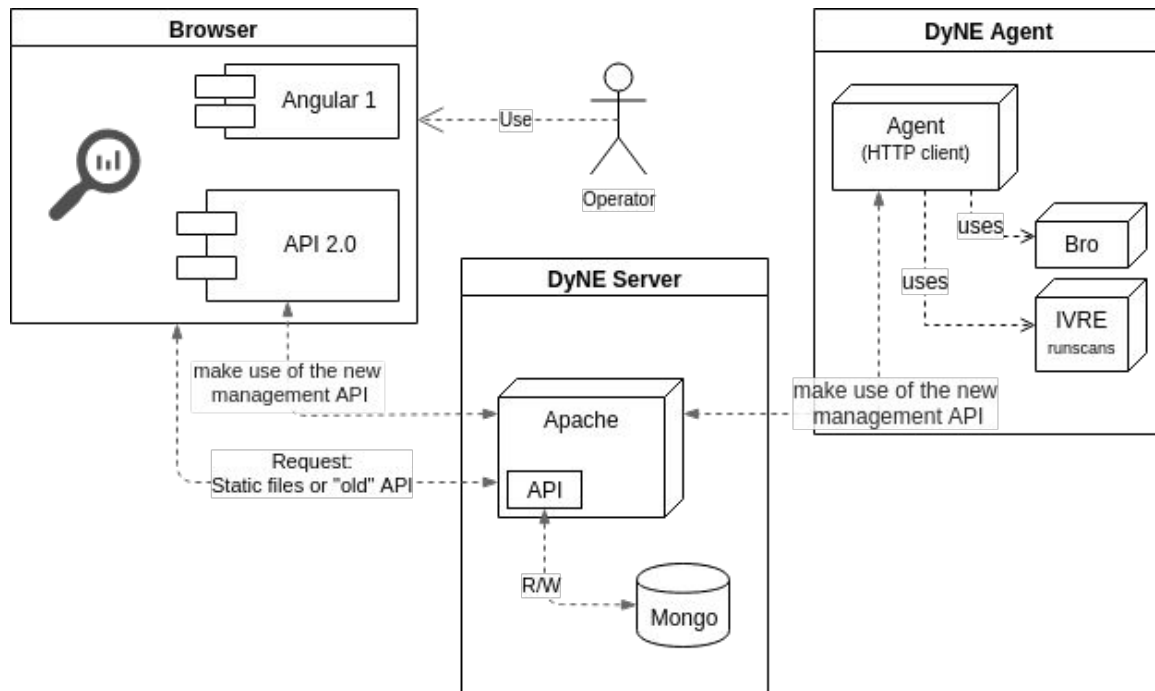
1. Message Broker (MQTT)

- 1.1. Scalable
- 1.2. Distributed
- 1.3. Publish-subscribe

2. Real-Time

3. Fault tolerant

DyNE Architecture (definitive)



DyNE

(conservative approach)

1. HTTP requests
 2. Not Real-Time
 3. Fault tolerant
 4. RESTful API
 5. Task Concept
-