TRUST aWARE

Enhancing Digital Security, Privacy and TRUST in softWARE

Static & Dynamic Analysis

Aniketh Girish, Gabriel Bogdan Hortea

Milan 26-27 March 2024 / FORUM ABI Lab

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

TRUST aWARE

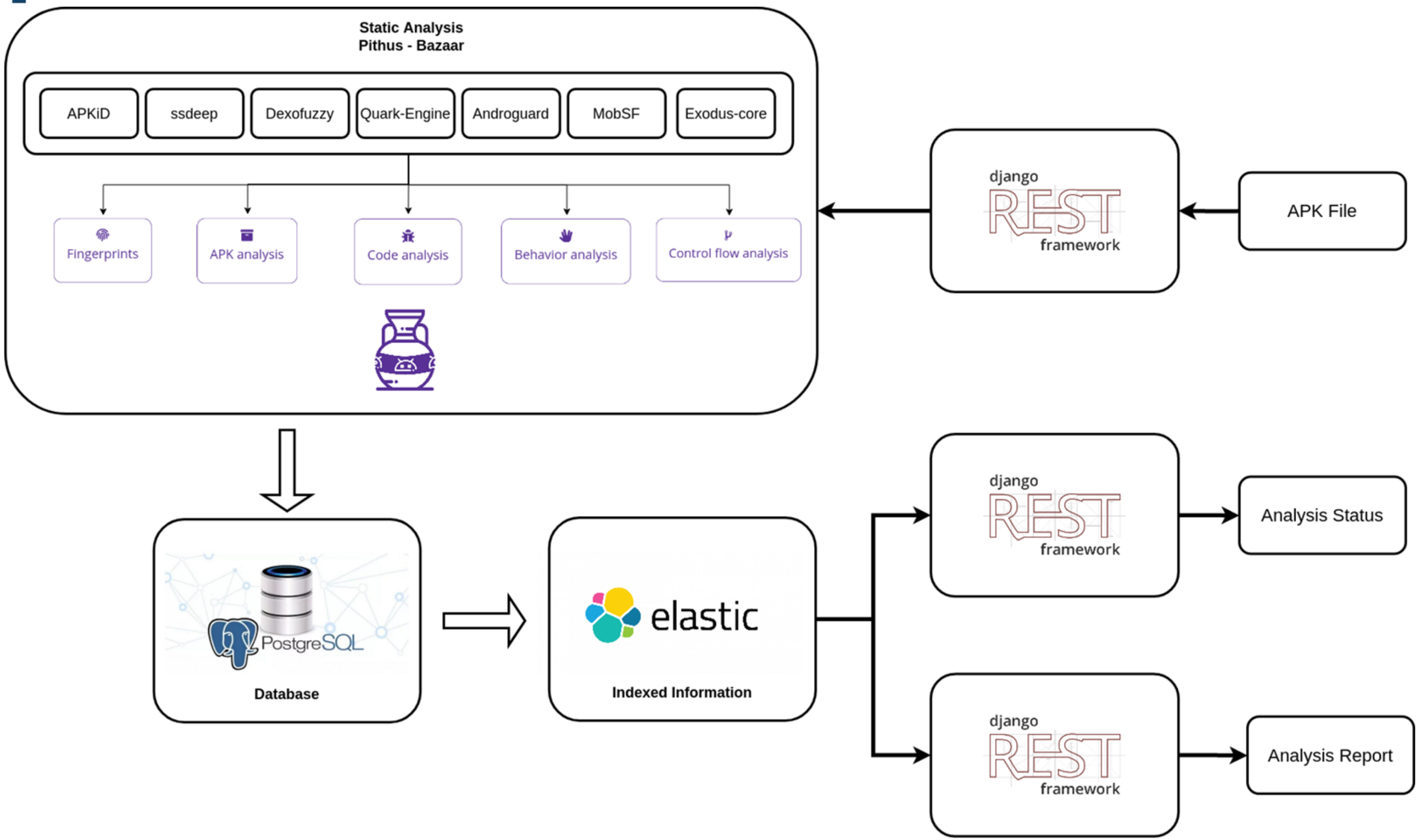
CONTENTS

Introduction - Importance of Software Analysis

- **Software Privacy & Security Challenges:** Modern software collects user data for commercial purposes, employing obfuscation techniques to avoid scrutiny, posing risks to uninformed users.
- **Dependency Dilemma:** Developers depend on third-party libraries, introducing privacy and security risks into the software supply chain, despite bearing responsibility for software integrity.
- **Analysis Techniques:** Security and privacy assessment uses static analysis (predictive but limited by obfuscation and cloud components) and dynamic analysis (actual behavior with coverage limitations and anti-testing vulnerabilities).
- **Assessment Gaps:** The effectiveness of existing analysis techniques remains under-assessed due to a lack of benchmarks, while cyberthreat intelligence lacks methodological transparency, leading to potential misclassification of software.

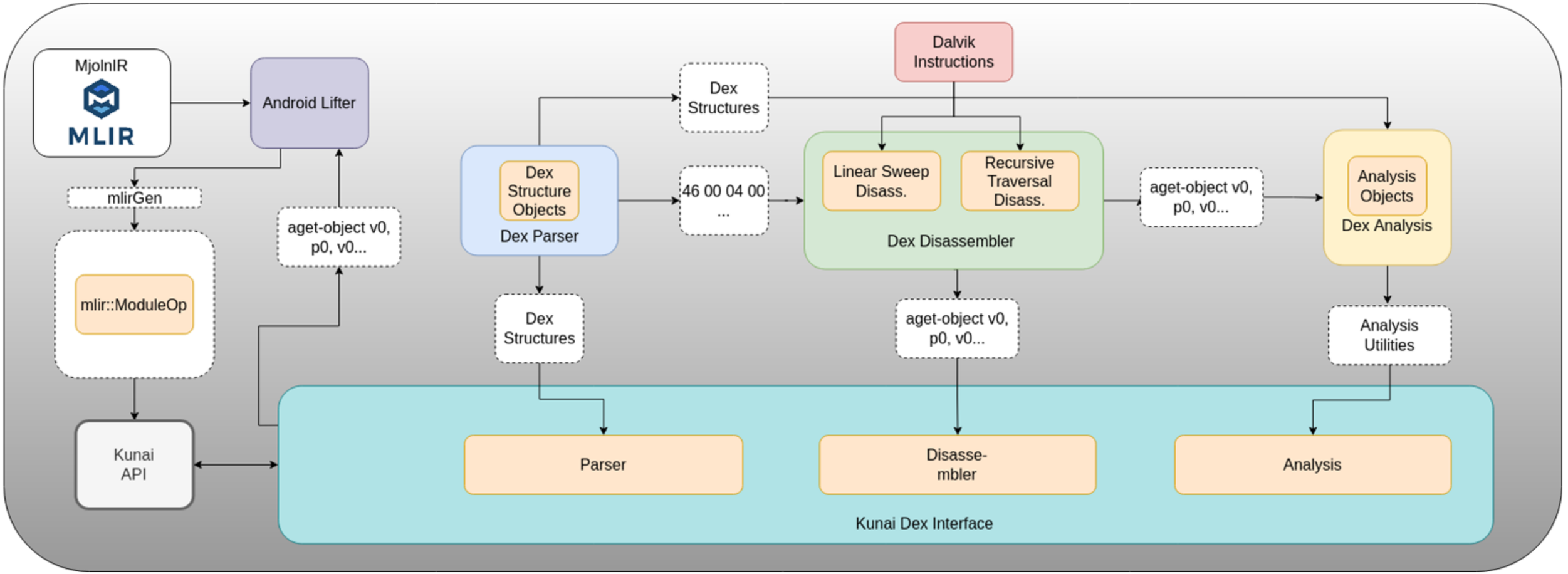
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Static Analysis Pipeline - Framework (UC3M)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Static Analysis Pipeline - Kunai (UC3M)

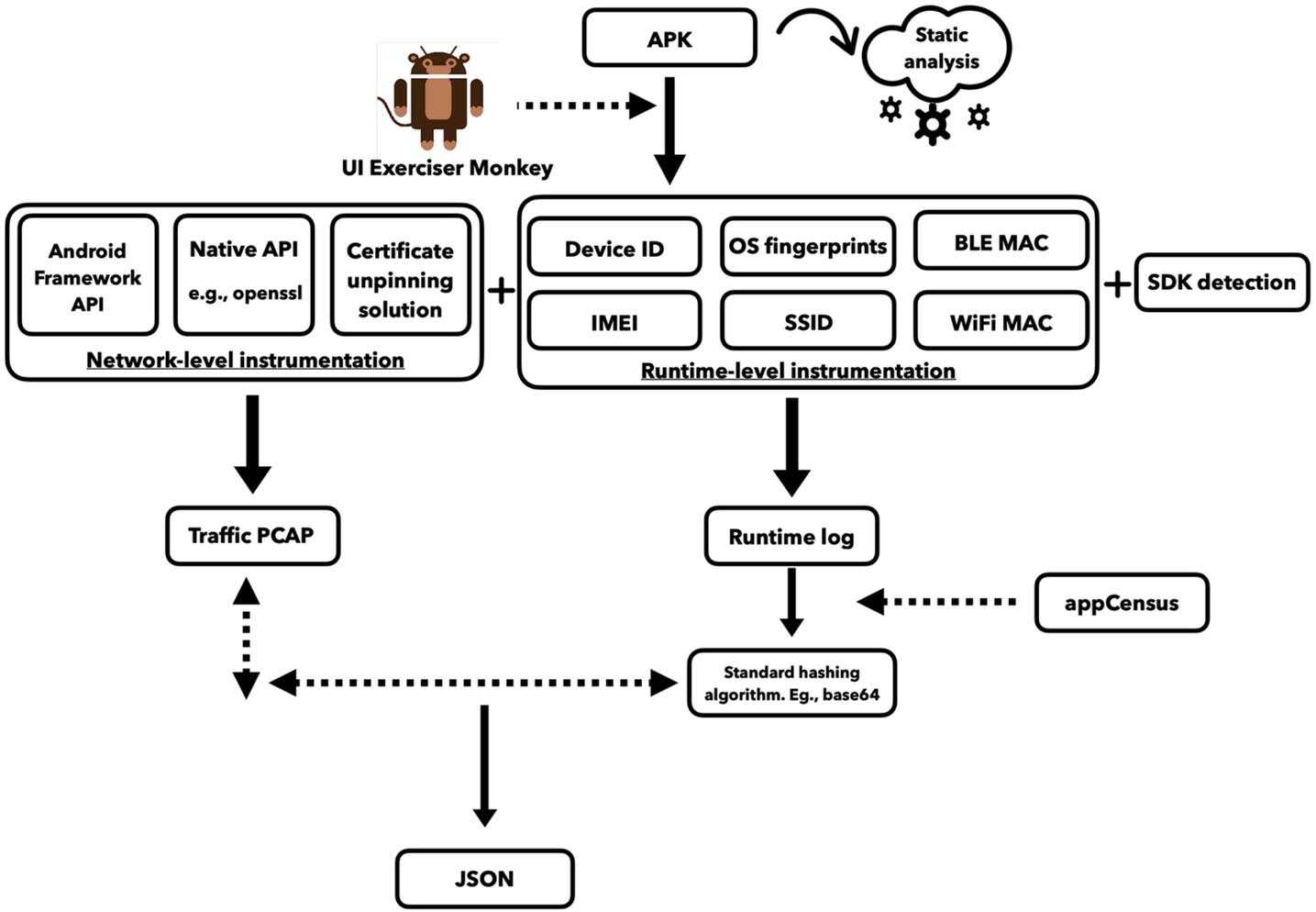


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Static Analysis Pipeline - Demo (UC3M)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Dynamic Analysis Pipeline (IMDEA)



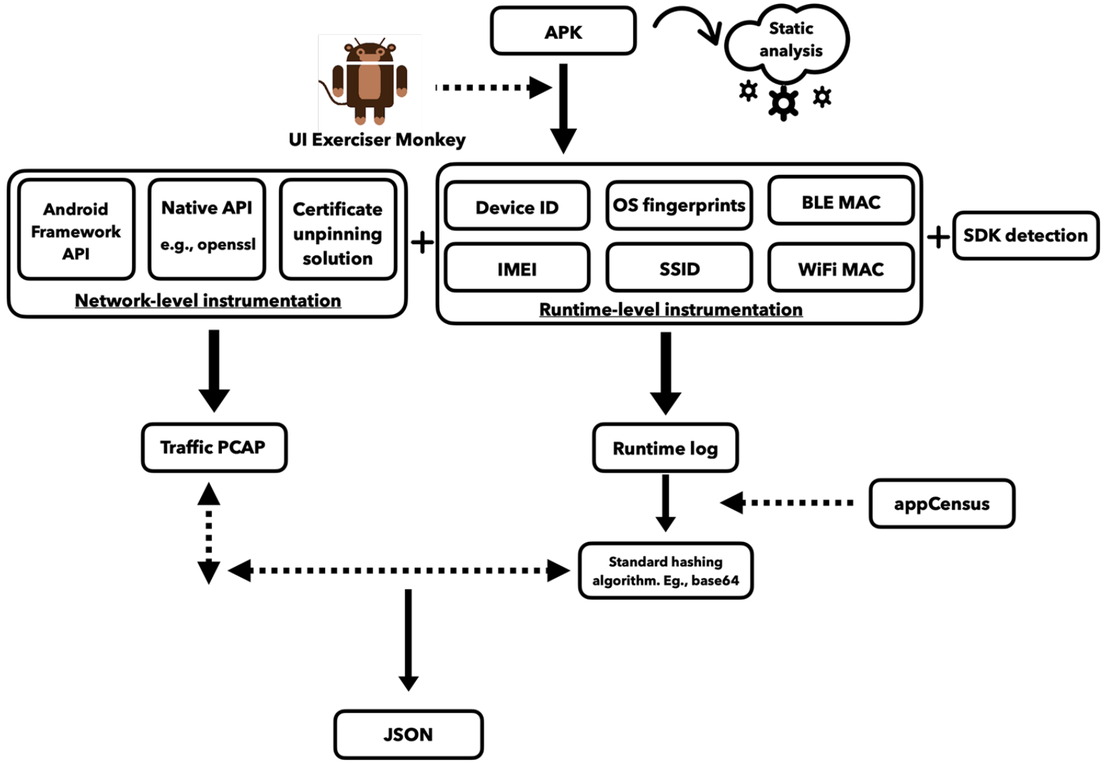
1. Runtime monitoring
2. Network layer instrumentation
3. SDK detection
4. Taint tracking
5. Final JSON report

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Dynamic Analysis Pipeline(IMDEA)

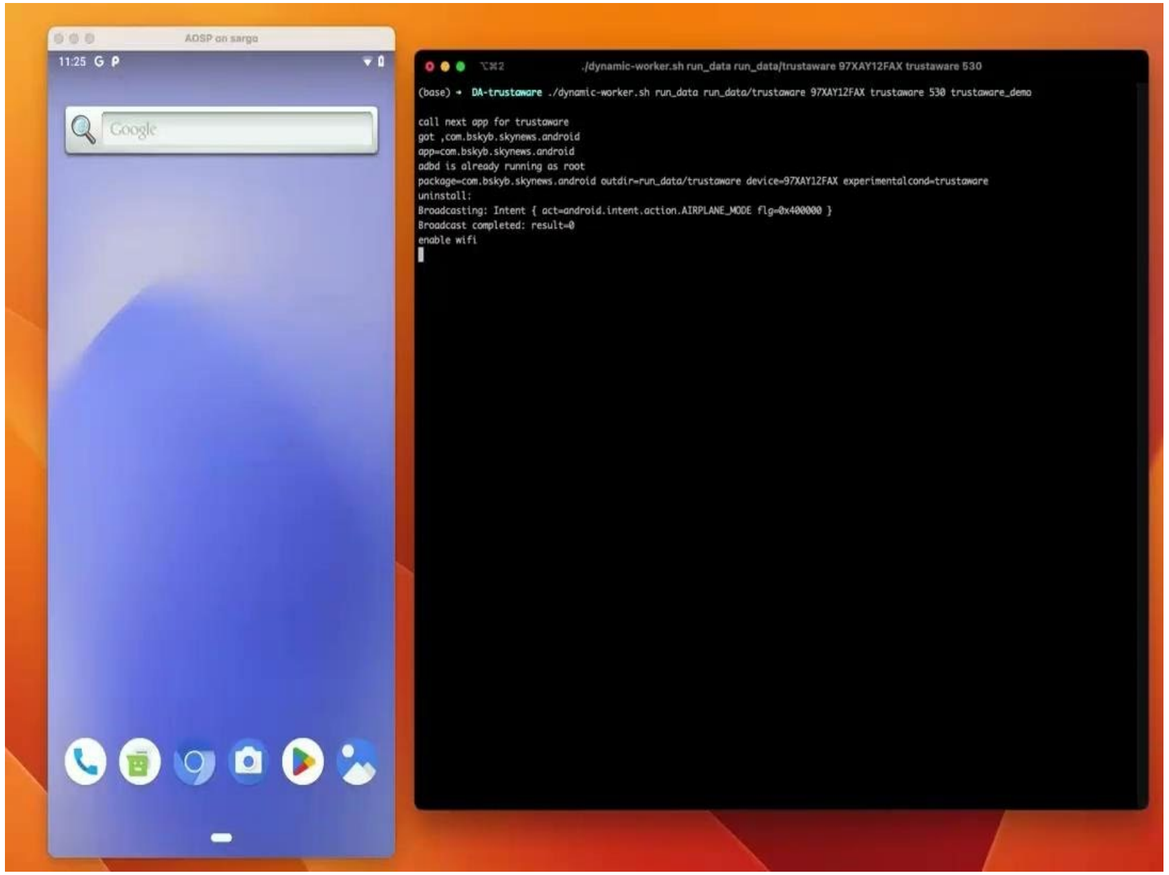
The dynamic analysis pipeline is designed to handle a high volume of apps, processing them one after the other

- Source code + Frida based instrumentation; Highly modular architecture
- ~5K LoC of JS and python
- Supports Android 9, 12, 14. Pipeline predominantly uses Android 12.
- Capable of circumventing certificate pinning on 18+ TLS libraries.
- Integration with AppCensus for improved coverage and data leak identification
- Has the capability to monitor more than 60 types of PII data types.
- Our SA + DA platform sends a combined report (JSON) to the MISP platform



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

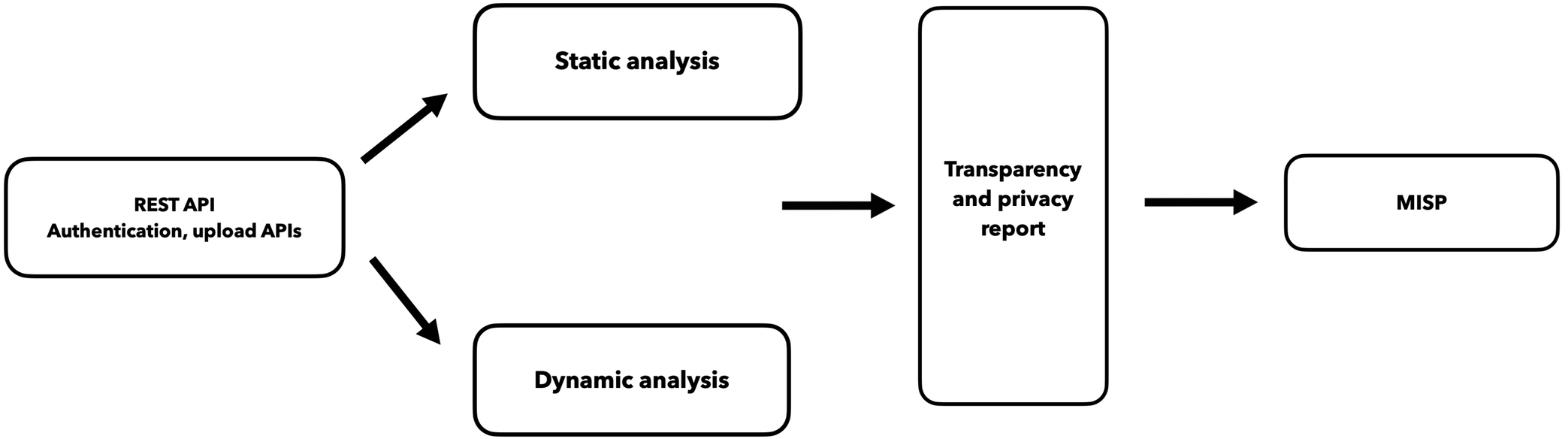
Dynamic Analysis Pipeline - Demo (IMDEA)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Connection API (IMDEA)

- Connection between Static and Dynamic Analysis Engines.
- Continuous testing of the pipeline; achieve stability and improved report data for MISP platform.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Sending Results to MISP (IMDEA)

MISP platform updated with:

- App metadata (e.g., package name, version, permissions)
- Dynamic analysis results (e.g., API calls, network traffic, file system access)


```
{
    "dynamic_analysis": {
        "http://imagenes.elpais.com": {
            "Incoming Traffic": {
                "PII": [
                    "communicated"
                ],
                "timestamp": "1698942359215"
            },
          "http://sdk.privacy-center.org": {
            "Outgoing Traffic": {
                "PII": [
                    "communicated",
                    "bluetooth"
                ],
                "timestamp": "1698942299876",
                "dst_ip": "18.67.240.26",
                "dst_port": "443"
            },
            "Incoming Traffic": {
                "PII": [
                    "communicated"
                ],
                "timestamp": "1698942299876"
            }
        },
```

```
"http://firebase-settings.crashlytics.com": {
            "Outgoing Traffic": {
                "PII": [
                    "communicated",
                    "bluetooth"
                ],
                "timestamp": "1698942299918",
                "dst_ip": "142.250.184.3",
                "dst_port": "443"
            },
            "Incoming Traffic": {
                "PII": [
                    "communicated"
                ],
                "timestamp": "1698942299961"
            }
        },
        "http://aax.amazon-adsystem.com": {
            "Outgoing Traffic": {
                "PII": [
                    "communicated",
                    "bluetooth",
                    "aaid",
                    "coarsegeolatlon",
                    "geolatlon"
                ],
                "timestamp": "1698942359359",
                "dst_ip": "18.154.54.56",
                "dst_port": "443"
            },
            "Incoming Traffic": {
                "PII": [
                    "communicated"
                ],
                "timestamp": "1698942359410"
            }
        },
```


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377