EIMI

KM11


I3A
Instituto de Investigación
en Informática de Albacete


UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

Índice

Introducción y motivación

¿Por qué?

- Heterogeneidad del entorno IoT.
- Incremento sustancial del malware.
- Automatización de la caracterización y la clasificación.

Público objetivo

- Analistas e investigadores.

Aportaciones

- Plataforma multi-arquitectura de ejecución, caracterización y clasificación de malware.

Estado del arte

Alternativas

- Limon sandbox
- Padawan
- Detux
- Cuckoo
- Falcon

Propuesta

Funcionalidades

- Soporta diferentes arquitecturas: ARM, MIPS, x86, x64, etc.
- Caracterización dinámica del malware basada en n-gramas.
- Clustering del malware.

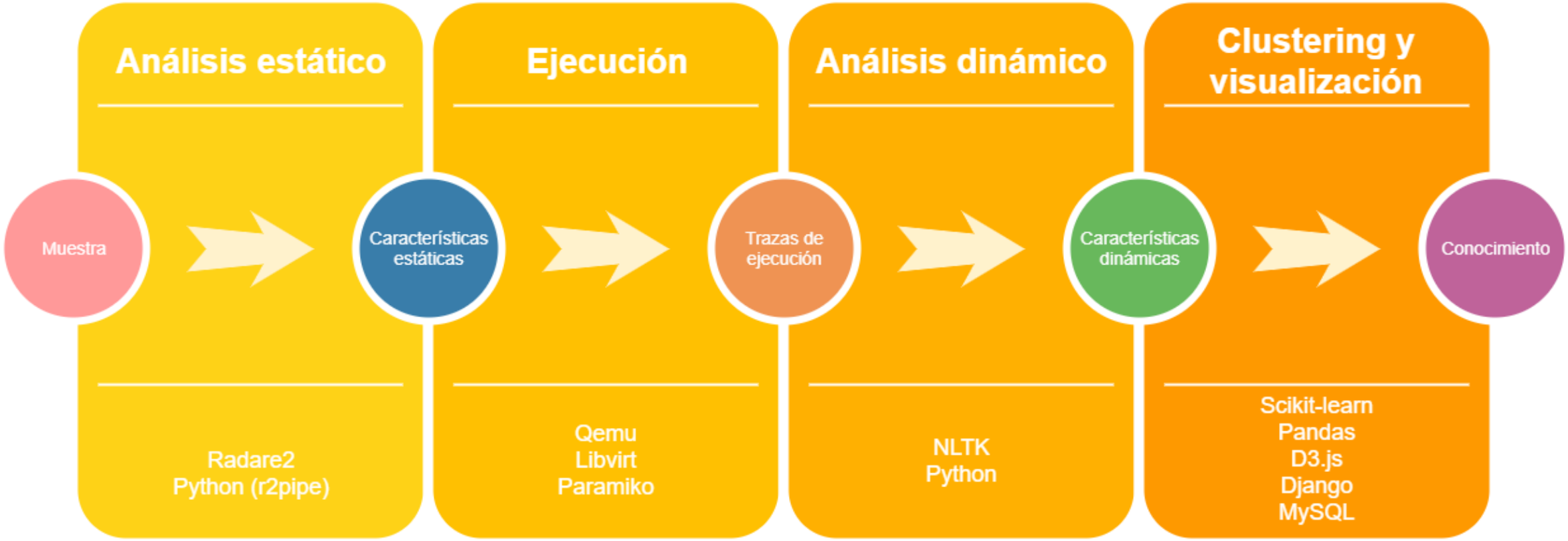
Características

- Modularidad.
- Liviano.

Aspectos de seguridad

- Caracterización y clasificación del malware inter-arquitectura.

Tecnologías



Planificación

Trabajo realizado.

- Máquinas construidas con Buildroot.
- Elección y primer contacto de las tecnologías y librerías a utilizar.
- Diseño del pipeline de la plataforma.
- Diseño del flujo de trabajo en equipo.

Trabajo a realizar.

- Implementación de módulos (Análisis estático, Ejecución, Análisis dinámico, Clustering y Visualización).
- Integración de módulos.
- Despliegue y evaluación.
- Documentación.

EIMI

KM11


I3A
Instituto de Investigación
en Informática de Albacete


UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA