AndroCIES: Automatización de la certificación de seguridad para aplicaciones Android

Manuel Ruiz, Rubén Ríos, Rodrigo Román, Antonio Muñoz

Network, Information and Computer Security (NICS) Lab

Universidad de Málaga

Juan Manuel Martínez, Jorge Wallace

DEKRA Testing and Certification, S.A.U.

Santander, 2022

NICS

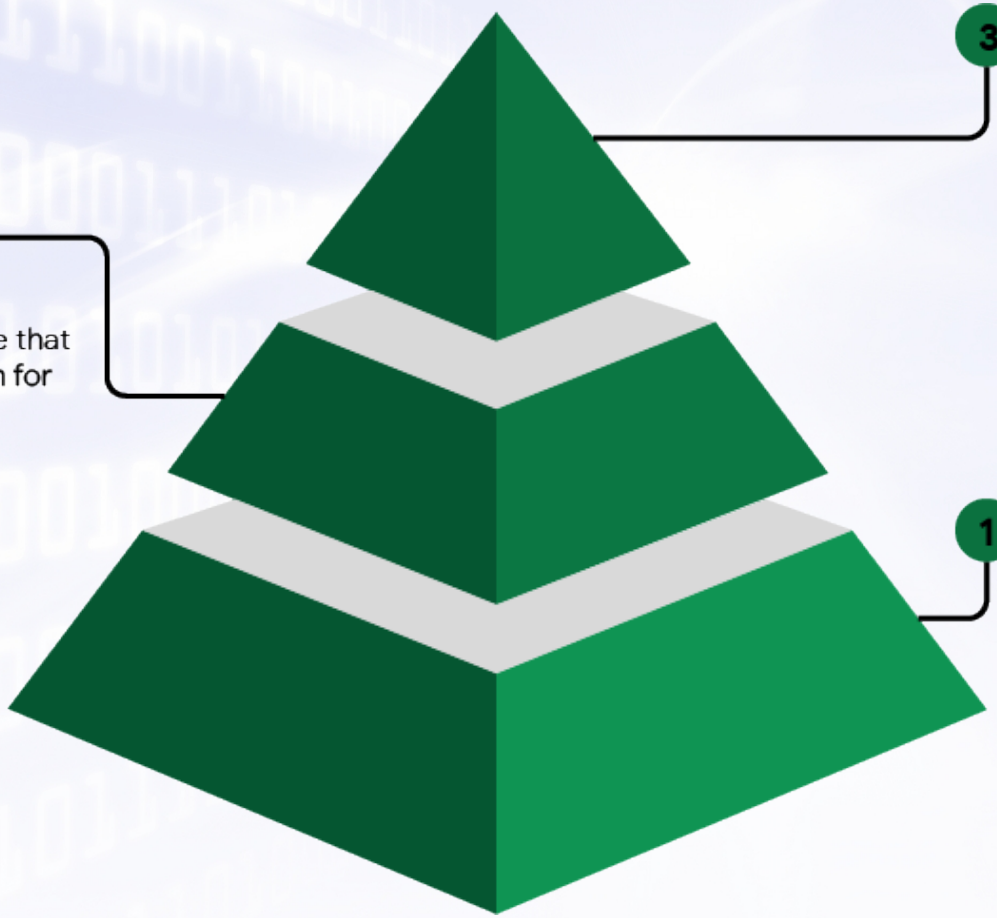
Popularidad y aplicaciones de baja calidad

- En 2020 había más de **1000 millones de usuarios** en Android
- Google Play, el proveedor oficial de aplicaciones en Android, cuenta con más de **2,5 millones de aplicaciones**.
  - El **40%** son aplicaciones de **baja calidad**
- Existe un problema de reputación

NICS

Estándares de seguridad y Google MASA

- Google MASA: Programa de seguridad en aplicaciones basado en **OWASP MASVS y MASTG**



3 Authorized labs

Google provides a list of accredited labs for developers

OWASP MASTG 2

Corresponding testing guidance that provides a single source of truth for how to objectively test for compliance with MASVS

1 OWASP MASVS

Industry recognized set of security criteria for mobile applications

NICS

Objetivos

- **Reducir el tiempo** y esfuerzo empleado **en la evaluación de aplicaciones móviles** por el equipo de certificación.

- Combinar, **clasificar y categorizar la información** procedente de varias herramientas **de análisis**, en función de los casos de prueba establecidos por los diferentes estándares.

- Presentar un **veredicto automatizado** o, en su defecto, agrupar toda la información necesaria para que el experto pueda realizar un veredicto con facilidad.

Estado de la técnica

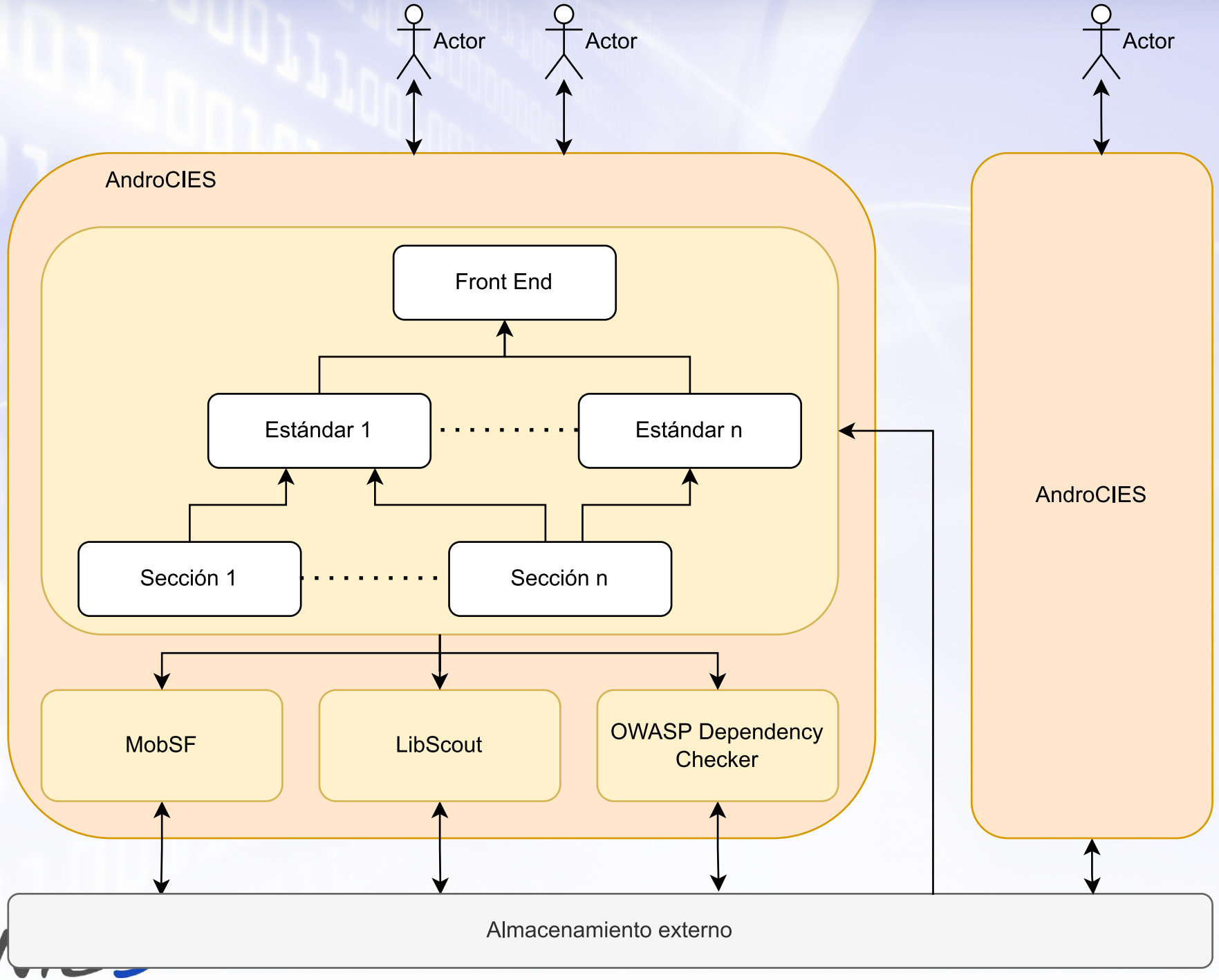
	Análisis					
	Permisos	Manifest	Código	Certificados	URLs	Librerías ext
AndroShield	✗	✓	✓	✗	✗	✗
Androtomsit Lite	✗	✓	✓	✓	✗	✗
MARA Framework	✓	✓	✓	✓	✓	✗
MobSF	✓	✓	✓	✓	✓	✓*
Ostorlab	✓	✓	✓	✓	✓	✓
Kryptowire	✓	✓	✓	✓	✓	✓
NowSecure	✓	✓	✓	✓	✓	✓

	SaaS	Clasificación de severidad	Formato de salida
AndroShield	✗	✓	Página Web
Androtomsit Lite	✗	✗	Fichero txt
MARA Framework	✗	✓	Ficheros json y txt
MobSF	✗	✓	Base de datos MySQL
Ostorlab	✓	✓	Página Web
Kryptowire	✓	✓	Página Web
NowSecure	✓	✓	Página Web

Requisitos

- **Completitud**: se evaluarán todos los casos de prueba del MASVS L1 que Dekra considera relevantes, alineados con Google MASA.
- **Extensibilidad**: se adaptará a los estándares actuales y futuros.
- **Portabilidad**: se desplegará en diferentes entornos y sistemas operativos
- **Persistencia**: se garantizará la permanencia de los datos tras los análisis.
- **Soporte multi-usuario**: se ofrecerá el servicio a varios usuarios a la vez
- **Usabilidad**: ofrecerá una interfaz sencilla, clara y concisa.

Diseño


Actor
Actor
Actor
AndroCIES
Front End
Estándar 1
Estándar n
Sección 1
Sección n
MobSF
LibScout
OWASP Dependency Checker
AndroCIES
Almacenamiento externo

UMA

UUID(MD5) : 5c0b97becfd2cd3732b2f357759b2c29

MobSF Analysis Manifest

OWASP MASVS

STORAGE

STORAGE-1

Storage of Credentials (FCS_STO_EXT.1.1)

Class: Security Functional Requirements
Description: The application does not store any credentials to non-volatile memory.

STORAGE-2

Permission "android.permission.WRITE_EXTERNAL_STORAGE" dangerous

Info: read/modify/delete external storage contents
Description: Allows an application to write to external storage.

android_temp_file info not detected

Description: App does not create temp file.
Owasp-mobile: m2
CWE: cwe-276
CVSS: 5.5

PLATFORM-4

All Objects Analysis

All | Exported | Without Permissions | Exported & Without Permissions

Activities

Content Providers

Broadcast Receivers

Services

com.adobe.phonegap.push.FCMService

Permission: None

Exported: True

- Level: warning
- A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

Manifest | File

com.adobe.phonegap.push.PushInstanceIDListenerService

Permission: None

Exported: True

- Level: warning
- A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.

Manifest | File

com.google.firebase.messaging.FirebaseMessagingService

Permission: None

Exported: True

- Level: high

Conclusión y Líneas futuras

- El interés de Google por una Play Store más segura y transparente está empujando a los laboratorios especializados a **mejorar sus procesos de certificación** de seguridad de aplicaciones.
- En promedio, se ha determinado **una reducción del 20% del tiempo empleado** para la evaluación respecto al estándar OWASP MASVS siguiendo la metodología de OWASP MASTG.
- Existen varias líneas de trabajo futuro:
  - Incorporación de técnicas de **análisis dinámico** de código.
  - Incorporación de **inteligencia artificial** para diferentes características como **la detección de falsos positivos**.

NICS

AndroCIES: Automatización de la certificación de seguridad para aplicaciones Android

Manuel Ruiz, Rubén Ríos, Rodrigo Román, Antonio Muñoz

Network, Information and Computer Security (NICS) Lab

Universidad de Málaga

Juan Manuel Martínez, Jorge Wallace

DEKRA Testing and Certification, S.A.U.

Santander, 2022

NICS