ANÁLISIS DE FLUJO DE INFORMACIÓN EN APLICACIONES ANDROID

Lina Marcela Jiménez Becerra

UNIVERSIDAD DE LOS ANDES
DEPARTAMENTO DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Junio 9, 2015

Background

Técnicas de análisis

- Análisis estático.

Background

Técnicas de análisis

- Análisis estático.
- Análisis dinámico.

Background

Técnicas de análisis

- Análisis estático.
- Análisis dinámico.
- Security Typed languages.

Background

Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación.

Sistema de anotaciones en Jif

- Lenguaje tipado de seguridad.
- Extensiones de seguridad para el lenguaje Java.
- Restricciones para uso de la información.
- Label checking.

Background

DML de JIF

- Principals
- Políticas
- Labels

Descripción del Problema

Manipulación de información del usuario

El desarrollador Android no tiene cómo definir políticas de seguridad para regular el flujo de información de sus aplicaciones.

Descripción del Problema

Manipulación de información del usuario

El desarrollador Android no tiene cómo definir políticas de seguridad para regular el flujo de información de sus aplicaciones.

Reporte McAffe

- Aplicaciones Android invasivas.
- No toda aplicación invasiva contiene malware.
- De las aplicaciones que más vulneran la privacidad del usuario 35 % contienen malware.

Descripción del Problema

Contramedidas existentes

- Políticas de control de acceso de la API.
- Data-Flow analysis con técnicas de análisis tainting.

Descripción del Problema

Contramedidas existentes

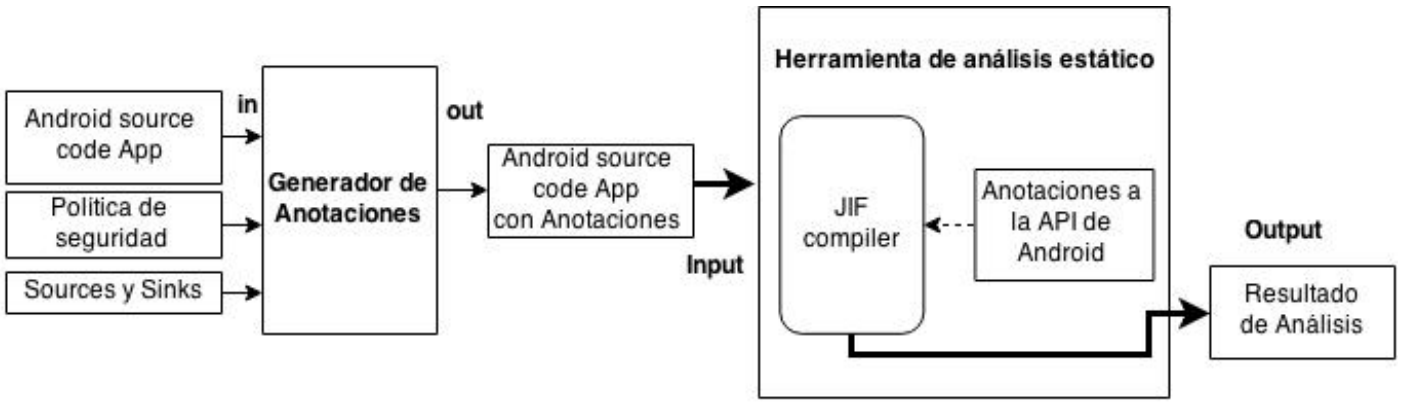
- Políticas de control de acceso de la API.
- Data-Flow analysis con técnicas de análisis tainting.

Herramienta que se requiere

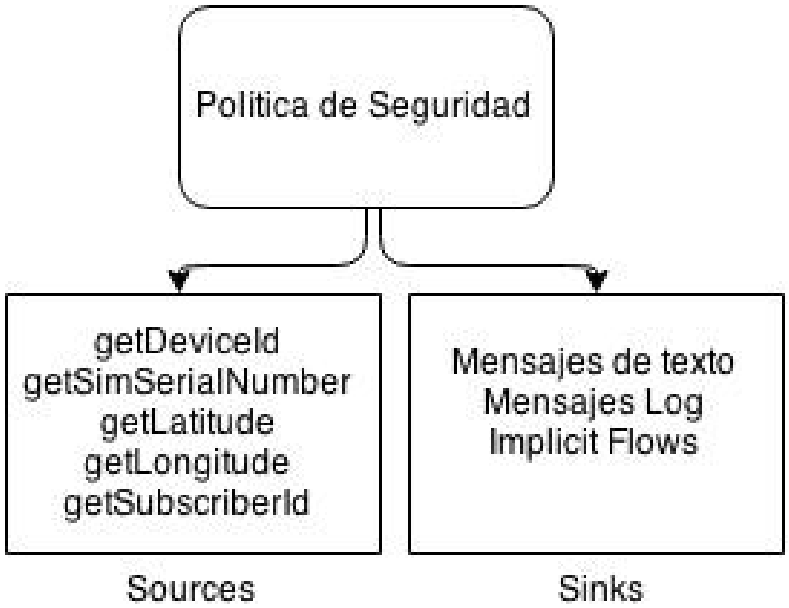
- Analizar el flujo de información del aplicativo.
- Garantizar políticas de confidencialidad e integridad desde la implementación.

Propuesta de solución

Herramienta de Análisis Estático



Política de Seguridad

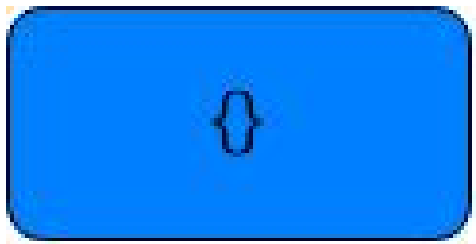


Flujos de información entre: información con nivel de seguridad alto e información con nivel de seguridad bajo.

Autoridad y Labels de Anotación

Autoridad Máxima

Nivel de Seguridad Alto



Nivel de Seguridad Bajo

Anotaciones a la API

Controlar canales

- Mensajes de texto (SmsManager)
- Mensajes log (Log)

Anotaciones a la API

Controlar canales

- Mensajes de texto (SmsManager)
- Mensajes log (Log)

Clases adicionales requeridas

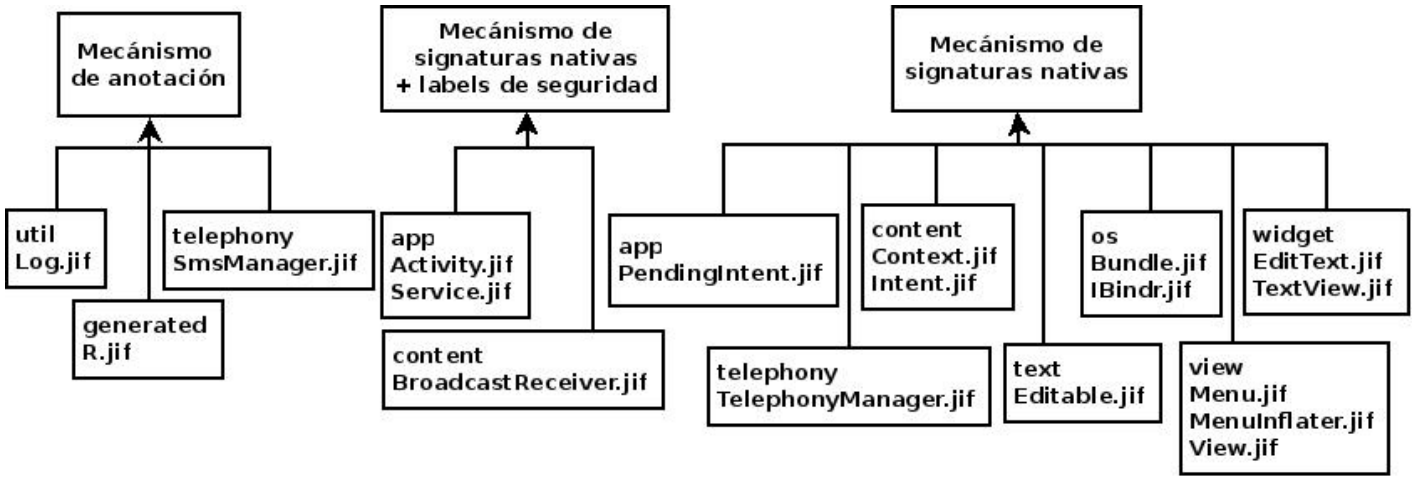
- Clases para los sources (TelephonyManager)
- Clases para métodos de sobresscritura (Activity)

Anotaciones a la API

Controlar canales

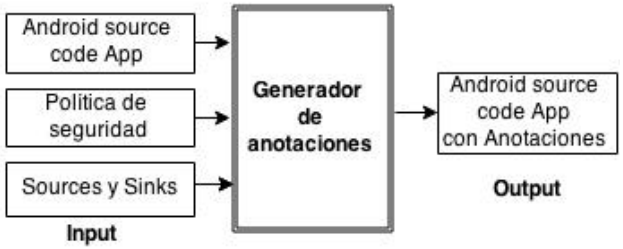
```
sendTextMessage{Alice:} (
String{Alice:} destinationAddress,
String{Alice:} sourceAddress,
String{}text,
PendingIntent{Alice:} sentIntent,
PendingIntent{Alice:} deliveryIntent
){}
```

Anotaciones a la API



Anotación de aplicativos a analizar

Generador de Anotaciones



- Objetivo de la anotación
- Elementos a anotar

Evaluación

- Conjunto de evaluación.
- DroidBench benchmark.

Evaluación

- Conjunto de evaluación.
- DroidBench benchmark.

	FlowDroid	JoDroid	Prototipo
Precisión	78,57 %	78,57 %	73,68 %
Recall	78,57	78,57 %	100 %
Detección Flujos Implícitos	No	Si	Si

Cuadro comparativo

Item	Prototipo vs FlowDroid				Prototipo vs JoDroid			
	ventaja	desvent	similit	diff	ventaja	desvent	similit	diff
Menor Precisión		✓				✓		
Mayor Recall	✓				✓			
Menor costo en desempeño					✓			
Bajo costo en desempeño			✓					
Detección de flujos implícitos	✓						✓	
No detección automática de sources y sinks		✓					✓	
No soporte para Análisis interApp		✓					✓	
Tipo de análisis(flujo de información; flujo de datos)				✓				
Tipo de análisis IFC							✓	
Técnica de análisis: PDG, slicing								✓

Conclusiones

- Herramienta de análisis mediante el sistema de anotaciones de Jif.

Conclusiones

- Herramienta de análisis mediante el sistema de anotaciones de Jif.
- Análisis de flujos implícitos.

Conclusiones

- Herramienta de análisis mediante el sistema de anotaciones de Jif.
- Análisis de flujos implícitos.
- Desempeño y completitud en el análisis.

Conclusiones

- Herramienta de análisis mediante el sistema de anotaciones de Jif.
- Análisis de flujos implícitos.
- Desempeño y completitud en el análisis.
- Retos para el análisis de aplicaciones Android mediante el sistema de anotaciones de Jif.

Trabajo Futuro

- Extensiones al esquema de anotación.
- Análisis de políticas de integridad.
- Mecanismos adicionales: declasificación y endorsement.