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

Qué deben saber??

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

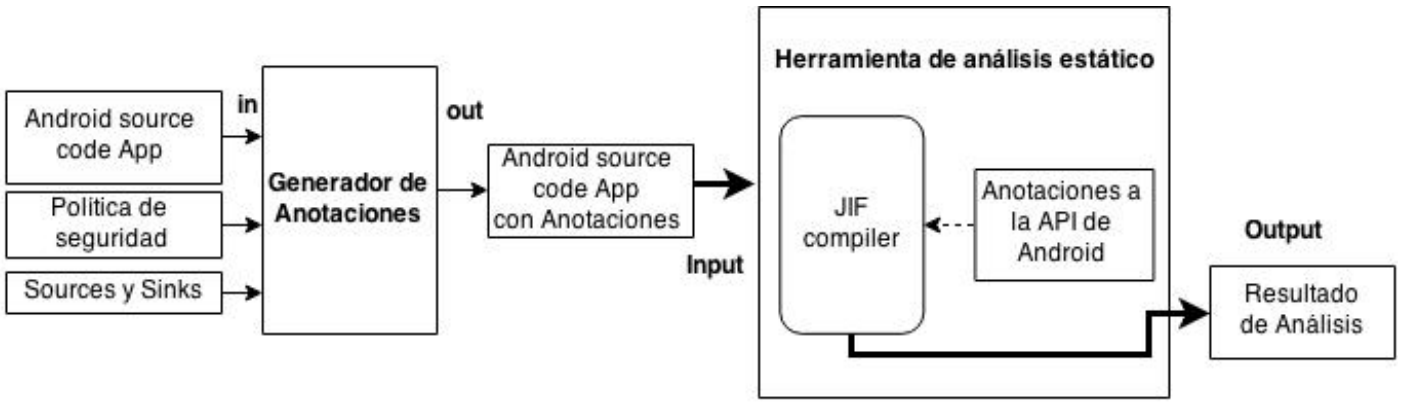
- Políticas de control de acceso de la API.
- Data-Flow analysis con técnicas de análisis tainting.

Herramienta que se requiere

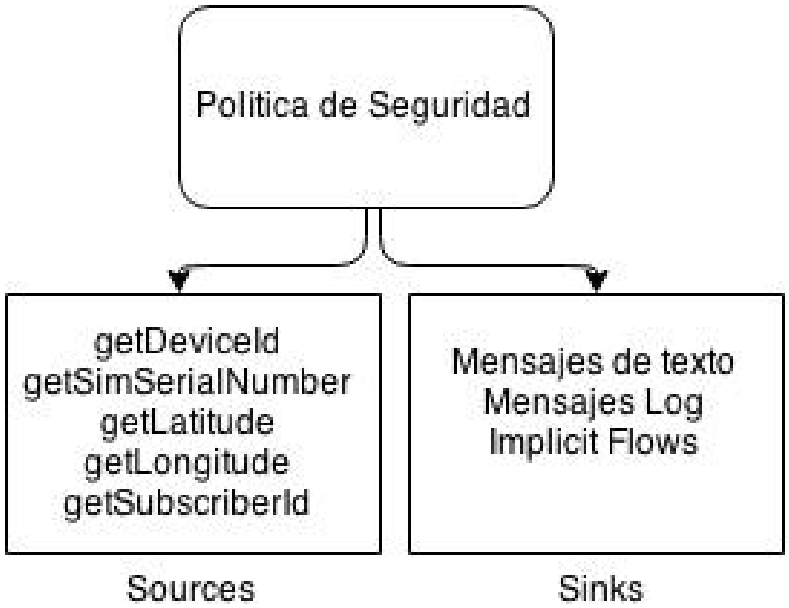
- Analizar el flujo de información del aplicativo.
- Garantizar políticas de confidencialidad e integridad desde la implementación.

Propuesta de solución

Herramienta de Análisis Estático



Política de Seguridad

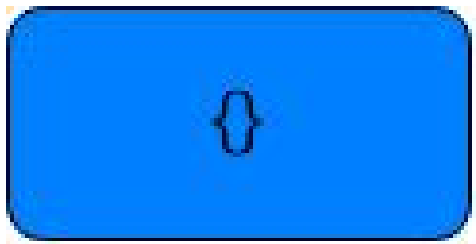


Flujos de información entre: información con nivel de seguridad alto e información con nivel de seguridad bajo.

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)

Clases adicionales requeridas

- Clases para los sources
- Clases para métodos de sobresscritura

Controlar canales

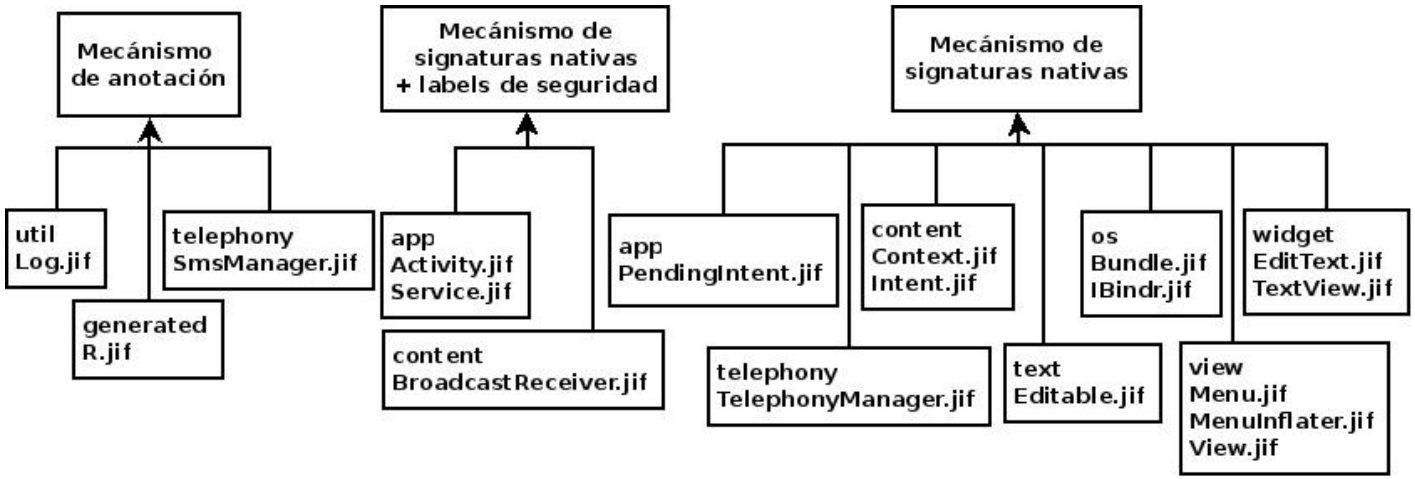
```
sendTextMessage{Alice:}(String{Alice:}destAdd,
String{Alice:}scAdd,
String{} text,
    PendingIntent{Alice:} sentIntent,
PendingIntent{Alice:} deliveryIntent) { }
```

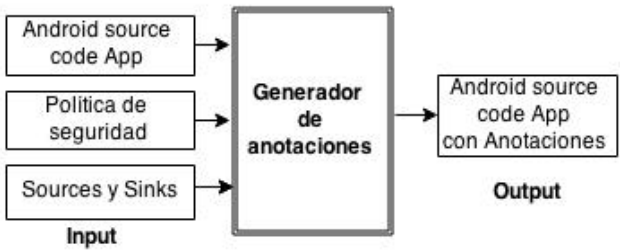
Clases adicionales requeridas

Mecanismos

- Anotación
- Signaturas Nativas
- signaturas nativas más labels de Seguridad

Anotaciones para Integrar Clases de la API




Android source code App
Politica de seguridad
Sources y Sinks
Input
Generador de anotaciones
Android source code App con Anotaciones
Output

Anotación de aplicativos a analizar

Generador de anotaciones

Objetivo de la anotación

- Métodos source contenidos en la clase
- Métodos que influencian el source
- Envio de información hacia canales con nivel de seguridad bajo

Anotación de aplicativos a analizar

Generador de anotaciones

Objetivo de la anotación

- Métodos source contenidos en la clase
- Métodos que influencian el source
- Envio de información hacia canales con nivel de seguridad bajo

Lo que se anota

- Variables source
- Métodos source
- Método no source

Evaluación

Comparación con FlowDroid y JoDroid

Conclu

bla, blaaaaaaa

Futuro

ampliar el setup