

# 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

# Background

## Técnicas de análisis

- Análisis estático.

# Background

## Técnicas de análisis

- Análisis estático.
- Análisis dinámico.

# Background

## Técnicas de análisis

- Análisis estático.
- Análisis dinámico.

# Background

## Técnicas de análisis

- Análisis estático.
- Análisis dinámico.

## Técnicas utilizadas en análisis estático

# Background

## Técnicas de análisis

- Análisis estático.
- Análisis dinámico.

## Técnicas utilizadas en análisis estático

- Técnicas de flujo de datos.

# Background

## Técnicas de análisis

- Análisis estático.
- Análisis dinámico.

## Técnicas utilizadas en análisis estático

- Técnicas de flujo de datos.
- Técnicas de flujo de control.



# Background

## Técnicas de análisis

- Análisis estático.
- Análisis dinámico.

## Técnicas utilizadas en análisis estático

- Técnicas de flujo de datos.
- Técnicas de flujo de control.
- Security Typed languages.

# Background

## Aplicaciones Android

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación: Activity, Service, Broadcast, Content Providers.

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación: Activity, Service, Broadcast, Content Providers.

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación: Activity, Service, Broadcast, Content Providers.

## Sistema de anotaciones en Jif

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación: Activity, Service, Broadcast, Content Providers.

## Sistema de anotaciones en Jif

- Lenguaje tipado de seguridad.



# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación: Activity, Service, Broadcast, Content Providers.

## Sistema de anotaciones en Jif

- Lenguaje tipado de seguridad.
- Extensiones de seguridad para el lenguaje Java.

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación: Activity, Service, Broadcast, Content Providers.

## Sistema de anotaciones en Jif

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

# Background

## Aplicaciones Android

- Aplicación Java con interfaces descritas en XML.
- Framework Android.
- Componentes de aplicación: Activity, Service, Broadcast, Content Providers.

## 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

Elementos del modelo de anotación:

- Principals
- Políticas
- Labels

# Background

## Principals

Autoridad sobre un sistema o programa(Alice, Bob, Chunck)

# Background

## Principals

Autoridad sobre un sistema o programa(Alice, Bob, Chunck)

## Políticas

{owner: reader list} u {owner: writer list}

# Background

## Principals

Autoridad sobre un sistema o programa(Alice, Bob, Chunck)

## Políticas

{owner: reader list} u {owner: writer list}

## Labels

Políticas de seguridad que se adicionan a las expresiones del programa.

```
int {Alice:} code;
```

# 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. Complejidad para prevenir fugas de información.



# 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. Complejidad para prevenir fugas de información.

## Reporte McAfee

- 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

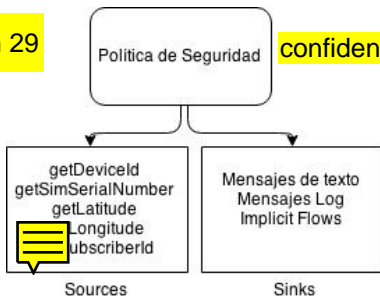
- Analizar el flujo de información del aplicativo.
- Garantizar políticas de confidencialidad e integridad desde la implementación.



# Política de Seguridad

min 31: Hacer un ejemplo donde los sources y sinks, sean

min 29



**confidencialidad**

Flujos de información  
confidencial: información con  
nivel de seguridad  
alto(sources) e  
información con nivel  
de seguridad  
bajo(sinks).



# Anotaciones a la API

## Por qué es necesario hacer anotaciones a la API?

### Controlar canales

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

min 36i

# Anotaciones a la API

## Controlar canales

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

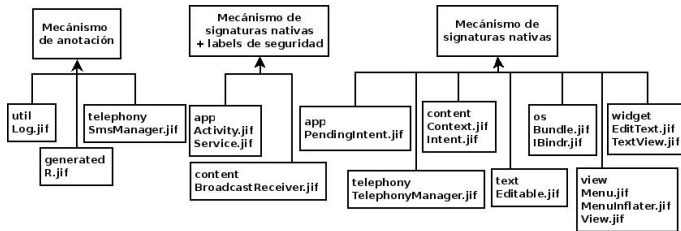
## Clases adicionales requeridas

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



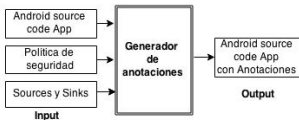


# Anotaciones a la API



# 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.

# Preguntas