

ANÁLISIS DE FLUJOS DE INFORMACIÓN EN APLICACIONES ANDROID

Lina Marcela Jiménez Becerra
Grupo COMIT
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes
Bogotá, Colombia
lm.jimenez12@uniandes.edu.co

Resumen—

El presente trabajo de investigación plantea aplicar técnicas de análisis basadas en control de flujo de información, con el fin de verificar la ausencia de fugas de información en aplicaciones Android, desde su construcción. Puesto que, controlar el acceso y uso de la información, representa una de las principales preocupaciones de seguridad en dichos aplicativos. Un estudio reciente de seguridad en dispositivos móviles, publicado por McAfee[1], revela que en el contexto de aplicativos Android: 80 % reúnen información de la ubicación, 82 % hacen seguimiento de alguna acción en el dispositivo, 57 % registran la forma de uso del celular (mediante Wi-Fi o mediante la red de telefonía), y 36 % conocen información de las cuentas de usuario. Adicionalmente, el informe señala que una aplicación invasiva no necesariamente contiene malware, y que su finalidad no siempre implica fraude; de las aplicaciones que más vulneran la privacidad del usuario, 35 % contienen malware.

Si bien, aplicaciones invasivas no necesariamente implican malware y/o acciones delictivas, el cuestionamiento de fondo es la forma y finalidad con que una aplicación manipula la información del usuario, y qué garantías puede ofrecer el desarrollador para que tal manipulación sea consentida.

CATEGORÍAS Y DESCRIPCIÓN DE TEMÁTICAS

Análisis de flujos de información en aplicaciones.

TERMINOS GENERALES

Técnicas Security-Typed, Técnicas de flujo de información, Técnicas de flujo de datos, Análisis Dinámico, Análisis estático.

PALABRAS CLAVE

Jif, Políticas de seguridad, Flujo de información, Verificación de políticas, Confidencialidad, Fuga de información.

I. INTRODUCCIÓN

En aplicativos Android, el manejo de la información del usuario, es una de las principales preocupaciones de seguridad. Según un estudio reciente de seguridad en dispositivos móviles, publicado por McAfee[1], una importante cantidad

de aplicaciones Android invaden la privacidad del usuario, reuniendo información detallada de su desplazamiento, acciones en el dispositivo, y su vida personal.

Por otro lado, para controlar el acceso a información manipulada por sus aplicaciones, el desarrollador cuenta con los mecanismos de seguridad proveídos por la API de Android, sin embargo, al estar basados en políticas de control de acceso, se limitan a verificar el uso de los recursos del sistema acorde a los privilegios del usuario, lo que suceda con la información una vez sea accedida, está fuera del alcance de este tipo de controles. Al no contar con herramientas de análisis de flujo de información en aplicaciones Android, o al utilizar librerías de terceros, para el desarrollador es difícil verificar el cumplimiento de políticas de confidencialidad e integridad en la aplicación próxima a liberar. Por consiguiente, el desarrollador no tiene cómo asegurar la ausencia de fugas de información en la aplicación.

Si bien, en el campo de aplicativos Android, existen diferentes propuestas para detectar fuga de información, en su mayoría están enfocadas a analizar aplicaciones de terceros, asumiendo que el atacante provee bytecode malicioso. Por tanto, aplican data-flow analysis partiendo del bytecode. Estas propuestas no abordan el problema del lado del desarrollador, analizando flujos de información de la aplicación para verificar el cumplimiento de políticas de confidencialidad.

Ante esto, y con el fin de proveer una herramienta de apoyo al desarrollador, de modo que verifique el cumplimiento de políticas de seguridad en sus aplicaciones, el presente trabajo aborda el problema de fugas de información en aplicaciones Android, analizando flujos de información de la aplicación, mediante técnicas de lenguajes tipados de seguridad.

El Artículo está organizado de la siguiente manera: XXX

II. CONTEXTO

III. DESCRIPCIÓN DEL PROBLEMA

IV. TRABAJOS RELACIONADOS

V. PROPUESTA

VI. TRABAJO FUTURO

VII. CONCLUSIONES

REFERENCIAS

- [1] McAfee. (2014, February) Who's watching you?, mcafee mobile security report. [Online]. Available: <http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf>