АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ ЗЛОУМЫШЛЕННОГО КОДА В ANDROID-ПРИЛОЖЕНИЯХ

Давыдов В.В.

Национальный технический университет «Харьковский политехнический институт», г. Харьков

Современные смартфоны являются повседневным источником хранения личных и конфиденциальных данных.

Наличие открытости исходного кода ядра операционной системы (ОС) *Android* привело к увеличению популярности мобильных устройств, базирующихся на данной ОС.

Архитектура ОС *Android* предоставляет 4 типа компонентов приложений: *Activity* (определяет пользовательский интерфейс), *Service* (выполнение фоновых процессов), *Content Provider* (хранение и распределение данных, используя реляционную базу данных), *Broadcast Receiver* (получение широковещательных сообщений от других приложений).

В работе рассмотрены современные методы обнаружения потенциальных утечек личных данных, которые чаще всего вызваны внедрением злоумышленного кода в *Android*-приложения, либо некомпетентностью разработчиков при разработке мобильных приложений.

Рассмотрены такие анализаторы: *FlowDroid, EPICC* (статический анализ байт-кода, основанный на анализе *AndroidManifest.xml* файла (содержащий информацию об используемых разрешениях и реализованных/используемых компонентах системы), а также декомпиляции и анализе скомпилированных классов – *classes.dex*), *TaintFlow, TamiHex* (анализ поведения приложения в режиме реального времени, основанный на межкомпонентных взаимодействиях в приложении с учетом анализа предназначения передаваемых параметров). Показаны недостатки, заключающиеся в:

- возможности анализа вызовов только тех методов, все аргументы которых являются строковыми константами;
- отсутсвии поддержки анализа данных, логгируемых сторонними приложениями в ОС *Android* 4.0 и выше;
- ряд инструментов для статтического анализа приложений используют пакет *java.lang.instrument*, который не доступен в ОС *Android*, что препятствует анализу приложений из *Android*-устройства;
- отсутствие анализа данных, оперируемых с статическими полями, СУБД (база данных *SQLite*) и *SharedPreferences* (стандартное средство *Android* для хранения настроек текущего приложения).

Определены пути совершенствования рассмотренных методов обнаружения злоумышленного кода в *Android*-приложениях.