А. Ю. СОЛДАТОВА, Д. П. ЗЕГЖДА, Е. Ю. ПАВЛЕНКО
Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург

ОБНАРУЖЕНИЕ МОШЕННИЧЕСТВА С МОБИЛЬНОЙ РЕКЛАМОЙ НА ОСНОВЕ АНАЛИЗА РАБОТЫ ANDROID-ПРИЛОЖЕНИЙ

В рамках доклада на основе исследования схемы работы мобильной рекламы введена модель нарушителя, с помощью которой определен способ реализации, присущий потенциально наиболее опасным нарушителям, – подмена SDK. В результате анализа требований участников схемы к рекламе в приложениях выделено 8 типов мошенничества, 6 из которых реализуется посредством подмены SDK. Для обнаружения мошенничества с рекламой представлен прототип системы обнаружения мошенничества с мобильной рекламой в Android-приложениях, превосходящий по точности аналог на 4 %.

Введение. Высокий рост затрат на мобильную рекламу, выраженный в увеличении объема мирового рынка соответствующей рекламной отрасли с 240 млрд долларов в 2020 году до 290 млрд долларов в 2021 году [1], провоцирует возрастающую активность злоумышленников в данной сфере. Согласно исследованию Juniper Research [2] в 2022 году мировые потери бюджетов цифровой рекламы из-за мошенничества достигнут 68 млрд долларов, что на 59 млрд долларов больше по сравнению с 2021 годом. Жертвами мошенничества с мобильной рекламой становятся как рекламодатели, теряющие прибыль, так и пользователи устройств, скачавшие рекламное ПО или перешедшие на недоверенный сайт вследствие манипулирования с рекламой в приложении. Владельцы программного обеспечения (ПО) и поставщики рекламы, в основном представленные рекламными сетями, несут в связи с мошенничеством репутационные потери, влекущие за собой прямые финансовые убытки.

Для решения указанной проблемы предлагается прототип системы обнаружения мошенничества с рекламой в Android-приложениях, основанный на статическом и динамическом анализе работы приложений. К достоинствам данного прототипа можно отнести определение нескольких типов мошенничества с рекламой, более высокую точность обнаружения мошенничества по сравнению с аналогом.

Модель нарушителя. В схеме работы рекламы выделены 4 основных участника взаимодействия: рекламодатель, владелец ПО, пользователь и поставщик рекламы, являющийся посредником между рекламодателем и владельцем ПО. Взаимодействие владельца ПО и пользователя происходит посредством мобильного приложения.

В результате анализа схемы работы рекламы определены возможные нарушители и векторы атак. Пользователь, в отличие от остальных участников схемы, определен как внешний нарушитель, т. к. в основе исследования лежат коммерческие приложения, использование которых не требует особых прав. В качестве внешних нарушителей были выделены террористические/экстремистские группировки, конкурирующие организации и преступные. На основе компетентности, оснащенности, уровня знаний нарушителя каждому сопоставлен уровень возможностей по реализации угроз информационной безопасности на основании проекта [3] и утвержденного [4] методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах». В результате анализа действий нарушителей в отчетах инцидентов информационной безопасности определены способы реализации мошенничества, присущие каждому нарушителю. Разработанная модель нарушителя в контексте мошенничества с рекламой приведена в табл. 1.

Таблица 1

Модель нарушителя в контексте мошенничества с рекламой

Нарушитель	Уровень возможностей	Способы реализации мошенничества
Пользователи	H1	Взаимодействие с устройством и легальным приложением
Конкурирующие организации	H2	Воздействие на каналы связи между участниками схемы. Воздействие на персонал.
Террористические, экстремистские группировки	H2	Воздействие на каналы связи между участниками схемы
Преступные группы	H2	Кликовые фермы. Распространение вредоносного ПО (ВПО). Воздействие на каналы связи между участниками схемы. Воздействие на персонал.
	H3	Использование эмуляторов, VPN и proxy-серверов, ботов. Использование уязвимостей кода ПО, SDK. Подмена SDK. Внедрение ВПО
Владельцы приложений	H3	Подмена SDK. Использование не декларированных возможностей ПО
Поставщики рекламы	H3	Подмена SDK

Согласно модели нарушителя подмена SDK является способом, который могут потенциально реализовать наиболее опасные злоумышленники.

Типы мошенничества с мобильной рекламой. Для определения типов мошенничества с рекламой установлены действия, нарушающие требования участников схемы к рекламе. Основными пунктами договоренности между рекламодателем и поставщиком рекламы является требования к рекламодателю по формату файла рекламы, его разрешению, соответствию цензурным и другим ограничениям, невыполнение которых предполагает прекращение взаимодействия. Основные требования к рекламе предъявляют магазины приложений к реализуемом в нем ПО и поставщики рекламы к владельцам приложений, применяющих их рекламные модули.

На основе анализа требований 3 самых распространенных рекламных сетей (Google AdMob, Unity Ads, Amazon Mobile Ad Network Program), являющихся поставщиком рекламы, и 2 магазинов приложений (Google Play, Amazon Appstore) выделены 8 типов мошенничества с рекламой: скрытая реклама, наложение рекламы, перехват нажатий, флуд, навязчивая реклама, инъекция нажатий, подмена идентификатора, подмена контента. Фрагмент сопоставления типа мошенничества, требования, которое нарушается, и семейства рекламного ПО, являющегося примером реализации типа мошенничества с рекламой приведен в табл. 2.

Таблица 2

Фрагмент сопоставления типа мошенничества требованиям и семейству рекламного ПО

Тип мошенничества	Пример нарушенного требования магазина-приложений или рекламной сети	Пример семейств рекламного ПО
Скрытая реклама	Запрещается размещение рекламы за пределами дисплея	OsOneClick, Plague
	Запрещается использовать рекламу, неотличимую от другого контента в приложении	
	Запрещается размещение рекламы в фоновом режиме	
Флуд	Запрещается использовать сторонние сервисы, генерирующие показы и нажатия	Hamob, Judy, FakeAdBlocker
Перехват нажатий	Запрещается считывать нажатия вне рекламы как нажатия на рекламу	Ghost

Типы мошенничества с мобильной рекламой на уровне приложения. Подмена SDK, являющаяся наиболее частым способом реализации мошенничества согласно исследованию Juniper Research [5] и способом, доступным потенциально наиболее опасными злоумышленниками, реализуется на уровне приложения. Классификация типов мошенничества по уровню реализации представлена в табл. 3.

Таблица 3

Классификация типов мошенничества по уровню реализации

	Уровень реализации		
	Трафик	Приложение	Устройство
Тип мошенничества	Флуд нажатий через VPN Флуд нажатий через proxy-сервера Подмена идентификатора приложения Подмена контента	Скрытая реклама Наложение рекламы Навязчивая реклама Перехват нажатий Флуд нажатий Подмена идентификатора приложения	Флуд нажатий Инъекция нажатий Сброс идентификатора устройства

Уровень трафика соответствует модели «фиктивный пользователь – фиктивное действие». Мошенничество на уровне приложения подразумевает применение махинаций с рекламой в приложении, установленном на устройстве пользователя, что соответствует модели «реальный пользователь – реальное действие». Использование реальных устройств в мошенничестве с рекламой относится к уровню устройства, что соответствует модели «фиктивный пользователь – реальное действие».

Таким образом, типами мошенничества, реализуемыми на уровне приложения, являются скрытая реклама, наложение рекламы, навязчивая реклама, перехват нажатий, флуд нажатий, подмена идентификатора приложения.

Предлагаемый прототип системы обнаружения мошенничества с рекламой. Архитектура прототипа состоит из модулей сбора информации, вычисления признаков и классификации. На этапе сбора данных собираются параметры работы приложения, которые затем обрабатываются для определения признаков. В результате анализа приложений, реализующих типы мошенничества на уровне приложений, выделено 6 типов признаков приложений с мошенничеством: сетевой трафик, элементы интерфейса, разрешения, компоненты, события, поведение. Примерами признаков, относящихся к типу «сетевой трафик», являются коэффициент входящего трафика к исходящему без взаимодействия с приложением, коэффициент входящего трафика к исходящему после нажатия на интерфейс. На основе полученных признаков выполняется классификация приложения на предмет реализации в нем мошенничества с рекламой.

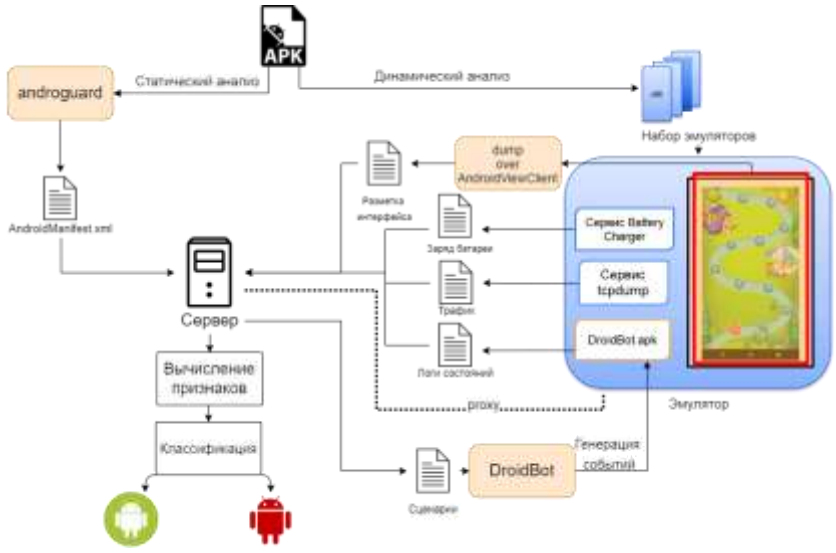

Рисунок. Общая схема реализации прототипа обнаружения мошенничества с рекламой на основе анализа работы Android-приложений

В реализации прототипа этап сбора данных состоит из статического и динамического анализа. При статическом анализе исследуется файл AndroidManifest.xml посредством утилиты androguard, из которого определяются разрешения, компоненты и события. Этап динамического анализа состоит в применении эмулятора из пакета Android SDK, на котором исполняется ис-

следуемый файл. В ходе его работы при использовании автоматизированного взаимодействия с помощью DroidBot записываются трафик, изменение заряда батареи, описание интерфейса, фоновые сервисы. Из полученных параметров вычисляется 59 признаков, которые передаются в классификатор. В качестве модели классификатор был выбрал случайный лес с 80 деревьями. Схема реализации прототипа приведены на рисунке.

Результаты тестирования метода обнаружения мошенничества с рекламой демонстрируют высокие значения для введенных типов мошенничества. Стоит отметить, что корректное сравнение точности предложенного метода с другими в настоящее время невозможно по причине отсутствия инструментов, реализующих аналогичный функционал. Однако при использовании предлагаемого прототипа в качестве бинарного классификатора, были получены результаты, превосходящие по точности средство FraudDroid [6] на 4 % по f1-мере (табл. 4).

Таблица 4

Сравнение предлагаемого прототипа с аналогом

Средство	Точность (accuracy)	Точность (precision)	Полнота (recall)	F1-мера
FraudDroid	0,93	0,92	0,94	0,92
Предложенный прототип	0,95	0,96	0,97	0,96

Заключение. В работе представлены типы мошенничества с мобильной рекламой, выделенные на основе анализа требований участником схемы работы рекламы, отчетов об инцидентах информационной безопасности. Предложенный в работе прототип обнаружения мошенничества с мобильной рекламой на основе анализа работы Android-приложений способен с высокой точностью определять приложения, реализующие мошенничество с мобильной рекламой.

ЛИТЕРАТУРА

1. Lexi Sydow. The New Normal in 2021: Five Things You Need to Know in Mobile // data.ai URL: https://www.data.ai/en/insights/market-data/2021-five-things-you-need-to-know-in-mobile/ (дата обращения: 09.04.2022).
2. Digital advertising spend lost to fraud to reach $68 billion globally in 2022 // Juniper Research URL: https://www.juniperresearch.com/press/digital-advertising-spend-lost-to-fraud-68-billion (дата обращения: 01.03.22).
3. Методика определения угроз безопасности информации в информационных системах. Проект. 2015.
4. Федеральная служба по техническому и экспортному контролю. Методический документ. Методика оценки угроз безопасности информации. 2021.
5. Ad Fraud Statistics (2022) // Business of Apps [Электронный ресурс]. URL: https://www.businessofapps.com/ads/ad-fraud/research/ad-fraud-statistics/ – (дата обращения: 15.05.2022).
6. FraudDroid: Automated Ad Fraud Detection for Android Apps // GitHub [Электронный ресурс]. URL: https://github.com/FraudDroid-mobile-ad-fraud /ExperimentResults – (дата обращения: 20.05.2022).

A.Y.Soldatova, D.P.Zegzhda, E.Y.Pavlenko (Peter the Great St. Petersburg Polytechnic University, Saint-Petersburg)

Detection of fraud with mobile advertising based on analysis of the work of Android applications

The paper presents an intruder model based on the study of mobile advertising scheme, with the help of which SDK spoofing was determined as the implementation method inherent in potentially the most dangerous intruders. As a result of the analysis of the participants requirements for advertising in applications 8 types of fraud were identified, 6 of which are realized by SDK spoofing. A prototype system for mobile advertising fraud detection in Android applications is presented, surpassing the analog by 4 % in f1-score.

Авторы готовы представить текст на английском языке для сборника материалов мультиконференции, который будет подан для индексирования в Scopus.