Столыпинский вестник

Научная статья

Original article

УДК 004.056.53

ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ КОМПРОМЕТАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ

IDENTIFYING SOURCES OF COMPROMISING PERSONAL DATA OF USERS OF MOBILE DEVICES

Мамадаев Муслим Магомедович, студент второго курса, МГТУ им.Н.Э.Баумана (2-я Бауманская ул., д.5, стр.1, Москва, 105005), Тел. +7(499) 263-63-91, mamad.muslim@mail.ru

Шмигельский Александр Сергеевич, студент второго курса, МГТУ им.Н.Э.Баумана (2-я Бауманская ул., д.5, стр.1, Москва, 105005), Тел. +7(499) 263-63-91, s5003626@gmail.com

Mamadayev Muslim Magomedovich, second-year student, Moscow State Technical University named after N.E. Bauman (2nd Baumanskaya st., 5, building 1, Moscow, 105005), Tel. +7(499) 263-63-91, mamad.muslim@mail.ru

Shmigelsky Alexander Sergeevich, second-year student, Moscow State Technical University named after N.E. Bauman (2nd Baumanskaya st., 5, building 1, Moscow, 105005), Tel. +7(499) 263-63-91, s5003626@gmail.com

Аннотация: Мобильные устройства обладают широкими техническими возможностями, что позволяет выполнять обработку разнообразных пользовательских данных, в том числе осуществлять банковские транзакции, что делает их привлекательными для вредоносного воздействия со стороны киберпреступников. В связи с наибольшей распространённостью платформы *Android,* исследование, проведенной в рамках написания настоящей статье, в области повышения уровня защищённости персональных данных пользователей мобильных устройства были ограничены данной платформой. В связи с вышеизложенным, авторами настоящей статьи, была предпринята попытка научного анализа и критического осмысления источников компрометации персональных данных у пользователей мобильных устройств.

Abstract: Mobile devices have wide technical capabilities, which allows you to process various user data, including banking transactions, which makes them attractive for malicious effects from cybercriminals. Due to the greatest prevalence of the Android platform, the study conducted in the framework of writing this article, in the field of increasing the level of security of personal data of mobile users, were limited by this platform. In connection with the above, the authors of this article, an attempt was made to scientific analysis and critical understanding of sources of compromising personal data among users of mobile devices.

Ключевые слова: защита персональных данных, киберпреступления, компрометация данных пользователей, защита информации, вредоносное воздействие, ОС Android.

Keywords: protection of personal data, cybercrimination, compromising user data, information protection, malicious effects, Android OS.

Корпорация Google (далее Google) и производители мобильных устройств постоянно совершенствуют систему безопасности, но открытость исходного кода и обширная фрагментация платформы делает данную систему одной из самых уязвимых для вредоносного воздействия. Главной причиной фрагментации экосистемы Android является применяемая технология при

создании мобильных устройств, основанная на системе кристалл/чип (system on a chip, SoC).

SoC заключается в интегрировании на одном микрочипе центрального процессора, графического ускорителя, радио-модуля и различной датчиковой аппаратуры.

Данная концепция позволяет уменьшить физический размер устройства, понизить энергопотребление и повысить производительность за счет лучшей интеграции компонентов, но для взаимодействия всей системы требуется разработка специальных драйверов. Драйвера разрабатываются производителями различных чипов на кристалле и, как правило, являются проприетарными и уникальны для каждой модели. В результате, производители мобильных устройств внедряют полученные драйвера для SoC – системы в собственную сборку, что приводит к зависимости процедур обновления программного обеспечения от производителя. [5, с. 119]

Из-за большого количества производителей чипсетов и мобильных устройств (ODM – производитель, изделия которого создаются по оригинальному проекту, OEM – производитель, детали и оборудование которого могут быть проданы другим производителям) образуется высокая степень фрагментации платформы без возможности оперативного обеспечения актуальными обновлениями мобильных устройств.

Политика Google направлена на обеспечение обновлениями устройств не старше 2-3 лет, что приводит к достаточно серьезным вопросам безопасности отрасли в целом. Соответственно, устройства старше трех лет, требуется считать потенциально уязвимыми. В случае сохранения тренда развития экосистемы Android к 2023 году оценка вероятности компрометации устройств на данной платформе будет в районе значения 0,4, что является причиной в потребности создания новых методов обеспечения безопасности пользовательских данных на мобильных устройствах. [1, с. 32]

В Российской Федерации правовое регулирование вопросов, связанных с персональными данными, осуществляется Федеральным законом от 27.07.2006

№ 152-ФЗ «О персональных данных». Согласно ст. 3 п. 1 ФЗ-152 персональными данными является любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу – субъекту персональных данных. Данный закон направлен на обеспечение защиты личной информации (далее PII, англ. personally identifiable information), относящейся к идентифицируемому лицу.

Рисунок 1. Классификация персональных данных

Определения личной информации определены в США в Руководящих принципах NIST по защите конфиденциальности личной информации (SP 800-122) и в Европе в Директиве ЕС 95/46/ЕС, а также ст. 4 Общего регламента по защите данных (GDPR).

Наиболее критическими данными являются «базовые», позволяющие с наибольшей степенью достоверности идентифицировать человека (ФИО, паспортные данные, дата и место рождения, место регистрации и место фактического проживания). Дополнительные данные не обеспечивают идентификацию личности напрямую, однако при наличии совокупности данных или совместно с базовыми данными, вероятность ошибки определения сводится к минимуму (информация об образовании, социальном статусе, профессии, номере телефона, номере страхового свидетельства и т.д.). Специальные персональные данные могут содержать информацию об ip – адресе, учётных записях и др. [7, с. 228]

К биометрическим персональным данным относится информация о физиологических и биологических особенностях человека. В условиях развития современных технологий, на основе голосового файла, либо изображения возможно идентифицировать пользователя с высокой точностью, что может служить основанием к признанию медиафайлов – персональными данными.

Дополнительные, специальные и биометрические типы данных (на основе которых невозможно однозначно определить их принадлежность конкретному лицу) далее будут обозначаться как сведения, соотносимые с конкретной личностью (далее ICP, англ. Information Correlation with the Person). В качестве примера, на рисунке 2 представлены типовые данные, обрабатываемые современными мобильными устройствами.

Таким образом, вопрос обеспечения сохранности данных в условиях объёма обрабатываемых и генерируемых PII и ICP на мобильных устройствах является важным. Рассмотрим основные типы программных источников, применяемых с целью возможной компрометации личности владельца устройства.

К данным типам источников относятся: [3, с. 162]

- службы операционных систем и сервисы, установленные производителями устройств;

- браузеры, осуществляющие сбор и хранение данных о посещённых страницах, а также веб-ресурсы, хранящие идентификаторы пользователя (например token или cookies);

- легальные приложения, обрабатывающие персональные данные;

- вредоносное программное обеспечение.

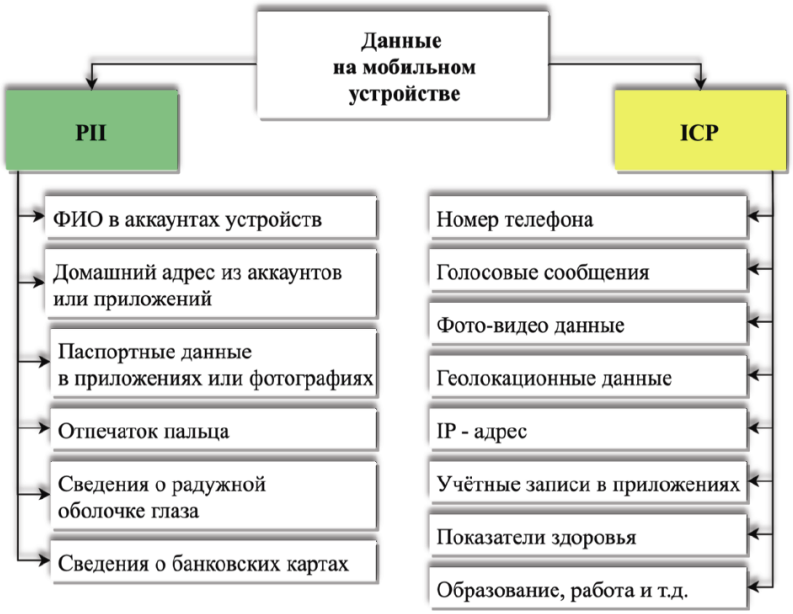

Рисунок 2. Обрабатываемые персональные данные на мобильном устройстве

В настоящее время техники распространения ВПО на мобильных устройствах классифицируются следующим образом: [4, с. 952]

1. Эксплуатация уязвимостей ядра Linux и его модулей. ОС Android является дистрибутивом Linux с собственной реализацией функций межпроцессорного взаимодействия, управления режимом «сна», защиты ядра (механизмом разделяемой памяти и т.д.) и высвобождения памяти. Таким образом, уязвимости, найденные в общих компонентах ядра, возможно применять на мобильных устройствах. Эксплойты (фрагмент программного кода или последовательность команд) предназначены для использования уязвимостей в ядре с целью получения пользовательских данных или повышения привилегий до прав администратора. Успешность проведения атаки может привести к отключению системы безопасности Android и установки «руткита» (скрытие активности вредоносных программ). Также одним из существующих векторов атак является наличие уязвимостей в модулях ядра производителей устройства.

2. *Эксплуатация уязвимостей аппаратных модулей*. Мобильные устройства обладают большим количеством аппаратных модулей, предназначенных для взаимодействия с другими устройствами. Данный тип

уязвимостей возможно эксплуатировать в зоне действия радиомодулей или при наличии физического доступа к мобильному устройству. Примеры атак: «отказ в обслуживании» на технологию *Wi-Fi Direct*; кража реквизитов банковских карт с помощью *NFC*; исполнение кода через уязвимость в *Bluetooth*; использование отладочного механизма через *adb* для администрирования устройства.

3. *Эксплуатация возможностей механизмов межкомпонентного взаимодействия.* Функционирование приложения ограничено песочницей процесса, что не позволяет производить непосредственный обмен данными между различными компонентами системы. Реализация обмена выполняется с помощью передачи и получения данных через устройство */dev/Binder* и различные сервисы ОС *Android*. Данный механизм имеет определённые архитектурные недостатки, позволяющие приложениям формировать запрос к данным через другие приложения с требуемыми разрешениями и получать результат через *ICC* (англ. *Integrated Circuit Card*). [2, с. 89]

4. *Эксплуатация уязвимостей в компонентах операционных систем, программах и драйверах*. Позволяет атакующей стороне обходить средства защиты *Android* и *SELinux*.

5. *Эксплуатация уязвимостей в компонентах производителей мобильных устройств*. Производители устройств, выполняют модификацию *Android*, размещая различные приложения в директории «*system*», т.е. запуск процессов производится в привилегированном режиме. Данные приложения могут содержать уязвимости, приводящие к утечкам данных, захвату учетных записей и установке ВПО. Также, производители сами могут модифицировать систему с целью внедрения недекларированного функционала.

6. *Эксплуатация уязвимостей в библиотеках*. В архитектуру *Android* включен ряд библиотек таких как *OpenGL, Audio Manager, Media Framework, libc* и т.д. Эксплуатирование уязвимостей в данных компонентах является одним из главных векторов атаки на текущий момент. Наиболее распространенные уязвимости компонента *Media Framework* позволяют

производить атаки типа удаленного выполнения кода (RCE) на пораженном устройстве (например, при работе с электронной почтой, просмотре сайтов в Интернете или обработке медиафайлов MMS).

7. *Эксплуатация уязвимостей в машинных кодах*. *Android* содержит инструментарий, позволяющий выполнять код C и C++ (Android NDK). Данная возможность порождает ошибки, характерные для низкоуровневых языков программирования (переполнением буфера, утечки памяти и т.д.). Сторонние библиотеки имеют возможность использования разрешений, выданных приложению, для совершения недекларированной активности. Сокрытие вредоносных функций и модулей приложения в машинных кодах зачастую используются авторами вредоносных приложений для обхода первичного анализа системами *Android*. [6, с. 225]

8. *Эксплуатация уязвимостей в пользовательских приложениях*. Приложения, установленные пользователем, могут содержать персональные данные, но хранение и доступ к данной информации не всегда обеспечивается должным образом (использование HTTP трафика, файлы данных приложения размещены в папках с общим доступом и т.д.).

9. *Использование методов социальной инженерии*, применяемые для передачи и последующей установки ВПО из различных источников (в том числе Play Market).

Анализ существующих техник распространения и закрепления ВПО показывает разнообразие векторов атак на мобильные ОС. В связи с большим количеством программно-аппаратных возможностей появляются несвойственные стационарным ПК виды воздействия на устройство. Также, различные методы сигнатурного и поведенческого анализа обладают рядом недостатков в условиях функционирования на мобильных устройствах. В мобильной разработке применение методов динамической загрузки исполняемого кода, полиморфизма или обфускации является распространённым явлением, что существенно понижает эффективность сигнатурных методов анализа кода.

Литература

1. Грибанов, А. А. Определение персональных данных, разграничение операторов и обработчиков персональных данных / А. А. Грибанов // Судья. – 2021. – № 4(124). – С. 30-34.
2. Жура, В. С. Методы определения признаков компрометации мобильного устройства / В. С. Жура // Ростов-на-Дону, 30 апреля 2022 года. – г. Ростов-на-Дону: Общество с ограниченной ответственностью "Манускрипт", 2022. – С. 88-90.
3. Иваченков, И. И. Защита данных пользователей от несанкционированной модификации на мобильных устройствах / И. И. Иваченков // Решение. – 2021. – Т. 1. – С. 161-162.
4. Калакуток, Б. А. Финансовое влияние компрометации персональных данных на деятельность компаний в условиях цифровизации экономики / Б. А. Калакуток // Экономика и предпринимательство. – 2021. – № 6(131). – С. 951-954.
5. Мамыкина, Е. В. Правовой статус субъектов, участвующих в персональных данных: субъект персональных данных; оператор персональных данных / Е. В. Мамыкина // Моя профессиональная карьера. – 2020. – Т. 3. – № 11. – С. 117-122.
6. Новик, А. М. Анализ безопасности идентификации пользователя в мобильном приложении при различных методах защиты персональных данных / А. М. Новик // Минск: Белорусский государственный университет информатики и радиоэлектроники, 2021. – С. 224-226.
7. Новик, А. М. Исследование скорости идентификации пользователя в мобильном приложении при различных методах защиты персональных данных / А. М. Новик // Минск: Белорусский государственный университет информатики и радиоэлектроники, 2021. – С. 227-229.

Literature

1. Gribanov, A. A. Definition of personal data, differentiation of operators and processors of personal data / A. A. Gribanov // Judge. - 2021. - No. 4 (124). – P. 30-34.
2. Zhura, V. S. Methods for determining signs of compromise of a mobile device / V. S. Zhura // Rostov-on-Don, April 30, 2022. - Rostov-on-Don: Manuscript Limited Liability Company, 2022. – P. 88-90.
3. Ivachenkov, I. I. Protection of user data from unauthorized modification on mobile devices / I. I. Ivachenkov // Solution. - 2021. - T. 1. – P. 161-162.
4. Kalakutok, B. A. Financial impact of personal data compromise on the activities of companies in the context of digitalization of the economy / B. A. Kalakutok // Mamykina, E. V. Legal status of subjects involved in personal data: subject of personal data; personal data operator / E. V. Mamykina // My professional career. - 2020. - T. 3. - No. 11. – P. 117-122.
5. Novik, A. M. Security analysis of user identification in a mobile application with various methods of personal data protection / A. M. Novik // Minsk: Belarusian State University of Informatics and Radioelectronics, 2021. – P. 224-226.
6. Novik, A. M. Study of the user identification speed in a mobile application with various methods of personal data protection / A. M. Novik // Minsk: Belarusian State University of Informatics and Radioelectronics, 2021. – P. 227-229.

Для цитирования: Мамадаев М.М., Шмигельский А.С. ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ КОМПРОМЕТАЦИИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ // Научный сетевой журнал «Столыпинский вестник» №1/2023.