Шаханова М.В., Солоненко Д.Ю. Управление информационной безопасностью мобильных устройств на платформе Android // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 1(27) с. 36–43

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ МОБИЛЬНЫХ УСТРОЙСТВ НА ПЛАТФОРМЕ ANDROID

Шаханова М.В., Солоненко Д.Ю.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: marinavl2007@yandex.ru

В настоящее время платформа Android является одной из самых распространенных платформ во всем мире. Большая часть людей пользуются телефонами на базе Android, хранят свои личные данные, банковские счета и фотографии, даже не задумываясь о том, сколькими способами можно потерять данные. В этой связи вопрос безопасности становится особенно актуальным. В этой статье речь пойдет о том, как происходит защита данных пользователя и какие существуют способы противодействия можно реализовать на этой платформе.

Ключевые слова: информационная безопасность бизнеса, Android, системная безопасность, защитник приложений, конфиденциальность, анализ программы, антивходной модуль.

MANAGEMENT OF INFORMATION SECURITY OF MOBILE DEVICES ON THE ANDROID PLATFORM

Shakhanova M. V., Solonenko D.Yu.
Maritime State University named after G.I. Nevelskoy, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: marinavl2007@yandex.ru

Currently, the Android platform is one of the most common platforms around the world. Most people use Android phones, store their personal data, bank accounts and photos, without even thinking about how many ways they can lose data. In this regard, the issue of security becomes particularly relevant. In this article, we will talk about how user data is protected and what methods of counteraction can be implemented on this platform.

Keywords: information Security, Android, System Security, Application Defender, Privacy, Program analysis, Anti-intrusion module.

С ростом популярности мобильных телефонов на платформе Android все больше внимания уделяется защите конфиденциальной информации на базе платформы Android.

После того, как в 2008 году Google выпустила интеллектуальную платформу Android 1.0, Android быстро заменил Symbian благодаря своему уникальному преимуществу с открытым исходным кодом и стал равным iPhone в индустрии мобильных телефонов. Производители мобильных телефонов конкурировали за выпуск мобильных телефонов с платформой Android и продемонстрировали рыночную тенденцию превышения спроса над предложением. В настоящее время все больше и больше людей используют мобильные телефоны с платформой

Android, число которых в Китае исчисляется десятками тысяч, особенно это касается молодых потребителей, стремящихся к моде.

Люди могут скачать Android бесплатно и внести в свою жизнь удобство и удовольствие. Однако они могут намеренно или ненамеренно сохранять свою личную информацию в мобильных телефонах. С более высокой степенью интеллектуализации мобильных телефонов это явление имеет тенденцию быть универсальным, и все больше и больше пользователей склонны сохранять свою личную информацию на мобильных телефонах, потому что это более удобно и конфиденциально по сравнению с ПК. Таким образом, случайная защита конфиденциальности мобильных телефонов может нести неизвестные риски для людей [1].

В жизни часто приходится видеть, что вы находите свой мобильный телефон оставленным дома, когда работаете; или в офисе после того, как вы вернетесь домой с работы; или в общежитии, когда вы находитесь в классе. Хуже того, вы можете найти его потерянным. В этих обстоятельствах не только мобильный телефон недоступен для использования, но и вы будете обеспокоены конфиденциальностью личных данных в мобильных телефонах.

В настоящее время большинство защитных программ или средств защиты мобильных телефонов с платформами Android (включая разблокировку экрана и разблокировку паролем) препятствуют нормальному использованию мобильных телефонов в некоторой степени. Таким образом, чтобы обеспечить нормальное и бесперебойное использование мобильных телефонов, пользователи предпочитают закрыть эти процедуры или меры. Кроме того, когда мобильные телефоны недоступны, утеряны или украдены, уже слишком поздно принимать меры безопасности. Когда мобильные телефоны утеряны, информация о конфиденциальности в них важнее.

После того, как контактная информация, содержимое SMS и информация о данных на SD-карте будут использованы незаконными лицами, трудно себе представить последствия.

Различные исследовательские и опытно-конструкторские группы укрепляют свои преимущества и предлагают свои меры защиты информации мобильных телефонов. В целом, для современных платформ Android программное обеспечение для защиты информации мобильного телефона в основном делится на следующие категории:

1. Блокировка экрана [2], которая охватывает блокировку экрана паролем и блокировку экрана жестами. Принцип заключается в том, чтобы предварительно установить команду ввода мобильного телефона, и каждый раз, когда мобильные телефоны включаются, им требуется определение пароля, что может предотвратить несанкционированное вторжение мобильных телефонов. Недостаток - неудобство.

2. Системная безопасность [3], обладающая различными функциями и обеспечивающая сканирование на вирусы [4–8], обнаружение файлов [9–12], антидомогательство звонков и сообщений для мобильных телефонов. Его особенность заключается в разнообразии функций, но он занимает слишком много системных ресурсов, что снижает удобство использования мобильных телефонов. Он не принадлежит к тому же диапазону этого исследования. Кроме того, надежность такого рода процедур крайне низка, и приватность пользователя легко может быть украдена [12].

3. Защитник приложений, принцип работы которого основан на использовании обычных прикладных программ для сохранения конфиденциальной информации пользователей. При запуске некоторых процедур может выполняться проверка команды для

защиты конфиденциальной информации пользователя. Его недостаток такой же, как блокировка экрана, препятствующая нормальному использованию мобильных телефонов [11].

Вышеуказанные три вида программ защиты информации имеют хорошее применение, и большинство мобильных телефонов обычно используют одну или несколько из них [11–12]. Кроме того, предлагается схема обнаружения Wi-Fi с помощью определения местоположения [5], позволяющая пользователю разумно переключаться на интерфейс Wi-Fi.

Однако все эти методы имеют следующие недостатки:

1. Меры защиты должны быть установлены заранее. Когда мобильные телефоны потеряны, невозможно составить план на случай чрезвычайной ситуации
2. Они очень хрупкие и все их можно прямо запретить или удалить.
3. Из-за отсутствия эффективного механизма управления паролями, как только пользователи забудут пароль или команду, возникнут проблемы.
4. Они снижают эффективность использования мобильного телефона, препятствуют нормальному использованию мобильных телефонов или занимают слишком много места.

Структура системы индивидуальной защиты конфиденциальности на платформе Android

Эта система разделена на передний интерфейс, фоновую программу и обработку данных. Пользователи могут выполнять соответствующие функции в интерфейсе переднего плана, например, переключение режимов, изменение информации, резервное копирование и восстановление контактов и восстановление пароля. Фоновая программа в основном включает четыре подсистемы, соответственно, подсистему обработки SMS, подсистему блокировки мобильного телефона, подсистему управления задачами и подсистему самозащиты. Система обработки данных в основном отвечает за операции, связанные с данными.

Архитектура системы показана на Рисунке 1. Телом взаимодействия между активным интерфейсом и фоновой программой является функция. Интерфейс переднего плана предназначен для выполнения некоторых специфических функций, например, переключение режимов, изменение информации, резервное копирование и восстановление контактов, восстановление пароля, отправка электронной почты, включение и отключение сетевых соединений.

- Подсистема управления задачами предназначена для управления фоновыми задачами, включая выполнение задач, устранение дублирования задач, контроль информации о конфигурации задач и восстановление прерываний задач;
- Подсистема обработки SMS отвечает за соответствующую обработку сообщений, включая мониторинг SMS, чтение и отправку SMS.
- Подсистема технического обслуживания отвечает за условия работы системы в оборудовании, включая запуск системы и непрерывную работу системы после запуска;
- Подсистема блокировки мобильных телефонов предназначена для блокировки мобильных телефонов для предотвращения незаконного использования мобильных телефонов, включая отображение информации о владельце, отображение причин блокировки экрана, восстановление пароля, связь с владельцем, прием телефонных звонков и разблокировку; подсистема защиты предназначена для самозащиты

системы, борьбы со злонамеренным повреждением системы внешним миром, включая принудительную остановку, очистку данных и удаление.

Удаленные мобильные телефоны могут взаимодействовать с системой, отправляя SMS, и выполнять соответствующие команды, содержащие пароль, например, блокировку, резервное копирование и форматирование. При резервном копировании контактной информации системе необходимо отправлять данные по сетевым соединениям, а данные контактной информации отправляются на почтовые серверы. При получении информации о текущем местоположении сетевые соединения и поставщик услуг на основе определения местоположения используются для передачи данных, отправки запроса на определение местоположения и получения информации о местоположении.

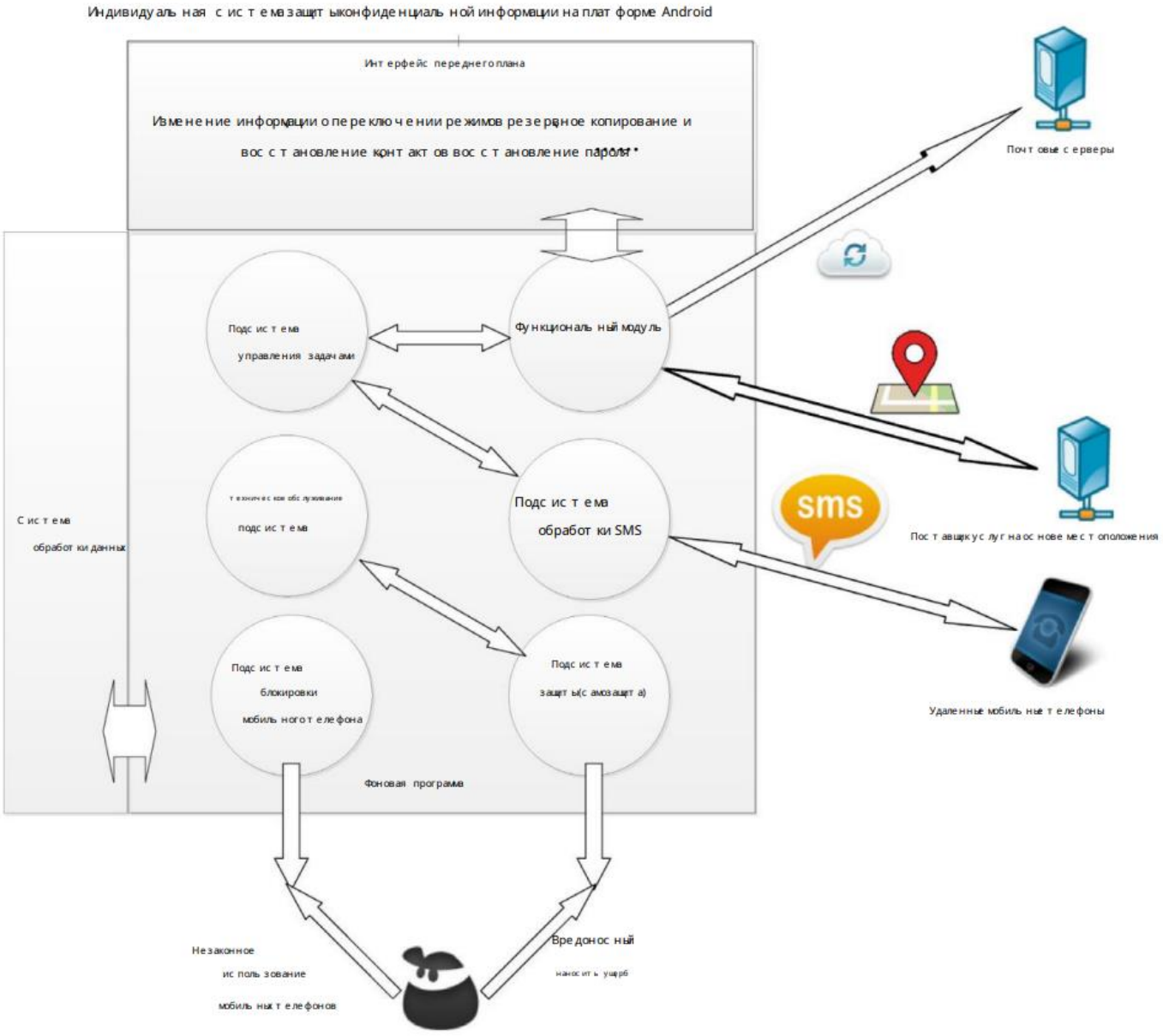

Рисунок 1 – Общая архитектура системы индивидуальной защиты конфиденциальности на платформе Android

Однако многие другие SMS-приложения на платформе Android (например, message) и SMS-приложения, разработанные другими производителями, имеют собственные функции мониторинга. Следовательно, для реализации перехвата SMS приоритет приемника широковещательной рассылки в этой системе по отношению к полученным SMS должен быть выше, чем у других приложений.

Полноэкранный антивходной модуль

В Android SDK есть прямой API экрана блокировки. Таким образом, экран блокировки этой системы должен создаваться вручную. В типичных мобильных телефонах Android пользовательские интерактивные компоненты включают панель уведомлений, главный экран и клавиатуру. Методы экрана для каждого интерактивного компонента показаны в таблице 1.

Ключ к полноэкранному антивходу лежит в построении полноэкранного интерфейса. Не существует способа освободить интерфейс, кроме автоматического освобождения, а именно отключения и перезапуска. Он может отображать панель уведомлений и клавиатуру мобильных телефонов Android. В этом интерфейсе есть место для отображения причин блокировки экрана, отображения информации о владельце, связи с владельцами, пароля.

Таблица 1 – Интерактивные компоненты мобильных телефонов Android и способы их отображения

Интерактивные компоненты	Отображение
Домашний экран	Экран блокировки дисплея
Панель уведомлений	Полноэкранный режим
Клавиатура	Экранная клавиатура

В платформе Android существует три способа реализации цели: уничтожение прикладных программ, принудительная остановка, удаление и очистка данных. На рисунке 2 показаны три режима деструкции программы. Эти три состояния подлежат, соответственно, копированию.

Принятый метод - процесс резервирования. Порождая два процесса и используя связь между ними, воспринимаются жизненные условия между ними. При обнаружении уничтожения одного процесса принимаются соответствующие меры по защите мобильных телефонов. Чтобы справиться с уничтожением данных очистки, необходимо выполнить синхронизацию данных между ведущими и подчиненными программами, чтобы предотвратить очистку данных одного процесса. В соответствии с различными типами данных и режимами синхронизации данных типы данных делятся на два типа: системные данные и данные записи дистанционного управления.

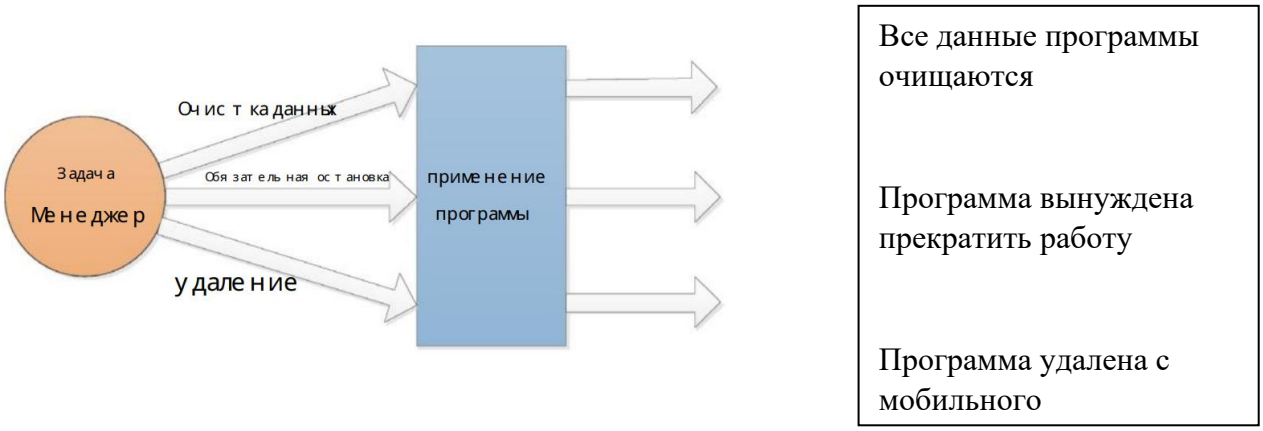

Рисунок 2 – Принципиальная схема трех режимов анализа программы

Чтобы повысить авторитет пользователя, диспетчер задач Android может удалить любую стороннюю программу, которая может эффективно препятствовать распространению вирусного троянца до определенного уровня. Однако в нем также может скрываться опасность нормальной работы этой системы. В режиме защиты используется механизм защиты процессов Android, чтобы пользователи не мешали работе системы.

Большинство представленных на рынке программ для защиты информации мобильных телефонов используют архитектуру C/S, которая сохраняет пароль на сервере. Когда пользователи забывают коды, они могут найти пароль через сервер. Это хлопотно и может иметь определенные потенциальные риски. Вышерассмотренная система позволит их избежать.

Список литературы

1. Wei TE, Jeng AB, Lee HM, Chen CH, Tien CW (2012) Конфиденциальность Android. В: Международная конференция по машинному обучению и кибернетике (ICMLC), 2012 г., том 5. IEEE, С. 1830–1837.
2. Винсент Мессина (2012 г.) Android4.0: экран блокировки.
3. Enck W, Ongtang M, McDaniel P (2009) IEEE Secur Priv 1: 50–57
4. Chiang HS, Tsaur WJ (2010) Поведенческий анализ мобильных вредоносных программ и превентивная стратегия с использованием онтологии. Опубликовано: Вторая международная конференция IEEE по социальным вычислениям (SocialCom), 2010 г. IEEE, С. 1080–1085
5. Алазаб М., Мунсами В., Баттен Л., Ланц П., Тиан Р. (2012) Анализ вредоносных и безопасных приложений для Android. В 2012 году прошла 32-я международная конференция по распределенным вычислительным системам (ICDCSW). IEEE, С. 608–616.
6. Zhou Y, Jiang X (2012) Анализ вредоносных программ для Android: характеристика и эволюция. В: Симпозиум IEEE 2012 г. по безопасности и конфиденциальности (SP). IEEE, С. 95–109.
7. Адил М., Токарчук Л.Н. (2011) Анализ системы обнаружения мобильных вредоносных программ с помощью семейств cabir и commwarrior. В: Третья международная

конференция IEEE 2011 г. по конфиденциальности, безопасности, рискам и доверию (PASSAT) и третья международная конференция IEEE 2011 г. по социальным вычислениям (SocialCom). IEEE, С. 1335–1343

8. Шмидт А.Д., Бай Р., Шмидт Х.Г., Клаузен Дж., Кираз О., Юксель К.А., Камтепе С.А., Албайрак С. (2009) Статический анализ исполняемых файлов для совместного обнаружения вредоносных программ на Android. В: IEEE международная конференция по коммуникациям, 2009. ICC'09.IEEE, С. 1–5
9. . Бласинг Т., Батюк Л., Шмидт А.Д., Камтепе С.А., Албайрак С. (2010) Система песочницы приложений Android для обнаружения подозрительного программного обеспечения. In: 2010 5-я международная конференция по вредоносному и нежелательному ПО (MALWARE). IEEE, С. 55–62.
10. Burguera I, Zurutuza U, Nadjm-Tehrani S (2011) Crowdroid: система обнаружения вредоносных программ на основе поведения для Android. В: Материалы 1-го семинара ACM по безопасности и конфиденциальности в смартфонах и мобильных устройствах. ACM, С. 15–26
11. Шабтай А., Канонов Ю., Эловичи Ю., Глезер С., Вайс Ю. (2012) безопасность. IEEE Secur Priv 1: 50–57 международная конференция по коммуникациям, 2009. ICC'09. IEEE, стр. 1–5 "Andromaly": поведенческий фреймворк для обнаружения вредоносного ПО для устройств Android. J Intell Inf Syst 38(1):161–190
12. Shakya N (2012) Вопросы конфиденциальности антивирусных приложений для смартфонов. В: 12-й исследовательский симпозиум студентов по компьютерным наукам Winona, С. 17.

References

1. Wei TE, Jeng AB, Lee HM, Chen CH, Tien CW (2012) Android Privacy. In: International Conference on Machine Learning and Cybernetics (ICMLC), 2012, Volume 5. IEEE, pp. 1830–1837.
2. Vincent Messina (2012) Android4.0: lock screen.
3. 3. Enck W, Ongtang M, McDaniel P (2009) IEEE Secur Priv 1: 50–57
4. Chiang HS, Tsaur WJ (2010) Behavioral analysis of mobile malware and preventive strategy using ontology. Published: Second IEEE International Conference on Social Computing (SocialCom), 2010 IEEE, pp. 1080–1085
5. Alazab M., Munsami V., Batten L., Lantz P., Tian R. (2012) Android Malicious and Safe Application Analysis. In 2012, the 32nd International Conference on Distributed Computing Systems (ICDCSW) was held. IEEE, pp. 608–616.
6. Zhou Y, Jiang X (2012) Android malware analysis: characterization and evolution. In: 2012 IEEE Symposium on Security and Privacy (SP). IEEE, pp. 95–109.
7. Adil M., Tokarchuk L.N. (2011) Analysis of the mobile malware detection system using the cabir and commwarrior families. Q: 2011 IEEE Third International Conference on Privacy, Security, Risk, and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom). IEEE, pp. 1335–1343

8. Schmidt A.D., Bai R., Schmidt H.G., Clausen J., Kiraz O., Yuksel K.A., Kamtepe S.A., Albayrak S. (2009) Static analysis of executable files for joint malware detection on android. In: IEEE International Communications Conference, 2009. ICC'09.IEEE, pp. 1–5
9. Blasing T., Batyuk L., Schmidt A.D., Kamtepe S.A., Albayrak S. (2010) Android Application Sandboxing System for Suspicious Software Detection. In: 2010 5th International Conference on Malicious and Unwanted Software (MALWARE). IEEE, pp. 55–62.
10. Burguera I, Zurutuza U, Nadjm-Tehrani S (2011) Crowdroid: A behavior-based malware detection system for Android. In: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. ACM, pp. 15–26
11. Shabtai A., Kanonov Yu., Elovichi Yu., Glezer S., Weiss Yu. (2012) Security. IEEE Secur Priv 1: 50–57 International Communications Conference, 2009. ICC'09. IEEE, pp. 1–5 "Andromaly": A Behavioral Malware Detection Framework for Android Devices. J Intell Inf Syst 38(1):161–190
12. Shakya N (2012) Privacy issues in smartphone antivirus applications. In: 12th Winona Computer Science Student Research Symposium, pp 17.