ЗАЩИТА ДАННЫХ МОБИЛЬНЫХ УСТРОЙСТВ НА БАЗЕ ОС ANDROID

Сидорова М.А.

Сидорова Марина Андреевна – магистрант,
кафедра общей физики,
Институт физики
Казанский (Приволжский) федеральный университет, г. Казань

Аннотация: *на сегодняшний день практически все смартфоны стали носителями важных персональных либо корпоративных данных. Также посредством телефона владельца можно легко получить доступ к его учетным записям, таким как Gmail, DropBox, FaceBook, персональным данным — паролям, номерам кредитных карт и адресам, и даже корпоративным сервисам. Поэтому в той или иной степени стоит побеспокоиться о конфиденциальности этих данных и использовать специальные средства для защиты телефона от несанкционированного доступа в случае его кражи или утери.*

Встроенные и бесплатные функции для защиты телефона являются весьма надежными. Они способны защитить от посторонних глаз контакты пользователя, его переписку и звонки, аккаунты в различных программах и сетях, а также файлы и папки, расположенные как в памяти телефона, так и на съемной SD-карте. Однако, при проведении анализа каждого способа защиты и детальном их изучении можно выявить ряд уязвимостей, которые будут являться для злоумышленника пропуском к Вашим персональным данным. Самый простой способ снять блокировку мобильного устройства – так называемый «хард ресет», однако, данный способ ведет к полной потере данных и всех установленных программ, так как, по сути, это возвращение телефона к заводским настройкам без сохранения данных. Поэтому рассматривать этот способ мы не будем.

В данной статье будут рассмотрены преимущества и недостатки встроенных средств защиты данных на устройствах Android, а также описана реализация приложения для ОС Android в качестве нового инновационного способа защиты данных мобильного устройства. Приложение представляет собой экран блокировки смарфтона, который позволяет устранить все текущие недостатки встроенных средств защиты смартфона.

Ключевые слова: ОС Android, экран блокировки, защита мобильных устройств, смартфоны, мобильное приложение, безопасность.

Встроенные средства защиты данных на устройствах Android

Операционная система Android обеспечивает восемь различных методов блокировки телефона или планшета, которые могут быть включены в «Настройки», «Безопасность», «Экран блокировки» (меню зависит от телефона).

- Прикосновение к экрану (Slide — для разблокировки необходимо провести пальцем по экрану в определенном направлении) — фактически, защита отсутствует;
- Распознавание лица (низкий уровень безопасности);
- Лицо и голос (низкий уровень безопасности);
- Подпись (низкий уровень безопасности);
- Рисунок или графический ключ (средний уровень безопасности);
- PIN (средний или высокий уровень безопасности);
- Пароль (высокий уровень безопасности);
- Отпечаток пальца (высокий уровень безопасности).

Рассмотрим подробнее преимущества и недостатки каждого способа защиты, исключая способ прикосновения к экрану, так как в данном способе отсутствует какая-либо защита.

1. Экран блокировки с Графическим Ключом.

Графический ключ – это один из самых популярных и удобных способов оградить свою личную информацию от просмотра нежелательными лицами. Предварительно вам следует выбрать уникальный графический узор, проведя пальцем линию, соединяющую в определенной последовательности девять точек квадрата размером 3*3 (рис. 1), появляющихся на дисплее смартфона. Эта комбинация и будет являться впоследствии ключом. Надёжность графического ключа варьируется в зависимости от сложности узора и количества задействованных точек.

Рис. 1. Экран блокировки с графическим ключом

Недостаток:

Однако у данного способа есть один существенный недостаток. Не все телефоны оснащены олеофобным покрытием - специальный слой, отталкивающий жир. То есть, отпечатки пальцев на таком покрытии не должны оставаться, но даже с таким покрытием экран заляпывается. Таким образом, владелец сам показывает, как разблокировать его аппарат. Просто посмотрев на экран, можно увидеть след от пальца и, перебрав несколько комбинаций, разблокировать девайс. Можно, конечно, протирать экран после каждого использования, но в реальной жизни довольно малое количество владельцев смартфонов прибегают к этому.

Также Ресурс «Phonearena» проводил небольшое исследование, в котором было изучено порядка 4000 различных графических ключей. [1] Выяснилось, что 77% из них начинаются с одного из четырёх углов, а 44% начинаются с левого верхнего. Более того, 10% всех комбинаций представляют собой какую-либо букву.

Поэтому для обеспечения безопасности рекомендуется использовать не менее 5 точек, что даст более 7000 комбинаций, а также использовать узоры с пересечением линий и включать опцию "Скрыть ключ", чтобы никто не смог подглядеть вводимый вами узор.

2. Распознавание лица

Еще один встроенный способ защиты смартфона - настроить устройство так, чтобы блокировка снималась при распознавании Вашего лица. Для этого нужно поместить телефон непосредственно перед лицом экраном к себе, выровнять изображение Вашего лица на экране в соответствии с белыми точками и подождать, пока телефон закончит сканирование лица, это занимает около 7-10 секунд (рис. 2).

Рис. 2. Распознавание лица

Недостаток:

Поначалу эта удобная и эффектная опция понравилась многим пользователям, однако через непродолжительное время первоначальные восторги уступили место разочарованию, так как оказалось, что блокировку можно взломать с помощью простой фотографии, либо телефон может разблокировать человек, похожий на вас.

В Android 4.1 этот недостаток был исправлен. Теперь для разблокировки устройства недостаточно просто смотреть в камеру. Потребуется несколько раз моргнуть, чтобы гаджет «поверил», что перед ним живой человек. К сожалению, можно взломать данный вид защиты посредством анимированной картинки. Для реализации задуманного потребуется не так уж много: фотография владельца, редактор изображений и минимальные навыки по ретушированию изображений.

3. Лицо и голос

Подобный вариант разблокирования дисплея работает подобно предыдущему способу. Разница состоит лишь в том, что дополнительно к визуальной идентификации владельца смартфон добавляет еще и голосовое распознавание. Для корректной работы система должны иметь образцы вашего голоса.

Недостаток:

Впрочем, эта система так же ненадежна, как и фото-пароль. Ее можно легко обмануть, продемонстрировав смартфону фотографию его владельца и прокрутив перед микрофоном аудиозапись его голоса, а также, если устройство попадет к человеку с голосом или лицом похожим на Ваш, он без особых усилий сможет им воспользоваться.

4. Подпись

В данном случае вам необходимо написать ваше ключевое слово (предлагается написать ваше имя) трижды (рис. 3). Именно с помощью данного слова и будет разблокировано ваше устройство.

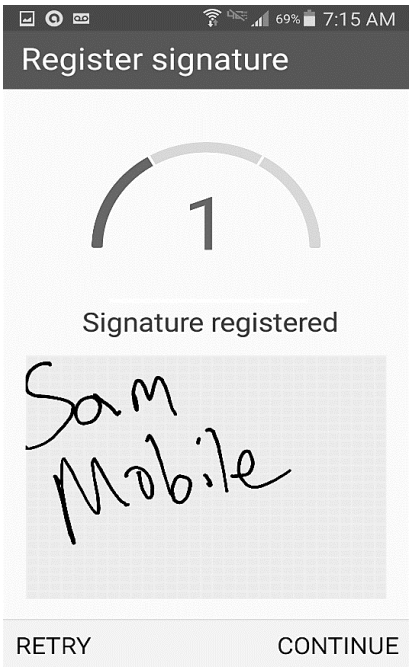

Рис. 3. Настройка разблокировки с помощью подписи

Недостаток:

Так как по умолчанию предлагается написать свое имя, злоумышленнику, обладающему даже минимальной информацией о владельце устройства, подделать ключевое слово не составит большого труда.

5. PIN-код и пароль

PIN – последовательность цифр, не менее четырех символов. Естественно, чем длиннее строка цифр, тем выше уровень безопасности. На разблокировку дается в общей сложности двадцать попыток, разделенных по пять штук с «минутой отдыха» между ними.

Пароль – наиболее высокий уровень безопасности. Содержит сочетание букв и цифр. Если вы используете пароль для доступа, можете использовать опцию «Шифрование телефона».

Недостатки:

Исследователи из университета Кембриджа Sören Preibusch и Ross Anderson опубликовало первый в мире количественный анализ сложности угадывания 4-циферного PIN-кода [2]. Всё бы хорошо, но, к сожалению, существенная часть опрошенных (23%) выбирает PIN-код в виде даты, — и почти треть из них использует дату своего рождения. Если злоумышленник знает день рождения владельца карты, то при грамотном подходе вероятность угадывания PIN-кода взлетает до 9%. Аналогичная ситуация и с паролем - если злоумышленник обладает информацией о Ваших персональных данных (имя, фамилия, дата рождения, кличка домашнего питомца и т.д.), то в большинстве случаев данное кодовое слово или комбинация и будет являться паролем. Можно использовать сложные пароли, состоящие из цифр и букв типа "qw29Nfp8QDcdf34hlgt", но простым людям, возможно, будет несколько неудобно вводить такой пароль каждый раз, когда надо разблокировать смартфон, так что напрямую стоит выбор между удобством и безопасностью.

Стоит добавить, что PIN-код или пароль также можно подобрать по оставшимся отпечаткам пальцев на экране смартфона.

6. Отпечаток пальца

О преимуществах использования технологии идентификации владельца мобильного устройства по отпечатку его пальца, сказано уже немало. Если выделить два основных компонента, то это будут удобство использования и открывающиеся новые возможности.

Недостаток:

К сожалению, при использовании данного способа защиты можно лишиться доступа к данным даже из-за небольшого пореза или загрязнения подушечки пальца. Однако, по умолчанию всегда задается альтернативный способ разблокировки экрана, например, PIN-код.

Вопрос о надежности защиты данных с помощью отпечатка пальца был поднят на конференции экспертов по разработке систем безопасности Black Hat в Лас-Вегасе [3]. Эксперты из FireEye повергли публику в шок, когда рассказали, что в некоторых Android-смартфонах отпечатки пальцев хранятся в незашифрованном виде. В частности, специалисты выяснили, что в аппарате HTC One Max отпечатки пальцев находятся в общем разделе файловой системы в виде незащищенного графического файла

dbgraw.bmp. Эти данные также уязвимы на аппаратах Samsung и Huawei. В результате злоумышленники с помощью любого вредоносного процесса или приложения могут получить доступ к данному изображению в высоком разрешении. К счастью, эту «лазейку» для хакеров уже постарались прикрыть. Однако эти обновления включены в последние версии Android, в то время как в прежних остались бреши.

Приложение блокировки экрана «Emoji» для смартфонов на базе ОС Android

Проанализировав недостатки всех вышеописанных способов защиты смартфонов, мною было реализовано приложение для блокировки экрана смартфона «Emoji» - это приложение для защиты вашего смартфона с помощью определенного ключа - последовательности смайликов, которая задается Вами при первоначальном запуске. Использование смайлов широко распространено в современном мире, так как данный элемент виртуальной формы общения очень удобен и информативен. Именно поэтому смайлики остаются не только прерогативой виртуального общения в Интернете или по мобильной связи, но и начинают прочно закрепляться и в других сферах деятельности человека.

Для задания пароля (комбинации смайликов) необходимо перетащить определенное количество смайликов с центральной части экрана, где они располагаются в случайном порядке, в нижнюю (рис. 4). На рисунке 4 для простоты представления и описания функциональности рассмотрен один из вариантов реализации приложения, где максимальное количество смайликов для установки пароля равно 8, и, следовательно, пароль может составлять комбинацию от 1 до 8 смайлов. Чем большее количество смайлов будет представлено для задания пароля, тем надежнее будет защита смартфона, так как число возможных комбинаций возрастает.

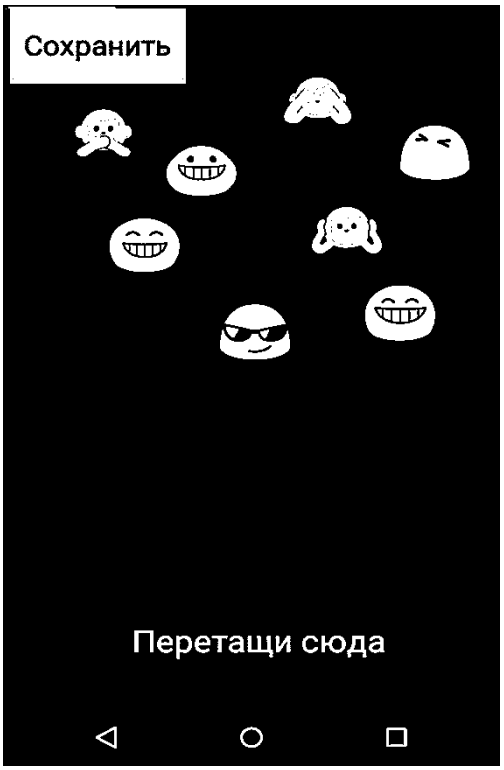

Рис. 4. Установка пароля блокировки экрана в приложении «Emoji»

Число возможных комбинаций при длине пароля от 1 до 8 смайлов будет составлять 109600, что уже полностью исключает возможность подбора пароля перебором. Однако, учитывая тот фактор, что обычно владельцы смартфонов задают пароль максимально простой к запоминанию, будем рассматривать ситуацию, что максимальная длина пароля будет составлять 5 смайликов. Используя основную формулу комбинаторики числа размещений A_n^m из n по m (1):

$$A_n^m = n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-m+1) = \frac{n!}{(n-m)!}, \qquad (1)$$

где n = 8 (количество элементов всего), а m равно длине пароля, несложно посчитать, что при длине пароля до 5 смайликов, общее количество возможных комбинаций будет составлять сумму размещений от 1 до 5 из 8 и равно 8800:

$A_8^1+A_8^2+A_8^3+A_8^4+A_8^5 = 8+56+336+1680+6720 = 8800$.

При каждой блокировке экрана смартфона расположение смайликов на экране меняется в случайном порядке, что исключает вероятность разблокировать телефон по следам от пальцев на экране.

Также данный способ блокировки экрана телефона защитит от случаев, когда злоумышленник, обладая даже самой минимальной информацией о владельце смартфона, сможет подобрать пароль или PIN-код, так как разгадать количество и последовательность смайлов в пароле достаточно сложно.

Количество попыток ввода пароля ограничено - 10 раз. Приложение также имеет дополнительную возможность ввода PIN-кода или аккаунта Google для случаев, когда владелец устройства забудет свой смайл-пароль.

Данным приложением можно заблокировать не только доступ к экрану, но и к другим важным папкам. Для этого достаточно «провалиться» в дополнительные настройки защиты системы и выбрать из предлагаемых папок нужные. Так, вы можете защитить персональные данные и пароли социальных сетей и аккаунтов, важных документов, телефонный справочник и многое другое.

Выводы:

Использовать или нет встроенные средства защиты смартфона, каждый может решить самостоятельно. По моему мнению, тут важно сохранить баланс между удобством использования и безопасностью, что как раз-таки достигается использованием приложения блокировки экрана «Emoji» - оно интуитивно понятно и удобно в использовании, обеспечивает высокую степень надежности, а также имеет привлекательный графический интерфейс, что немаловажно для молодого поколения - целевой аудитории пользователей смартфонов. Тем, кто хочет надежно защитить персональную информацию, можно посоветовать использовать многоуровневую защиту, тем более, что современные смартфоны - это позволяют. Например, после ввода пароля, графического ключа или PIN-кода идентифицироваться при помощи отпечатка пальца [4].

Вооружившись необходимой информацией, почерпнутой из этой статьи, и проведя несколько дополнительных действий со своим смартфоном на базе ОС Android, можно надежно защитить его от доступа к нему посторонних лиц.

Список литературы

1. Веб-сайт www.phonearena.com, статья «Study finds that Android lock patterns tend to be too simple, just like passwords» [Электронный ресурс]. Режим доступа: http://www.phonearena.com/news/Study-finds-that-Android-lock-patterns-tend-to-be-too-simple-just-like-passwords_id72948/ (дата обращения: 10.06.2017).
2. Информационный портал по безопасности, статья «Сложно ли угадать PIN-код?» от 13.09.2012. [Электронный ресурс]. Режим доступа: http://security-corp.org/os/android/5826-slozhno-li-ugadat-pin-kod.html/ (дата обращения: 10.06.2017).
3. Сетевое новостное издание RT News, статья «Хакеры рассказали о способах кражи отпечатков пальцев у владельцев устройств на Android» от 07.08.2015 [Электронный ресурс]. Режим доступа: https://russian.rt.com/article/107807/ (дата обращения: 11.06.2017).
4. Информационный веб-ресурс http://gsmpress.ru, статья «Сканер отпечатков пальцев в смартфоне: плюсы и минусы» от 11.11.2016 [Электронный ресурс]. Режим доступа: http://gsmpress.ru/articlesitem/2511-skaner-otpechatkov-palcev-v-smartfone%3A-pljusy-i-minusy.html#sthash.jUJWFjfX.dpuf/ (дата обращения: 10.06.2017).