УДК 004.056.53 + 004.451

Кондрашин Д. В., Горшенин В. В.

ГРАФИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ДЛЯ ANDROID УСТРОЙСТВ

Целью данной работы является разработка собственного программного продукта, реализующего надежную графическую аутентификацию для мобильной операционной системы Android. Приложение должно быть устойчиво, к самым распространенным видам атак, в частности к атаке подглядывания из-за плеча. В итоге было создано приложение AlphaLocker, которое сейчас доступно для скачивания в Google Market. Имеется уже около 500 скачиваний из разных стран мира. В данные момент ведется доработка приложения с учетом полученных комментариев.

Ключевые слова: *информационная безопасность, аутентификация, схема треугольника, мобильные операционные системы, Android, графический пароль.*

Kondrashin D. V., Gorshenin V. V.

GRAPHIC AUTHENTICATION FOR ANDROID DEVICES

The aim of the article is to develop individual software which implements reliable graphical authentication for Android mobile operating system. The application is to be resistant to the most common types of attacks and spying over the shoulder attack in particular. As a result, the AlphaLocker application was created and is now available for download in Google Market. There have already been about 500 downloads from various countries all over the world. At the moment the application is being debugged taking into account comments received.

Keywords: *information security, authentication, delta network, mobile operating systems, Android, picture password.*

Сейчас сложно представить человека, не имеющего смартфона или планшетного компьютера. В связи с этим объем и важность информации, хранимой на мобильных устройствах, стремительно растут. И, следовательно, необходимы средства для защиты хранимой информации и самого устройства от несанкционированного доступа.

Наиболее логичным и простым решением данной проблемы является использование надежной схемы аутентификации в системе.

Наиболее распространенным методом аутентификации в компьютерной системе является механизм, основанный на том, что пользователь вводит имя пользователя и текстовый пароль. Однако у этой схемы можно выделить ряд недостатков.

Например, буквенно-цифровые пароли обеспечивают высокую безопасность, если

они сложны. Однако многие пользователи испытывают трудности в запоминании случайных строк символов.

Поэтому становятся возможными атаки по словарю или атаки полного перебора. Другой недостаток символьного пароля заключается в том, что такая схема аутентификации не решает так называемую проблему «подглядывания из-за плеча». Заключается она в следующем: если во время ввода пароля злоумышленник имеет возможность увидеть или снять на видео процесс ввода пароля, то он без труда сможет повторить его позже.

В рамках данной работы речь пойдет о другой альтернативе текстовым паролям - графической аутентификации. Графические пароли имеют ряд преимуществ.

Использование изображений в качестве паролей делает невозможной атаку по словарю частично из-за большого пространства паролей и, главное, потому что не существует доступных для поиска словарей для графической информации. И наконец, некоторые схемы графической аутентификации позволяют решить проблему «подглядывания из-за плеча».

Целью данной работы является разработка собственного программного продукта, реализующего надежную графическую аутентификацию для одной из наиболее популярных мобильных операционных систем – Android.

При выборе метода аутентификации было решено использовать *схему треугольника*, так как она наиболее понятна для пользователя и одновременно устойчива к подглядыванию через плечо. При входе система будет случайным образом выбирать размещение N изображений. При установке пароля пользователь выбирает M изображений из базы размера N. При входе система случайным образом выбирает и рассеивает по экрану K изображений из базы, среди которых ровно 3 парольных. Пользователь должен найти выбранные парольные изображения и выбрать область внутри невидимого треугольника, созданного этими 3 изображениями.

Учитывая, что приложение ориентировано для использования на планшетных компьютерах и смартфонах, схема была несколько изменена с целью адаптации под мобильные устройства.

- Использовались легко запоминаемые графические изображения в виде латинских строчных и прописных букв.
- Изображения выводятся на экран в дискретной сетке.
- Уменьшение количества выводимых на экран изображений за счет разбиения раунда на два этапа и опционального задания количества успешно пройденных раундов (в первой половине раунда пользователь должен выбрать изображение внутри парольного треугольника, во второй половине – вне треугольника).
- Также для усложнения подбора пароля количество ошибок при вводе пароля ограничено, после чего происходит блокировка устройства.
- Площадь парольного треугольника не должна превышать 1/3 экрана.

Рис. 1. Первая половина раунда

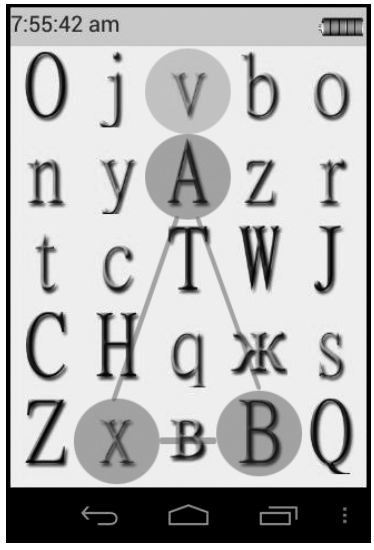

Рис. 2. Вторая половина раунда

Рис. 3. Выбор графического пароля

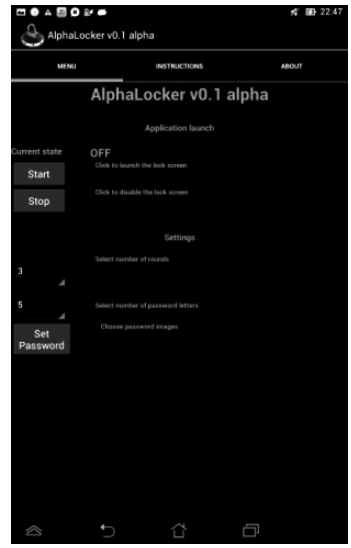

Рис. 4. Меню настройки

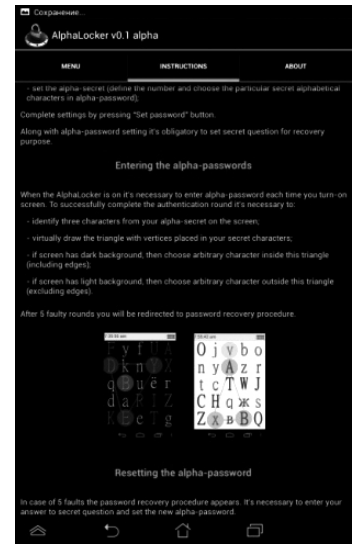

Рис. 5. Вкладка Instuctions

При такой реализации вероятность пройти один раунд наудачу приближенно равняется 0,016, причем при увеличении количества раундов она уменьшается экспоненциально.

Количество возможных паролей есть «биномиальный коэффициент». В нашем случае при N = 52, M = 5 число возможных паролей равно 2598960. При этом реализация приложения допускает всего 5 ошибок, что делает атаку полным перебором на данное приложение практически невозможной.

В случае подглядывания из-за плеча понадобится около 700 полноценных записей входа в систему, чтобы определить пароль пользователя. То есть если пользователь будет входить в систему каждый день в среднем по 10 раз, включая выходные и праздники, злоумышленнику придется подсматривать за ним почти 2 месяца.

Следующим шагам для создания надежного приложения был анализ ОС Android, в частности пришлось столкнуться со следующими проблемами:

• Запуск приложения при блокировке экрана.

• Не системное приложение не может перехватить нажатие кнопки Home.

• Не системное приложение не может перехватить двойное нажатие/удерживание кнопки Home, вызывающее менеджер задач.

• Блокировка остальных аппаратных кнопок.

Для решения первой и последней проблем достаточно переопределить соответствующие обработчики системных событий.

Решением второй проблемы являлось написание собственного системного загрузчика приложений (Launcher) и его установка в систему. Для этого при установке приложения пользователь должен согласиться с изменением загрузчика по умолчанию. После чего, если экран заблокирован, то вызывается наш загрузчик, который не позволяет закрыть приложение нажатием кнопки Home. После входа пользователя в систему, управление передается стандартному загрузчику android и система функционирует как обычно.

Для решения третьей проблемы при вызове менеджера задач приложение автоматически выбирает себя текущей задачей, после чего посылает сообщение о закрытии менеджера.

Последним этапом в разработке приложения было создание максимально удобного для пользователя интерфейса (вывод заряда батареи, уведомлений о пропущенных звонках и смс, отображение времени на экране блокировки и другое).

А также создание меню настроек, в котором пользователь может включить или отключить блокировку экрана приложением, установить количество раундов и парольных картинок. Здесь же происходит установка или изменение пароля. При первом запуске пользователь может беспрепятственно установить пароль и настройки для восстановления пароля. Для смены пароля потребуется ввести подтверждение старого пароля. Также стоит отметить, что изменение количества раундов или парольных изображений происходит только при смене пароля.

Для удобства пользователя в меню существует вкладка “Instructions”, которая содержит описание всех необходимых от пользователя действий по настройке приложения и аутентификации в системе.

В итоге было разработано приложение AlphaLocker, которое реализует схему треугольника для экрана блокировки операционной системы Android.

Далее был проведен ряд тестов, чтобы убедиться, что разработанное приложение действительно обеспечивает надежную защиту устройства и хранимой на нем информации.

Приложение доступно в Google Market по ссылке:

https://play.google.com/store/apps/details?id=com.AlphaLocker

или на официальном сайте:

http://alphalocker.bloolocker.com/

Примечания

1. Sobrado L., Birget, J. Graphical Passwords // The Rutgers Scholar, Rutgers University, Camden New Jersey. – 2002. - 4.
2. Jansen W., Gavrila S., Korolev и др. Picture Password: A Visual Login.
3. Technique for Mobile Devices // NIST Report - NISTIR7030. – 2003.
4. Голощапов А. Л. Google Android. Создание приложений для смартфонов и планшетных ПК. 2-е издание // БХВ-Петербург, 2013.
5. Рето Майер. Android 4. Программирование приложений для планшетных компьютеров и смартфонов // М.: Эксмо, 2013

Кондрашин Дмитрий Вячеславович, студент ЧелГУ. E-mail: dimon-280894@mail.ru

Горшенин Владимир Викторович, ст. преподаватель ЧелГУ.

Dmitry Vyacheslavovich Kondrashin, student of Chelyabinsk State University. E-mail: dimon-280894@mail.ru

Vladimir Viktorovich Gorshenin, senior lecturer of Chelyabinsk State University.