Mobile Devices as a Platform for Biometric Security
Gavrikov I. (Russian Federation)
Мобильные устройства как перспективная платформа для биометрической безопасности
Гавриков И. В. (Российская Федерация)

Гавриков Илья Владимирович / Gavrikov Ilya – студент,
кафедра бизнес-информатики и математического моделирования,
Институт экономики и управления,
Крымский федеральный университет имени В. И. Вернадского, г. Симферополь

Аннотация: *данная статья описывает технологию MBS (мобильной биометрической безопасности) — перспективного применения мобильных устройств как бюджетных платформ для аутентификации пользователя по его биометрическим данным.*
Abstract: *the article describes MBS technology (Mobile Biometric Security) – the prospective use of mobile devices as budget platforms for user authentication based on their biometric data.*

Ключевые слова: *мобильные устройства, биометрия, аутентификация, информационная безопасность.*
Keywords: *mobile devices, biometrics, authentication, information security.*

Персональные мобильные устройства становятся всё более многофункциональными, заменяя собой и вытесняя с рынка существующие устройства.

В то же время, информационная безопасность и мобильные устройства становятся всё более взаимосвязаны. Двухфакторная аутентификация уже используется в таких компаниях как Google, Twitter, Facebook, Apple, Microsoft, Valve Software, Blizzard Entertainment и других и даже внедрена в качестве средства безопасности в MIT. Однако у двухфакторной аутентификации также существуют свои уязвимости [1], что вынуждает производителей и разработчиков использовать более сложные алгоритмы аутентификации. Один из вариантов таких алгоритмов — биометрическая аутентификация.

Многофакторная аутентификация зависит от базового фактора, обычно представляемого фактором знания — например, паролем или PIN-кодом. Базовый фактор дополняется другим фактором (или несколькими), которые могут включать в себя фактор владения, т.е. то, что имеется у пользователя в наличии, и фактор свойства, т.е. то, что неотделимо от пользователя. Двухфакторная аутентификация обычно использует факторы владения в виде одноразовых кодов, отправляемых пользователю или генерируемых на его устройстве. Факторы свойства включают в себя отпечатки пальцев, черты лица, радужные оболочки глаз и голос. Пользователю легче предоставить эти факторы для проведения аутентификации, однако их труднее регистрировать и хранить, среди прочего из-за вопросов приватности.

По сравнению с факторами владения факторы свойства используются не так широко. Тем не менее, крупные компании уже начинают использовать биометрию в своих алгоритмах аутентификации. С добавлением сканера отпечатка пальца в iPhone 5S, биометрическая аутентификация поистине вышла на массовый рынок. По данным исследований количество сканеров отпечатка пальца в устройствах увеличится на 17% до 2020 года [2]. На рынке голосовой биометрии также ожидается до 22% роста в период 2014-2019 гг. [3]. На рынок выходит и лицевая биометрия — так, MasterCard недавно запустила пилотную программу аутентификации пользователей посредством селфи [4]. Стоит также отметить недавнее объявление Samsung о добавлении системы сканирования радужной оболочки глаза в свой новый флагман, Galaxy Note 7 [5].

Постоянно растущие требования к безопасности и преимущества, связанные с использованием биометрической аутентификации, дополняют друг друга, однако до недавнего времени внедрение биометрической аутентификации требовало большого количества средств и ресурсов, что является серьёзным препятствием для предприятий малого бизнеса. Однако с появлением биометрических технологий в современных мобильных устройствах, сравнимый уровень безопасности может быть достигнут со значительно меньшими затратами. Такой подход, называемый автором технологией MBS (mobile biometric security, мобильная биометрическая безопасность), позволяет любому предприятию, способному приобрести мобильное устройство, внедрить биометрические меры безопасности.

Ввиду количества разных сенсоров и функций, встроенных в современные мобильные устройства, MBS-приложения могут использоваться для создания многоуровневой системы безопасности на основе лишь одного устройства. Так, современный смартфон с комплексным MBS-приложением способен аутентифицировать пользователей на основе их отпечатка пальца, голоса, черт лица и радужной оболочки глаза одновременно, что в связке с PIN-кодом или паролем в качестве базового фактора значительно затрудняет взлом системы безопасности компании. MBS-приложение на мобильном

устройстве может быть использовано для защиты целого ряда имущества компании — от информации до рабочих станций и до самого здания или офиса.

Главная слабость технологии MBS на данный момент заключается в относительной сложности создания алгоритмов для надёжной идентификации и верификации биометрических данных. Однако затраты на исследования и разработку программного уровня на порядок меньше стоимости сравнимых по функциональности коммерческих наборов и комплексов безопасности.

Литература

1. *Konoth Radhesh Krishnan, van der Veen Victor, Bos Herbert*. How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. VU University Amsterdam, 2015. 17 с.
2. Biometrics Market Boosted By Fingerprint Sensors in Smartphones. [Электронный ресурс]: ABIresearch.URL: https://www.abiresearch.com/press/biometrics-market-boosted-by-fingerprint-sensors-i/ (дата обращения: 18.08.2016).
3. *Swapnil Devale*. Voice Recognition Biometrics Market Statistics. [Электронный ресурс]: LinkedIn. URL: https://www.linkedin.com/pulse/voice-recognition-biometrics-market-statistics-expected-devale/ (дата обращения: 18.08.2016).
4. Replacing Passwords with Selfies. [Электронный ресурс]: MasterCard Newsroom. URL: http://newsroom.mastercard.com/videos/replacing-passwords-with-selfies/ (дата обращения: 18.08.2016).
5. Samsung doubles down on security with iris scanner in Galaxy Note 7. [Электронный ресурс]: The Verge. URL: http://www.theverge.com/2016/8/2/12348580/samsung-doubles-down-on-security-with-iris-scanner-in-galaxy-note-7/ (дата обращения: 20.08.2016).