DOI: 10.30888/2415-7538.2018-09-2-025

УДК 004.056.53

PROBLEMS OF INFORMATION SECURITY OF MOBILE USERS
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ

Gnidenko I.G. / Гниденко И.Г.
c.e.s., as. prof. / к.э.н., доц.
Egorova I.V. / Егорова И.В.
c.e.s., as. prof. / к.э.н., доц.
Chernoknizhnyi G.M./Чернокнижный Г.М.
c.t.s., as.prof. / к.т.н., доц.
Saint-Petersburg State University of Economics,
St. PetersburgRussian Federation, 21 Sadovaya street, 191023
Санкт-Петербургский государственный экономический университет,
Россия, 191023, Санкт-Петербург, улица Садовая, дом 21

Аннотация. *В работе рассматриваются информационные угрозы пользователям, возникающие при пользовании мобильными устройствами, в частности: угрозы, связанные с похищением персональных данных; угрозы целостности данных; угрозы, связанные с несанкционированным использованием принадлежащих пользователю устройств и нарушением их работы. Рассматриваются меры, повышающие безопасность персональных данных пользователей.*

Ключевые слова: *угроза, безопасность, персональные данные, пароль, аутентификация, криптография, антивирус.*

С широким распространением применения мобильных устройств и роста популярности сетевых сервисов возник целый ряд новых проблем и угроз компьютерной безопасности. При этом часть проблем относится к безопасности корпоративных и служебных данных, а другая угрожает безопасности личных данных обычных пользователей.

Стало трудно полностью отделить личные данные от служебных. Смартфоны, которые являются личными устройствами, могут подключаться к корпоративным сетям и одновременно использоваться для ведения частной переписки и доступа в социальные сети. Это создает угрозу, как целостности, так и обеспечению конфиденциальности корпоративных или служебных данных. И здесь по-прежнему лучшим решением может являться запрет использования личных устройств или ограничения для сотрудников на использование некоторых сетевых ресурсов, например, социальных сетей.

Угрозы рядовым пользователям можно разделить на несколько категорий:

—угрозы, связанные с похищением персональных данных;

—угрозы целостности данных;

—угрозы, связанные с несанкционированным использованием принадлежащих пользователю устройств и нарушением их работы.

Широкое распространение интернет магазинов и электронных платежных систем создает угрозу похищения персональных данных пользователя. Утрата смартфона и пренебрежение элементарными правилами обеспечения безопасности могут привести к пропаже денег со счетов и получению злоумышленниками кредитов от имени пользователя [1].

Сетевые сервисы, такие как: электронная почта, социальные сети, интернет магазины, облачные хранилища данных, платежные системы, требуют от пользователей предоставления личных данных в различном объёме. При этом личные данные могут быть похищены как при атаках на сервисы из сети Интернет, так и недобросовестными сотрудниками, обеспечивающими работу этих сервисов. После этого персональные данные могут быть использованы преступниками при совершении мошеннических сделок [2, 3]. Правда, для этого обычно нужны не просто персональные данные, а сканированные паспортные данные.

Ситуацию усугубляет обнаружение серьёзных ошибок в системном программном обеспечении, а такие ошибки выявляются регулярно. Последний инцидент связан с обнаружением критической уязвимости в протоколе WPA2, который используется для защиты передаваемых данных в сетях Wi-Fi. Обнаруженная уязвимость позволяет читать зашифрованную информацию, передаваемую между точкой доступа и пользовательскими устройствами. Информация об уязвимости была опубликована в октябре 2017 года, но исправления некоторыми производителями оборудования и программного обеспечения выпущены только в начале 2018 года [4]. И это обычная для таких случаев ситуация, выпуск исправлений требует от нескольких дней до нескольких месяцев.

Недостаточные знания рядовых пользователей о компьютерной безопасности также ухудшают ситуацию, не все пользователи понимают необходимость применения антивирусов. По данным собранным Microsoft более чем на 50% компьютеров с операционной системой Windows 10 антивирус либо выключен, либо не обновляется [5]. Не лучше ситуация и на мобильных устройствах под управлением Android.

В последнее время и некоторые специалисты по компьютерной безопасности говорят о бесполезности антивирусного программного обеспечения. Это объясняется тем, что даже использование антивируса не гарантирует полную защиту компьютера или мобильного устройства, так как постоянно появляются новые угрозы и способы проникновения вредоносного программного обеспечения на компьютеры, планшеты и смартфоны [6].

Кроме того, сами антивирусы несут потенциальную угрозу для пользователей, так как для своей работы требуют прав на доступ к ресурсам компьютера, которых обычно не имеет рядовой пользователь. Поэтому антивирус может собирать данные и отправлять их в указанное место.

Кроме применения антивирусов имеется ещё ряд рекомендаций для пользователей, которые позволяют повысить их уровень безопасности. Список таких рекомендаций можно найти на сайтах ведущих российских разработчиков антивирусов: «Лаборатория Касперского», «Доктор Веб». Для пользователей банковских систем рекомендации по безопасности обычно приведены на сайте соответствующего банка.

Одной из рекомендуемых мер безопасности является применение только легального программного обеспечения. Однако известны случаи распространения троянских программ вместе с программным обеспечением,

полученным из официального магазина GooglePlay. В сентябре 2017 года в игре “JewelsStarClassic” была обнаружена функциональность, предназначенная для похищения данных банковских карт [7]. Через некоторое время после установки игра запрашивала разрешения на доступ к специальным возможностям Android, если пользователь давал доступ, то программа могла выводить поддельное окно для настройки платежного сервиса. При этом запрашивались данные банковской карты, которые потом отправлялись вирусописателям.

Этот пример показывает важность следования еще одной рекомендации для пользователей Android: при установке программы и в дальнейшем при её эксплуатации внимательно относится к запрашиваемым программой разрешениям. Иногда лучше отказаться от пользования программой, если не ясно с какой целью она запрашивает некоторые разрешения.

К угрозам целостности данных относятся некоторые вирусы, блокирующие работу компьютера. При этом они могут зашифровывать данные пользователя. За разблокировку и расшифровку требуют вознаграждение. При этом даже в случае уплаты вознаграждения данные не всегда восстанавливаются. Чтобы не потерять важную информацию пользователям рекомендуется регулярно выполнять резервное копирование.

Способом распространения вирусов-вымогателей может быть, например, письмо, полученное по электронной почте. Поэтому ещё одна рекомендация по безопасности для пользователей заключается в том, чтобы не открывать письма, полученные из неизвестных источников, такие письма лучше сразу удалять.

Защитить данные пользователя от несанкционированного доступа позволяют системы идентификации и аутентификации [8]. К ним, прежде всего, относятся системы парольной защиты. Широкое распространение таких систем обусловлено низкой стоимостью и простотой организации и использования. Однако надежность парольных систем защиты во многом ограничивается действиями самих пользователей, которые предпочитаю использовать несложные пароли, одинаковые для различных ресурсов, а также халатно относятся к хранению паролей. Исследования, проводимые специалистами в области информационной безопасности, позволило выявить наиболее часто используемые пароли (табл.1) [9].

Для раскрытия пароля пользователя может быть использован метод тотального перебора, при котором подбор пароля осуществляется с помощью проверки всех возможных сочетаний символов. Сложность и длительность такого подбора существенно возрастает с увеличением длины пароля, а также мощности алфавита (количеством различных символов, используемых в пароле).

Многие пользователи предпочитают использовать короткие, легко запоминаемые пароли, содержащие небольшой набор символов (табл.2, 3)[9].

Таблица 1

Наиболее часто используемые пароли

Пароль	Доля (%)
1234567	3,36
12345678	1,65
123456	1,02
Пустая строка	0,72
12345	0,47
7654321	0,31
qweasd	0,27
123	0,25
qwerty	0,25
123456789	0,23

Таблица 2

Наиболее часто используемые наборы символов

Набор символов	Доля (%)
Только цифры	52,73
Символы английского алфавита в нижнем регистре	17,96
Символы английского алфавита в нижнем регистре и цифры	17,51
Символы английского алфавита в разных регистрах и цифры	3,4
Символы английского алфавита в разных регистрах	1,63
Символы английского алфавита в верхнем регистре и цифры	1,35
Символы русского алфавита в нижнем регистре	1,12

Разработчики современных информационных ресурсов требует от пользователя задания длинных паролей, обязательно включающих как прописные и строчные буквы русского и латинского алфавита, так и цифры, и специальные символы. Из таблицы видно, что использование пароля становится все более популярным, но большинство владельцев смартфонов продолжают устанавливать четырехзначный PIN-код, который легко обходится одним из следующих способов:

—можно подсмотреть во время ввода;

—найти в социальных сетях данные, имеющие значения для пользователя (имена и фамилии пользователя и членов его семьи, даты рождения, клички домашних животных и т.д.). Статистика использования подобных «слабых» с точки зрения возможности раскрытия паролей приведена в табл.4 [9];

—использовать брутфорс или полный перебор. Если подключить, например, к смартфону iOS устройство IP-Box, можно перебрать все четырехсимвольные пароли за 17 часов.

Помимо простого перебора для раскрытия пароля пользователя может использоваться метод словарной атаки, при котором в качестве паролей проверяются слова, входящие в публично распространяемые словари, или их

модификация (изменение раскладки клавиатуры, порядка следования букв в слове на обратный и т.д.).

Таблица 3

Длина используемых пользователем паролей

Количество символов	Доля (%)
0	0,71
1	0,26
2	0,39
3	1,37
4	2,03
5	4,86
6	27,22
7	21,75
8	25,22
9	6,5
10	4,42
11	2,83
12	1,33
13	0,4
14	0,34
15	0,1
16	0,09
17	0,02
18	0,01
19	0,01
20	0,008
>20	0,02

Таблица 4

Статистика использования легко раскрываемых паролей

Содержание пароля	Доля (%)
Полное совпадение пароля с именем пользователя	3,94
Частичное совпадение пароля с именем пользователя	0,7
Пароль содержится в публично распространяемых словарях	14,69
Пароль является пустой строкой	0,7

Одни и те же пароли могут использоваться в течение длительного периода, их своевременная смена не производится. Более того, одни и те же пароля могут использоваться для доступа к различным ресурсам. Обычно пользователи не конфигурируют устройство так, чтобы информация на смартфоне удалялась после нескольких неудачных попыток ввода пароля.

Все эти факторы существенно снижают эффективность парольной защиты.

Усилить защиту и снизить угрозы третьего типа, связанные с несанкционированным использованием принадлежащих пользователю

мобильных устройств, позволяет использование биометрической, а также двухфакторной аутентификации. Сама по себе биометрическая аутентификация не является решением всех проблем, но она избавляет от ввода паролей, более проста и доступна обычному пользователю.

Наиболее популярный способ биометрической аутентификации – на основе отпечатков пальцев. Однако он не свободен от недостатка: хакеры научились создавать поддельные отпечатки пальцев. При этом, в отличие от паролей, отпечатки нельзя изменить в случае их попадания в руки хакера. Если отпечаток используется для доступа к Apple Pay, PayPal, или Samsung Pay на мобильном устройстве, риски от использования поддельных отпечатков значительно возрастают. Но создание поддельных отпечатков требует времени и хороших навыков. Поэтому шансы на то, что хакер или вор использует устройство для доступа к данным раньше, чем пользователь сотрет всю информацию при помощи удаленной команды, достаточно малы.

Усиленную защиту дает двухфакторная аутентификация: биометрия и сильный пароль. Этот режим доступен как при использовании Apple Touch ID, так и Samsung Fingerprint Scanner.

Дополнительно защитить информацию позволяет шифрование данных, реализованное на iOS-устройствах и на устройствах на базе Android.

Рекомендуется также установить приложения на ноутбук или компьютер, которые позволяют удаленно обнаруживать инциденты на смартфоне и блокировать его или стирать информацию.

Можно сделать вывод, что число угроз информационной безопасности растет, и они становятся более разнообразными, а методы противодействия им более сложными и нет универсального средства, применение которого гарантировало бы полную безопасность.

Минимальными требованиями к защите мобильных устройств являются: использование программ и данных, полученных только из надёжных легальных источников, надежная аутентификация, использование криптографии, выполнение резервного копирования наиболее важной информации в облако, применение антивируса. При этом более защищёнными будут пользователи, знающие об актуальных угрозах и понимающие механизмы, которыми пользуются злоумышленники.

В заключении остается добавить: в использовании мобильного устройства самым важным является бдительность его владельца: нужно всегда сохранять свой смартфон как кошелек с деньгами.

Литература:

1. Как персональные данные могут использоваться для мошенничества с сотовыми операторами [электронный ресурс]. URL:http://www.securitylab.ru/blog/company/securityinform/153190.php (дата обращения 30.03.2018).

2. Гниденко И.Г., Мердина О.Д. Методы защиты программного обеспечения от несанкционированного доступа// Международная научно-практическая конференция «Перспективы развития науки и образования».

Сб.науч.тр.- М.: АР-Консалт, 2013. - С. 110-115.

3. Как берутся кредиты по чужому паспорту [электронный ресурс]. URL:http://www.securitylab.ru/blog/company/securityinform/152810.php (дата обращения 31.03.2018).

4. Опубликована подробная информация о проблемах WPA2 [электронный ресурс]. URL:https://xakep.ru/2017/10/16/wpa2-krack-2/ (дата обращения 31.03.2018).

5. Антивирусная правДА! Жёлтый уровень безопасности [электронный ресурс]. URL:https://www.drweb.ru/pravda/issue/?number=397 (дата обращения 02.04.2018).

6. Васильева И.Н. Управление информационной безопасностью. Учебное пособие. СПб.: Изд-во СПбГЭУ. 2014. - 172с.

7. Троянец в GooglePlay [электронный ресурс]. URL:https://news.drweb.ru/show/review/?lng=kk&i=11505#googleplay (дата обращения 31.03.2018).

8. Чернокнижный Г.М., Боховко А.Г. Подход к разработке комплексной процедуры аутентификации пользователей информационных систем // Межд. науч. конф. Евразийского Научного Объединения. «Актуальные вопросы развития науки в мире» - М., апрель 2015. - С.56-57.

9. Анализ проблем парольной защиты в российских компаниях [электронный ресурс]. URL:http://www.securitylab.ru/analytics/381943.php (дата обращения 29.03.2018).

Abstract. *The paper deals with information threats to users arising from the use of mobile devices, in particular: threats related to the theft of personal data; threats to the integrity of data; threats related to the unauthorized use of user-owned devices and violation of their work. The article describes a critical vulnerability in the WPA2 Protocol, which is used to protect transmitted data in Wi-Fi networks. The statistics of used passwords are given, insufficient attention to strong passwords is noted. The necessary measures are proposed to improve the security of personal data of mobile users: enhanced password authentication, biometric and two-factor authentication, cryptographic protection, backup.*

Key words: *threat, security, personal data, password, authentication, cryptography, antivirus.*

References:

1. How personal data can be used for fraud with mobile operators [electronic resource]. URL:http://www.securitylab.ru/blog/company/securityinform/153190.php (accessed 30.03.2018).

2. Gnidenko I. G., Merdina O. D. Methods of software protection against unauthorized access// international scientific and practical conference "Prospects of development of science and education". SB.science.Tr.- Moscow: AR-consult, 2013. - S. 110-115.

3. How to take loans on someone else's passport [electronic resource]. URL:http://www.securitylab.ru/blog/company/securityinform/152810.php (31.03.2018).

4. Detailed information about WPA2 problems has been published [electronic resource]. URL:https://xakep.EN/2017/10/16/wpa2-krack-2/ (accessed 31.03.2018).

5. Antivirus truth! Yellow security level [electronic resource]. URL:https://www.drweb.ru/pravda/issue/?number=397 (accessed 02.04.2018).

6. Vassilyeva I. N. Information security management. Textbook.SPb.: Publishing house of St. Petersburg state economic University. 2014. - 172C.

7. The Trojan in Google play [electronic resource].

URL: https: / / news.drweb.EN/show/review/?lng=kk & I=11505#googleplay (accessed 31.03.2018).

8. Chernoknizhnyi G. M., Bokhovko A. G. Approach to the development of a comprehensive authentication procedures of users of information systems // Intern. science. Conf. Eurasian Scientific Delicious. "Topical issues of development of science in the world" - M., April 2015. - Pages 56-57.

9. Analysis of password protection problems in Russian companies [electronic resource]. URL:http://www.securitylab.ru/analytics/381943.php (accessed 29.03.2018).

Статья отправлена: 06.04.2018 г.

© Чернокнижный Г.М.