Глава 3

Пароли, пароли, пароли...

В этой главе мы поговорим о паролях — как правильно с ними обращаться, где хранить и зачем их нужно регулярно менять. Узнаем, какие пароли надежны, а какие нет и почему. Научимся придумывать и запоминать надежные пароли.

Театр начинается с вешалки, а безопасность в компьютерных системах — с пароля[1]. Приходя в театр, вы сдаете в гардероб только одно пальто и получаете один номерок, за утерю которого администрация вам грозит штрафом. А современному пользователю компьютерными системами приходится хранить как минимум несколько десятков паролей, и потерять их проще простого. Если каждый пароль представить театральным номерком, их наберется целая куча — ни в карман положить, ни в руках удержать. Осталось только нанизать их на веревочку и повесить на шею.

Хотя пароли — это всего лишь набор символов, и они не будут бряцать у вас на шее или оттопыривать карман, с ними придет другая проблема — их необходимо помнить. Поэтому многие люди, чтобы не напрягать память, выбирают очень простые комбинации в качестве секретного ключа и начинают применять один и тот же пароль во всех используемых системах.

> *Корпорация SplashData регулярно публикует список 100 самых ненадежных паролей года, и уже несколько лет подряд первое место занимает пароль «123456». Его используют около 17% пользователей. На втором месте — пароль «password», да и другие популярные пароли ненамного сложнее.*

Для защиты телефона часто используется ПИН-код[2], состоящий из четырех цифр, — это тоже пароль. Увы, и здесь пользователи

---

1 *Пароль (фр. parole — слово) — условное слово или набор символов, предназначенный для подтверждения личности или полномочий. Для входа в разные компьютерные системы используется комбинация — имя пользователя (логин) и пароль.*

2 *ПИН — персональный идентификационный номер (PIN — Personal Identification Number). Чаще всего это — комбинация из четырех цифр, которая представляет собой пароль для доступа к устройству или банковской карте.*

не блещут фантазией, склоняясь в пользу примитивных вариантов. Недавно отдел исследований киберугроз и уязвимостей компании Splunk опубликовал список наиболее часто используемых ПИН-кодов, который выглядит следующим образом: 1234, 1111, 0000, 1212, 7777, 1004, 2000, 4444, 2222, 6969, 9999, 3333, 5555, 6666, 1122, 1313, 8888, 4321, 2001, 1010.

С его помощью можно взломать 26% всех смартфонов.

Не лучше обстоит дело и с графическими ключами Android Lock Pattern (ALP). ALP может содержать от четырех до девяти узлов, что суммарно дает 389,112 возможных комбинаций. Также, как в случае с обычными паролями, число комбинаций возрастает экспоненциально вместе с длиной графического ключа. И точно также люди чаще всего выбирают самые примитивные варианты, которые им проще запомнить, а хакерам — проще подобрать.

Норвежская исследовательница Марте Лёге (Marte Løge) проанализировала относительно небольшую базу из 4000 ключей ALP и получила весьма интересные результаты:

- *44% ALP начинаются из верхнего левого узла;*
- *77% начинаются в одном из четырех углов экрана;*
- *5 — среднее число задействованных в графическом пароле узлов, то есть взломщику придется перебрать менее 8000 комбинаций;*
- *во многих случаях графический пароль состоит из 4 узлов, а это уже менее 1624 комбинаций;*

- *чаще всего ALP вводят слева направо и сверху вниз, что тоже значительно облегчает подбор.*

Более 10% полученных Лёге паролей оказались обычным буквами, которые пользователи чертили на экране. Хуже того — почти всегда выяснялось, что это не просто буква, но первая буква имени опрошенного, его супруга или супруги, ребенка и так далее.

Как сделать графический пароль более сложным? Во-первых, в графическом ключе стоит использовать большее количество узлов. Во-вторых, стоит добавить пересечений. Они усложняют хакерам подбор комбинации и могут запутать злоумышленника, если тот решит подсмотреть пароль через плечо жертвы. В-третьих, стоит отключить опцию «показывать паттерн» в настройках безопасности Android: если линии между точками не будут отображаться на экране, подсмотреть ваш пароль станет еще сложнее[1].

Если ваш графический пароль подсмотрит случайный попутчик в метро, это, по большому счету, не страшно. Ведь чтобы воспользоваться увиденным, наблюдательному попутчику еще нужно украсть у вас телефон. Другое дело, когда секретным «узором» завладевает человек, потенциально имеющий доступ к телефону жертвы, — например, кто-то из одноклассников вашего ребенка. Узнав пароль, он может от имени владельца телефона написать что-то в соцсети — оскорбить, поссорить, выставить в неприятном свете или даже опубликовать нечто противозаконное. Потом будет крайне трудно доказать, что это сделал не ваш ребенок.

---

1 *Графические ключи так же предсказуемы, как пароли «123456» и «password» // Журнал «Хакер», 21 августа 2015.*

То, с чем не справится человек, легко сделает искусственный интеллект: он проанализирует ваши движения и распознает пароль.

К сожалению, даже сложный графический пароль не всегда способен остановить злоумышленника. То, с чем не справится человек, легко сделает искусственный интеллект: он проанализирует ваши движения и распознает пароль. Пока такие исследования проводятся только в лабораториях университетов, но завтра хакерские инструменты могут появиться в открытом доступе.

> *Группа исследователей из Университета Ланкастера, Университета Бата и Северо-Западного университета Китая разработала программное обеспечение, способное расшифровать ваши движения пальцем по экрану с потрясающей точностью. В ходе тестирования исследователи смогли взломать 95% графических паролей Android за пять попыток — до того, как операционная система заблокировала дальнейшие действия.*
>
> *Все, что нужно было сделать команде исследователей, это снять «скрытой камерой», как пользователь разблокировал свой телефон. Причем для этого экспериментаторам не понадобилась какая-то спецтехника — стандартной камеры смартфона оказалось более чем достаточно.*
>
> *Как заявили в Google, визуальное хакерство стало одной из причин, согласно которой в Android была добавлена функция SmartLock, «снижающая частоту, с которой пользователям необходимо вводить свой ПИН-код / пароль / графический шаблон, и поэтому затрудняющая проведение подобных атак»[1].*

1 *Your Android Pattern Lock Could Be Incredibly Easy To Crack // Forbes, 23 января 2017.*

Эти и другие исследования показывают, что пользователи крайне беспечно относятся к защите своей информации, даже зная, что она представляет значительную ценность. А беспечность, вошедшая в привычку, многократно повышает ваши риски. Именно поэтому важно с детства воспитывать серьезное отношение к паролям. Это — один из важнейших элементов цифровой гигиены.

Как работает пароль?

Древние римляне изобрели бетон, водопровод, канализацию, центральное отопление, газеты, римское право и много других полезных для цивилизации вещей. Пароли — тоже их изобретение. Историк Полибий, живший во II веке до нашей эры, так описывает применение паролей:

> *«Вот каким образом они обеспечивают безопасное прохождение ночью. Из десяти манипул, расположенных в нижней части улицы, командир выбирает одного солдата, который освобождается от несения караульной службы. Этот солдат каждую ночь приходит к трибуну и получает от него пароль — деревянную табличку со словом. Сначала солдат показывает пароль своему командиру, а потом идет с табличкой к следующему, который, в свою очередь, передает табличку другому».*

Принцип действия пароля не изменился до наших дней. Нужно выбирать кодовое слово и по секрету передать тому, кто охраняет доступ к ресурсу, будь то крепостные ворота, облачное хранилище фотографий, социальная сеть или что-то еще. Потом часовой

(или программа) спрашивает всякого вновь пришедшего, знает ли он пароль. Если ответ правильный, то пропускает его, если нет, то возможны варианты. Вражеского лазутчика попытаются поймать или застрелить, обычному же пользователю просто покажут на экране окно с надписью «Доступ запрещен», а после нескольких неудачных попыток заблокируют вход в систему. Это не смертельно, но обидно и зачастую хлопотно. Если речь идет, например, об интернет-банке, то вам, вероятно, придется идти с паспортом в офис и доказывать, что именно вы владелец денежных средств, просто забыли пароль.

> *«Железным» аналогом пароля можно считать кодовые замки, которые используются в самых разных устройствах — от банковских сейфов до вокзальных камер хранения и противоугонных тросов для велосипедов.*

До широкого распространения компьютеров большинство секретов, в том числе государственной важности, охранялось при помощи хитроумных механических устройств, потому что все документы были бумажными, и скрыть их от посторонних глаз можно было, лишь положив в сейф. Но даже зная, насколько опасной может быть утечка информации, люди порой проявляли удивительную беспечность в отношении кодов своих замков — тех же паролей. В этом смысле весьма показательна история, рассказанная одним из самых известных физиков XX века, лауреатом Нобелевской премии Ричардом Фейнманом.

Помимо прочего, он любил, как бы сейчас сказали, троллить своих коллег и начальников, в том числе и по вопросам безопасности. Во время работы на Манхэттенском проекте в Лос-Аламосе у Фейнмана появилось два увлечения: игра на барабанах

и вскрытие замков. Для начала он научился открывать обычные висячие замки с трехцилиндровыми механизмами, которые использовались в шкафах с секретными документами. Вот как он это описывал в своей книге «Вы, конечно, шутите, мистер Фейнман»:

> *«Чтобы продемонстрировать никчемность этих замков, всякий раз, когда мне нужен был чей-нибудь отчет, а хозяина отчета не оказывалось на месте, я просто заходил в его кабинет, открывал шкаф и брал нужную бумагу. Закончив с ней работать, я отдавал ее хозяину со словами: «Спасибо за твой отчет!». В ответ я слышал:*
> *— А где ты его взял?*
> *— У тебя в шкафу.*
> *— Но я его запер!*
> *— Знаю, что ты его запер. Но замки — барахло!»*
> *Потом в Лос-Аламосе появились шкафы с кодовыми замками: чтобы открыть такой замок, необходимо было знать комбинацию цифр. Эти шкафы стали вызовом для любознательности Фейнмана. Чтобы изучить, как работает кодовый замок, он разобрал один из них в своем кабинете. Но это не помогло. Тогда он купил несколько книжек известных взломщиков, чтобы ознакомиться с «лучшими практиками». Но и там не нашел ответа. В итоге Фейнман разработал собственный метод. Однажды, стоя возле шкафа с открытым замком, он заметил: если аккуратно поворачивать лимб, пока запирающий стержень не перестанет возвращаться в исходное положение, то можно узнать последнее число в комбинации. Этот же прием в чуть усложненном виде позволил ему узнать и второе число. А первое оставалось подобрать простым перебором при закрытом замке.*

Затем Фейнман использовал сочетание методов социальной инженерии со своими техническими навыками (именно так и делают современные хакеры):

«Я практиковался и практиковался до тех пор, пока не достиг той степени совершенства, при которой мог подобрать последние два числа на открытом замке, почти не глядя на лимб. И тогда я стал проделывать такую штуку: зайдя к коллеге в кабинет для обсуждения какой-нибудь физической задачи, я прислонялся к открытому шкафу и как бы в забывчивости крутил его лимб туда-сюда, как это делает человек, рассеянно играющий ключами во время разговора. Иногда я не смотрел на стержень, а просто клал на него палец — чтобы знать, когда он пойдет вверх. Таким способом я выяснил последние два числа на нескольких сейфах. Вернувшись в свой кабинет, я записывал пары последних чисел на бумажке, которую хранил в замке своего сейфа. Чтобы достать бумажку, я каждый раз разбирал свой замок — это место я считал самым надежным».

Фейнман пару раз продемонстрировал свои удивительные способности по открыванию секретных замков, но как настоящий фокусник хранил свой метод в секрете. После этого его стали звать на помощь, когда срочно требовалось открыть шкаф, хозяин которого был в отъезде. Если это был «неизученный» шкаф, Фейнман отказывался. А если из числа попавших в «разработку», то шел в свой кабинет якобы за инструментами, смотрел в шпаргалку, а дальше оставалось только перебрать двадцать первых чисел — и вуаля, дело сделано! Люди думали, что он открывает хитрые замки без всякой предварительной информации, и Фейнман старался поддерживать эту легенду.

Многие мамы нередко удивляются, как их дети умудряются подобрать пароль к телефону или компьютеру. Точно также, как мистер Фейнман, они очень наблюдательны, очень мотивированы и у них есть куча времени, чтобы заниматься перебором вариантов. Вот один из детских лайфхаков (рассказ мамы):

> *«Мои сыновья начисто вытирали экран айпада. Потом подходили ко мне и говорили, что им срочно нужно что-то сделать — и для этого я должна разблокировать айпад. А после того, как я его разблокирую, они смотрели на оставленные мною отпечатки пальцев и быстро вычисляли простой пароль, составленный из цифр. С более сложным паролем им пришлось повозиться, ведь по отпечаткам пальцев на экране нельзя определить порядок символов. Но они стали подбирать пароль по смыслу, и у них снова получилось».*

Что тут скажешь? Молодцы! Кстати, таким же образом по отпечаткам на клавиатуре Николас Кейдж добыл пароль к секретному компьютеру в «Сокровищах нации».

Зная о склонности пользователей к беспечности, разработчики стали устанавливать более высокие требования к паролям, чтобы заставить людей заботиться о безопасности. Сегодня стандартом де-факто стало требование, чтобы длина пароля была не менее восьми символов, и чтобы пароль обязательно включал заглавные и строчные буквы, цифры и специальные символы (#, $, %, @, &, ! и другие). Чуть позже мы узнаем, чем это обусловлено.

Человек не в состоянии запомнить сложные комбинации и вынужден свои пароли где-то хранить.

Но тут другая беда — человек не в состоянии запомнить такие сложные комбинации и вынужден свои пароли где-то хранить. Чаще всего пароли оставляют в текстовом файле на рабочем столе компьютера или в заметках в телефоне, откуда их и похищают злоумышленники. Некоторые выбирают варианты еще легче: например, используют один и тот же пароль ко всем сервисам, записывают его на бумажке и прикрепляют на видном месте возле компьютера. А потом делают селфи и выкладывают фото в какой-нибудь соцсети. Нужно ли удивляться, что через некоторое время их данные оказываются похищенными?

Нолан Сорренто, главный злодей в фильме Стивена Спилберга «Первому игроку приготовиться», тоже хранил свой пароль записанным на бумажке, которая была приклеена к боковой панели его крутейшей игровой системы. И когда он вызвал к себе в кабинет Уэйда Уоттса в образе его аватара Парсифаля, чтобы попытаться его уговорить работать на корпорацию IOI, тот, естественно, увидел и запомнил этот пароль, благодаря чему Уэйд и его друзья смогли проникнуть в систему Нолана и заставить освободить Саманту.

«— Вы дистанционно взломали его машину?
— У него стационарная точка. Найти просто, хакнуть тяжело.
— Правда, этот тупица хранил там же записку с паролем.»

Никогда не делайте так, как Нолан Сорренто! Если бы не эта его оплошность, пасхантерам[1] было бы гораздо труднее победить.

---

1 *Пасхантер (англ. Gunter) — охотник за «пасхалками», пользователь игры «ОАЗИС», который ищет Пасхальное яйцо Холлидея, создателя игры. Нашедший его получит полный контроль над виртуальной реальностью. («Первому игроку приготовиться»).*

Два ключа лучше, чем один, или Двухфакторная аутентификация

Наверное, у многих на двери в квартиру стоят два замка — для большей надежности. Точно также и в компьютерных системах, чтобы впустить пользователя, часто, кроме пароля, используется еще и второй параметр.

Второй пароль? Ни в коем случае. Нужен другой, независимый канал, по которому можно подтвердить, что вы это вы.

Второй пароль? Нет, ни в коем случае. Если злоумышленники как-то узнали один пароль, возможно, они заполучили всю базу или смогли внедриться в систему и перехватывают информацию. Или кто-то украл ваш ноутбук вместе со всеми паролями. В таких случаях специалисты говорят, что канал скомпрометирован.

Поэтому нужен другой, независимый канал, по которому можно подтвердить, что вы это вы. Эти каналы должны быть принципиально разными. Парольная защита основывается на знании ключа. В принципе, знанием может обладать кто угодно — тот, кто украл или получил пароль. Тогда в игру вступает второй фактор, который основан на владении чем-либо — чаще всего телефоном или USB-ключом. Конечно, эту вещь тоже можно украсть, но маловероятно, что одновременно с паролем.

Обычно в роли второго канала используется SMS — вам на телефон приходит код, который надо ввести в специальное поле для подтверждения входа в систему или совершения каких-то действий. Обычно, подтверждение нужно, чтобы перевести деньги или изменить какие-то важные данные.

Увы, и SMS могут перехватить. Шпионские приложения на Android умеют принимать SMS-сообщения незаметно для владельца телефона — так, что на экране не появится никаких уведомлений и не будет звукового сигнала, а потом быстренько передают полученный код жулику, который уже ввел ваш пароль на своем компьютере. Технически возможен перехват SMS и без установки шпионских программ. Это могут делать спецслужбы или коррумпированные сотрудники оператора сотовой связи — подробнее мы поговорим об этом в главе, посвященной мобильным телефонам. А пока можно остановиться на том, что в целом SMS-канал считается достаточно надежным, если вы не устанавливаете разные «левые» программы из непроверенных источников и не даете свой телефон в руки посторонним.

Непосредственно для входа в систему два ключа используют редко — мы ведь и квартиру не каждый раз закрываем на оба замка, это было бы неудобно. Но не помешает удостовериться, что входит настоящий пользователь, а не жулик, когда система замечает попытку входа с нового компьютера или телефона, — в этом случае задействуется двойная проверка.

Дополнительно вам на почту придет сообщение о входе с неизвестного устройства. Если вам подарили новый телефон, и вы с него зашли в свой аккаунт, то это сообщение можно просто принять к сведению. А если действительно кто-то другой пытался вас взломать, то вы узнаете об этом и сможете быстро поменять пароль. Так что не забывайте проверять вашу электронную почту, даже если не пользуетесь ею регулярно.

Кстати, поскольку пока большинство сервисов для подтверждения входа или важных действий полагается именно на SMS, не держите

телефон в одной сумке с ноутбуком — это будет слишком щедрым подарком ворам.

Не держите телефон в одной сумке с ноутбуком — это будет слишком щедрым подарком ворам.

Главный плюс подтверждения входа при помощи SMS — простота. Каждый, у кого есть мобильный телефон, с этим справится. И при этом код подтверждения всегда будет разный, а это безопаснее, чем постоянный пароль. Однако, есть и минусы — ваш телефон всегда должен быть заряжен, оплачен и находиться в зоне действия сети, иначе SMS-ка к вам не придет. К тому же для многих смартфон стал сегодня основным или даже единственным средством доступа в интернет, поэтому фактически происходит слияние двух факторов в один — если кто-то завладел вашим телефоном, он с него войдет в ваш аккаунт и на него же получит код. Так что плюс оборачивается минусом.

Чем мы располагаем, кроме SMS, в качестве второго фактора? Еще можно использовать электронную почту — это следующий по популярности канал. Вам точно также приходит на почту код, который надо ввести для подтверждения ваших прав. Более редко встречается использование телефонного звонка, когда код сообщают вам голосом. Почти совсем ушло из практики использование заранее напечатанных резервных кодов и специальных генераторов ключей. USB-ключи все еще используются банками, особенно как носитель электронной подписи, но это не массовое явление.

В дополнение к паролю часто используется капча (CAPTCHA, Completely Automatic Public Turing Test to Tell Computers and Humans Apart) — механизм, с помощью которого веб-сайт отличает людей от ботов (программ-роботов), заставляя их проходить обратный

тест Тьюринга. Обычно пользователю предлагается ввести в поле формы выражение из цифр и букв разного регистра, изображенное на автоматически сгенерированной картинке, или определить, где на показанной картинке находятся автомобили, мосты, дорожные знаки или еще что-нибудь. Предполагается, что тупая программа с такой задачей не справится, а человек — запросто.

Капча не только не допускает массовой регистрации ботов в соцсетях или на других сервисах, но еще препятствует автоматизированным попыткам взломать пароль путем перебора вариантов — ведь в таком случае программа-взломщик должна еще распознать изображение и правильно ответить на вопрос. Теоретически это возможно, однако всегда нужно взвешивать, стоит ли овчинка выделки. Чаще всего нет, поэтому механизм капчи действительно помогает повысить уровень защищенности системы.

Усы, лапы и хвост — вот мои документы!

Кот Матроскин заявлял совершено справедливо про усы, лапы и хвост, потому что для идентификации пользователя можно использовать какое-либо из присущих ему свойств: отпечатки пальцев, лицо, рисунок радужной оболочки или сетчатки глаза, снимок кровеносных сосудов в руке, голос, походку, сердечный ритм, ДНК в конце концов. То есть биометрические данные, которые по своей природе уникальны и однозначно связаны с человеком.

> *Казалось бы, вот оно, решение! Наукой доказано, что у людей не бывает одинаковых отпечатков пальцев — даже у близнецов. Вот вам и универсальный пароль!*

Любители детективов и фантастики на это лишь усмехнутся и расскажут кучу историй, как преступникам, или, наоборот, хорошим парням удавалось использовать чужие отпечатки, чтобы проникнуть на секретный объект или взломать систему. В кино такие вещи часто излишне драматизируют — на самом деле необязательно воображать всякие ужасы вроде отрубания пальцев или вырывания глаз. В реальной жизни есть способы более гуманные и не менее эффективные, хотя и такой риск исключать нельзя, поскольку бандиты могут оказаться технически неграмотными и поступить, как им кажется, проще.

На что годится мертвый палец?

Вопрос далеко не праздный, им интересуются как преступники, так и полицейские. Ответ зависит от типа биометрического датчика и конкретного устройства. Хотя многие устройства анализируют биологическое состояние пальца (например, при помощи инфракрасного датчика), следует признать, что такая возможность все-таки существует. Бывало, когда полицейские пользовались этим свойством для разблокировки айфонов погибших террористов или людей, умерших от передозировки наркотиков, чтобы выйти на след дилера, но с переменным успехом. А в 2005 году был случай, когда малазийские угонщики автомобилей отрезали палец владельца Mercedes-Benz, чтобы обойти высокотехнологичную систему безопасности.

Если производителям биометрических устройств не удастся исключить такую возможность, это может стать источником серьезной опасности получения увечий

для владельцев потенциально привлекательных активов, использование или доступ к которым заблокированы биометрической защитой[1].

Однако чаще пальцы все-таки подделывают: изготовление желатиновых или силиконовых слепков не является особенно сложной задачей для специалиста. А добыть оригинальный отпечаток даже очень высокопоставленного лица не составляет большого труда, что продемонстрировали активисты из Chaos Computer Club, опубликовавшие в своем журнале «пальчики» министра внутренних дел Германии Вольфганга Шойбле, которые они сняли со стакана, использованного им во время публичного мероприятия. Фокус был проделан в 2008 году, чтобы продемонстрировать фундаментальные риски биометрических систем, но тем не менее технология получила широкое распространение. Более того, обязательное применение дактилоскопии в государственных системах, планируемое сегодня во многих странах, может привести к дискриминации некоторых людей, и это тоже надо учитывать.

Люди без отпечатков пальцев

Существуют редкие генетические мутации, при которых у человека может не быть отпечатков пальцев вообще. Люди с синдромом Негели или дерматопатией пигментной ретикулярной формы, например, могут не иметь отпечатков пальцев. Оба заболевания являются формами эктодермальной дисплазии, и отсутствие отпечатков в этом случае — всего лишь самый безобидный из симптомов.

---

1 *Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации. // Блог компании «ИНТЕМС»*

Отпечатки пальцев могут также исчезнуть в результате побочных эффектов от приема некоторых лекарственных препаратов, например, капецитабина (выпускается под брендом Кселода), противоракового препарата, применение которого (задокументировано) приводило к исчезновению отпечатков пальцев.

Еще более интересным случаем является адерматоглифия. Единственным проявлением этой генетической мутации является отсутствие папиллярного рисунка на всех пальцах, ладонях рук и подошвах ног. У этой мутации нет никаких сопутствующих проявлений, выраженных в нарушении нормальной жизнедеятельности или снижении продолжительности жизни. То есть адерматоглифия не является заболеванием. Люди, обладающие этой особенностью, могут иметь сложности в общении с силовыми структурами и получении виз. Но если они встанут на преступный путь, то смогут обходиться без перчаток.

А, в общем, и нечаянный порез может на некоторое время лишить вас возможности разблокировать свой телефон. Так что слишком полагаться на эту технологию не стоит — хотя после заживления раны папиллярный рисунок обычно восстанавливается[1].

Никто не спорит, что очень удобно разблокировать пальцем телефон или ноутбук, открыть дверь в квартиру, получить деньги в банкомате, расплатиться за покупку в магазине или завести дви-

1 *Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации. // Блог компании «ИНТЕМС»*

гатель машины. Но всегда, когда вы слышите об удобстве в связи с безопасностью, стоит насторожиться. Действительно ли метод идентификации человека по отпечатку пальца безопасен? Что будет, если кто-то украдет эту информацию?

Действительно ли метод идентификации человека по отпечатку пальца безопасен? Что будет, если кто-то украдет эту информацию?

Чтобы разобраться, давайте заглянем на технический уровень и посмотрим, как это работает. На самом деле телефон не может «видеть» ваш палец — с датчика он получает не снимок всего отпечатка, а некий соответствующий ему цифровой код, который сравнивает с хранящимся в памяти. Если коды совпадают, значит, доступ разрешен. То есть достаточно украсть эту информацию, чтобы попытаться войти в систему под вашим именем.

В этом смысле пароли имеют преимущество перед биометрией, потому что могут быть заменены на новые даже при подозрении на утечку, а палец или глаз так легко не поменяешь. Помните, чего это стоило герою Тома Круза в фильме «Особое мнение»? Собственно, здесь и пересекаются основное преимущество и главный недостаток всех биометрических систем — высокая точность идентификации человека вызывает большие сложности при компрометации системы.

Поэтому защите биометрических систем приходится уделять повышенное внимание. Во-первых, практически в обязательном порядке применять шифрование данных. Во-вторых, использовать так называемый метод «отменяемой биометрии», суть которого состоит в том, что в биометрический признак (отпечаток пальца, например) вносится повторяемое искажение — как будто в системе хранится ваше изображение, полученное при помощи кривого зеркала. В слу-

чае утечки данных вам достаточно изменить кривизну зеркала, чтобы сгенерировать новый ключ вместо скомпрометированного.

Есть и еще одна проблема: при использовании биометрии всегда существует вероятность ложного пропуска и ложного отказа. В первом случае это значит, что доступ будет открыт случайному человеку, чьи биометрические данные просто очень похожи на ваши; во втором — законный владелец данных не сможет войти в систему, потому что она его не узнала.

Качественные характеристики биометрических систем[1]

Метод биометрической идентификации	Коэффициент пропуска	Коэффициент ложного отказа
Отпечаток пальца	0,001%	0,6%
Распознавание лица 2D	0,1%	2,5%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Дело в том, что сканеры отпечатков пальцев и другие биометрические датчики, особенно встроенные в потребительские приборы, несо-

1 *Биометрия от «А» до «Я» полное руководство биометрической идентификации и аутентификации. // Блог компании «ИНТЕМС»*

вершенны — это и является источником ошибок. Кроме случайной ошибки существует и вероятность срабатывания системы на «муляж». Но по мере развития технологий качество датчиков повышается, и примитивные методы обмана, такие как «желатиновые пальцы», перестают работать. В свою очередь, исследователи обнаруживают все новые уязвимости таких систем.

Группа исследователей из университета Нью-Йорка и Мичиганского университета разработала способ взломать практически любой гаджет, защищенный технологией сканирования отпечатков пальцев. При этом отпечатки владельца для этого не нужны вовсе! Специалисты создали, если можно так выразиться, изображение «универсального отпечатка пальца». В этом рисунке присутствуют отличительные признаки огромного количества разных отпечатков абсолютно разных людей. Как показали опыты, этого достаточно для того, чтобы обмануть большинство недорогих сканеров, устанавливаемых в мобильных телефонах, планшетах, ноутбуках и другой электронике.

Для того чтобы сделать «ключ от всех биометрических замков», ученые взяли за основу базу данных, состоящую из более чем 800 реальных отпечатков. При помощи специального компьютерного алгоритма они были совмещены таким образом, что в итоге получившийся «ключ» имеет схожесть на 26–65% с любым отпечатком, взятым у случайного человека, не находившегося в исходной базе.

Высокотехнологичные сканеры обмануть таким образом вряд ли получится, но вот устройства повседневного пользования — вполне. Дело в том, что сканеры наподобие Touch ID

имеют малую площадь, что не дает им возможности считать весь отпечаток пальца, и сенсор «ориентируется» лишь по фрагменту. Эта уязвимость как раз и была использована учеными. Как говорят сами исследователи, существует очень высокая вероятность того, что за несколько попыток авторизации, которые предоставляет система мобильного телефона, сканер может попасть на похожий участок «универсального отпечатка». Если системе авторизации удастся определить несколько признаков соответствия, она посчитает «универсальный отпечаток» за отпечаток владельца и разблокирует электронное устройство. Во время испытаний удалось успешно обмануть сканер в 15% случаев, что указывает на весьма большую «дыру» в этой системе авторизации[1].

То есть надо признать, что биометрия не обеспечивает 100% защиты от действий злоумышленников. Однако она может существенно снизить риски несанкционированного доступа. Поэтому эксперты советуют защищать одной лишь биометрией только данные, не имеющих особой ценности.

Например, когда нужно сделать так, чтобы ребенок, который взял поиграть родительский гаджет, не мог случайно разослать неуместные фотографии по вашим контактам, совершить покупку в интернет-магазине или перевести средства с банковского счета. Таких неприятностей можно избежать, если установить запуск важных приложений и подтверждение финансовых операций по отпечатку пальца.

---

1 *Создано изображение «универсального отпечатка пальца», способное обмануть большинство сенсоров // Hi-News.ru, 18 апреля 2017.*

Кроме того, биометрия — защита на случай экстренных ситуаций. В Японии после разрушительного землетрясения и цунами в марте 2011 года множество людей лишились не только своих банковских карт, но и документов. Они вынуждены были проходить через долгие и утомительные процедуры идентификации личности, чтобы снять деньги со своих счетов. После этого в стране создали единую биометрическую систему, которая исключает такую проблему в будущем.

Датчик распознавания отпечатка пальца на телефонах компании Apple впервые появился в модели iPhone 5S, представленной в 2013 году, и стал обязательным элементом всех новых устройств. Он позволяет их владельцам производить разблокировку, а также подтверждать покупки в App Store, iTunes и iBooks. Компании Apple удалось не только сделать одно из самых точных биометрических устройств для массового пользователя, но и разработать действительно надежное решение для безопасного хранения идентификационных данных.

Здесь важно сказать, что некой централизованной базы отпечатков не существует в принципе, поэтому никто не может ее взломать и украсть. Все отпечатки хранятся только на самом устройстве в специальной защищенной области Secure Enclave, расположенной непосредственно на процессоре. Точнее говоря, хранятся не сами снимки отпечатков, а их цифровые образы, дополнительно зашифрованные. Эта информация не записывается в резервные копии iTunes и iCloud, серверы компании или любой другой источник.

Прежде чем начать использовать Touch ID, нужно создать резервный пароль в качестве дополнительной защиты. Он понадобится для разблокировки телефона в случаях, когда:

- *устройство было выключено или перезагружено;*
- *был добавлен отпечаток еще одного пальца;*
- *устройство получило команду удаленной блокировки через Find My iPhone;*
- *произошло пять безуспешных попыток разблокирования подряд с помощью отпечатка;*
- *устройство ни разу не было разблокировано в течение двух суток;*
- *прошло более шести суток с момента последнего ввода кода блокировки, а само устройство не было разблокировано датчиком Touch ID в течение восьми часов.*

Слив ключа, впрочем, не означает, что теперь смартфон не может обеспечивать безопасность: важные данные, хранящиеся в Secure Enclave, защищены другими ключами, которые все еще не найдены и, скорее всего, не будут. Все, что можно сделать, это расшифровать и изучить секретную систему Apple, которая работает на криптографическом процессоре. Получить доступ к данным, которые там хранятся, таким образом, нельзя.

Иначе говоря, технология Touch ID пока остается устойчивой к взлому. Другое дело, что ее можно обмануть, используя разные приемы.

Осторожно, мошенники!

В 2018 году появились сообщения о мошеннических приложениях в AppStore, которые использовали технологию Touch ID. Они маскировались под приложения якобы для отслеживания здоровья, которые назывались Heart Rate Monitor, Fitness Balanceapp и Calories Trackerapp (сейчас эти приложения уже удалены).

Их работа была основана не на вредоносном ПО, а на хорошем понимании человеческого поведения. Люди привыкли использовать Touch ID не только для разблокировки телефона, поэтому часто даже не задумываются о том, когда приложение просит их приложить палец к датчику. После того, как вы отсканируете отпечаток пальца, такое мошенническое приложение быстро показывает всплывающее окно с внутренней покупкой и списывает со счета от $90 до $120, одновременно уменьшая яркость экрана, чтобы это окно было сложно увидеть[1].

Лицо вместо пальца

С выходом смартфона iPhone X в 2017 году Apple заменила дактилоскопический датчик Touch ID на систему идентификации пользователей по лицам Face ID, которая использует набор камер True Depth. По сути, это комплекс из двух датчиков — 7-мегапиксельной фронтальной камеры и инфракрасной камеры — и двух

1 *Берегитесь хитроумного мошенничества с Touch ID, проникшего в App Store // Habr.com, 8 декабря 2018.*

инфракрасных осветителей — «проектора точек» (всего точек 30 тысяч) и «заполняющего» излучателя (свет от обоих невидим).

С помощью этой системы iPhone сканирует лицо владельца в формате 3D, затем обрабатывает изображение специальной нейросетью и создает цифровой отпечаток, который используется для разблокировки. Точно также, как было и с Touch ID, биометрические данные хранятся в специальной защищенной области на самом телефоне в зашифрованном виде и никуда не передаются.

Хакеры всех мастей тут же бросились ломать новую игрушку и кое-каких успехов достигли. Буквально через несколько дней после начала продаж телефонов с Face ID, в ноябре 2017 года вьетнамская компания Bkav сообщила, что им удалось обмануть систему с помощью сложной маски, сделанной из комбинации 2D и 3D деталей, но повозиться им пришлось изрядно, и повторить такой трюк будет чрезвычайно сложно[1].

В августе 2019 года на конференции хакеров Black Hat в Лас-Вегасе показали еще один изощренный способ «ломануть» Face ID и получить доступ к iPhone спящего или мертвого человека. Как оказалось, если пользователь носит очки, то система игнорирует область вокруг глаз, воспринимая ее как пустое пространство

1 *Vietnamese Firm Bkav Claims to Have Beaten Apple Face ID With an Elaborate Mask // GIZMODO.com, 11 декабря 2017.*

с белой точкой блика от подсветки посередине черного зрачка, считая это достаточным, чтобы определить, что человек жив и бодрствует. Специалисты из Tencent Security Xuanwu Lab взяли обычные очки, наклеили на них по куску черной ленты с небольшой белой точкой в центре, надели их на «спящего» пользователя и успешно разблокировали его телефон[1].

Однако оснований для паники пока нет. Все эти сценарии трудно воспроизвести в жизни. Сама Apple заявляет, что ее система распознавания лиц предназначена для удобства, а не абсолютной безопасности. Она менее уязвима, чем Touch ID, и в целом работает. Говорят, что Touch ID может вернуться в усовершенствованном виде полноэкранного датчика, Apple уже оформила соответствующий патент. Но подтверждения этой информации до сих пор нет.

- *Использовать вместо пароля лицо или отпечаток пальца вполне можно.*

В общем, использовать вместо пароля лицо или отпечаток пальца вполне можно. Кое-какие способы их обхода существуют, но реальной опасности для обычных пользователей они не представляют. Остальные биометрические технологии еще не созрели для массового применения, и в жизни вы можете встретиться с ними реже, чем в кино. Однако пройдет совсем немного времени, и то, что вчера было фантастикой, станет нашим повседневным опытом, как стала им, например, идентификация человека по ДНК.

---

1 *Biometric Authentication Under Threat: Liveness Detection Hacking // Конференция «Black Hat USA», 3-8 августа 2019.*

«Мой пылесос шпионит за мной» — о паролях по умолчанию на разных устройствах

Нет, это не исповедь параноика на приеме у психиатра. Это вполне реалистичный сценарий, который реализуется, если вы станете без должного внимания впускать в свой дом разнообразные умные устройства, в том числе и бытовые приборы, у которых становится все больше «мозгов».

Сегодня микрокомпьютер может быть встроен во что угодно, хоть в лампочку.

Сегодня микрокомпьютер может быть встроен во что угодно, хоть в лампочку. А если там есть компьютер, значит, на нем есть операционная система, в которой есть администратор, у которого есть пароль на доступ ко всему. Как правило, эти пароли устанавливаются еще на фабрике и потом не меняются, чем часто и пользуются злоумышленники. Как правило, это пользователь «admin» с паролем «admin» — иными словами, кто угодно может зайти в систему и сделать любую пакость.

Итак, давайте проведем небольшую ревизию умных устройств в вашем доме, которые могут иметь пароль по умолчанию.

Прежде всего, это роутер, который обеспечивает подключение к интернету и раздает wi-fi по квартире. Большинство из них так и используется с заводскими настройками. Обычно провайдеры рекомендуют их сменить, но кто читает их рекомендации? Известны и такие случаи, когда производитель, наоборот, рекомендовал

«сохранить установки и настройки по умолчанию». Интернет работает — и отлично! Между тем, это очень серьезная брешь в вашей цифровой крепости, фактически — незапертые входные ворота. Естественно, сначала хакерам придется взломать ваш wi-fi, ведь вы же не настолько наивны, чтобы открыть доступ к своей беспроводной сети без пароля, да?

> *Запаролить роутер, не обладая техническими навыками, непросто. Но это важно сделать! Поспособствует вам в этом множество инструкций, которые легко найти в интернете, указав модель вашего роутера. Или кто-то из знающих людей, которым вы доверяете.*

Если ваш телевизор достаточно новый, то он, скорее всего, тоже оснащен встроенным компьютером, пароль которого также нужно сменить с заводского на собственный. Вы спросите: где тут риск? Зачем злоумышленнику ваш телевизор? Если в телевизоре есть встроенная камера и микрофон, то он может превратиться в шпионское устройство. Кроме того, в памяти телевизора может оказаться много конфиденциальной информации — например, вам же надо оплачивать подписки, а это значит, что в телевизоре могут быть ваши платежные данные — вот уже и улов для хакеров. Посмотрели на большом экране фотографии из отпуска — а среди них оказались и фото паспортов. В общем, к телевизору надо относиться как к настоящему компьютеру и принимать такие же меры безопасности.

К телевизору надо относиться как к настоящему компьютеру и принимать такие же меры безопасности.

Более того, появились умные пылесосы с видеокамерами, которые также подключаются к домашнему wi-fi. Имея возможность

перемещаться по дому, они способны превратиться в настоящих соглядатаев и начать шпионить за вами. Не забудьте и про холодильники, которые сами заказывают продукты, про кондиционеры, отопительные системы, умные розетки, умные лампочки и так далее.

Приборы, которыми можно управлять удаленно, как правило, имеют коды доступа. Заводские настройки всем известны, и если их не поменять перед началом использования, то этим вы очень сильно облегчите задачу взломщикам.

Вот еще одна история про Ричарда Фейнмана, на этот раз о паролях по умолчанию.

> *В послевоенное лето хозяйственники Лос-Аламоса[1] вывозили кое-что из списанного имущества. Среди этих вещей был сейф одного из высокопоставленных сотрудников. Прибыв сюда во время войны, он решил, что шкафы недостаточно надежны для его секретов, и заказал специальный сейф, который с трудом втащили в его кабинет. Все в Лос-Аламосе знали об этом сейфе. Но прежде чем отправить сейф на распродажу, его надо было опорожнить, а сам сотрудник был на Бикини[2]. Кроме него шифра никто не знал.*

---

1 *Лос-Аламосская национальная лаборатория (ЛАНЛ, англ. Los Alamos National Laboratory, LANL, ранее — Site Y, LASL) — одна из шестнадцати национальных лабораторий Министерства энергетики США и одна из двух лабораторий, ведущих в США секретные работы по ядерному оружию. Находится в городе Лос-Аламос, штат Нью-Мексико, США. Управляется службой Triad National Security, LLC. Основана в 1943 году.*

2 *Бикини — атолл в Тихом океане, где проводились испытания ядерного оружия.*

Разумеется, первым делом позвали Фейнмана как известного взломщика. Но кодов от этого сейфа у него не было, к тому же ему было некогда, поэтому он попробовал уговорить секретаршу все-таки позвонить на Бикини и узнать комбинацию чисел. И вот, пока Фейнман ее уговаривал, пришел местный слесарь и запросто открыл знаменитый сейф.

«Этот слесарь гораздо лучший взломщик, чем я», — подумал мистер Фейнман. Он потратил несколько недель, чтобы подружиться со слесарем и расспросить того, как ему удалось открыть сейф.

Ответ оказался ошеломляюще простым:

— Я знаю, что замки приходят с завода, установленными на 25-0-25 или на 50-25-50, — сказал слесарь. — И я подумал: «Чем черт не шутит? Может, этот олух не потрудился сменить комбинацию». Вторая комбинация открыла замок.

Узнав это, Фейнман прошелся по кабинетам своего здания, пробуя две заводские комбинации, и открыл каждый пятый сейф.

Бывает и хуже: в 2004 году из воспоминаний Брюса Блэйра стало известно, что в течение почти двадцати лет коды запуска ядерных ракет США были «00000000» — да-да, восемь нулей! По правде сказать, сначала вообще никаких кодов не было, только в 1962 году президенту Кеннеди пришла в голову мысль, что ядерную войну может начать кто угодно — террористы, захватившие ракетную шахту, диверсанты или просто какой-нибудь полковник по собственной инициативе. Поэтому он приказал оборудовать

все ракеты специальным устройством контроля Permissive Action Link (PAL), которое блокировало систему запуска до введения правильного кода. Система считалась абсолютно надежной, и, наверное, так оно и было, только военные, чтобы не «заморачиваться» на всех пусковых установках, сбросили коды в ноль.

Купив или получив в подарок новую вещь, никогда не оставляйте заводские пароли по умолчанию.

Мораль этой истории такова: купив или получив в подарок новую вещь, никогда — слышите, никогда! — не оставляйте заводские пароли по умолчанию. Точно также поступайте и с прежними паролями, если вещь пришла к вам от другого владельца.

Украсть оптом, ломать поодиночке

Чтобы заполучить пароль, у злоумышленников есть два основных способа: взлом или кража. Например, можно попытаться перехватить легионера, несущего табличку с паролем, и отнять ее — это будет грубый взлом. А можно заслать шпиона, чтобы он втерся к вам доверие, и вы бы сами ему все рассказали — это уже будет кража с помощью социально-психологической инженерии.

Чтобы заполучить пароль, у злоумышленников есть два основных способа: взлом или кража.

Трудно сказать, какой метод эффективнее, ведь, чтобы воспользоваться отнятой у легионера табличкой, враг должен был уметь читать по-латыни, а среди варваров этот навык едва ли был широ-

ко распространен. Но уж читать-то современные хакеры умеют, и если ваш пароль попал к ним в руки, они не преминут пустить его в дело. (Поэтому разработчики стараются их запутать, но об этом чуть ниже.) К тому же взлом всегда оставляет следы, и жертва постарается восстановить защиту. А кража может долгое время оставаться незамеченной.

Взлом всегда оставляет следы. А кража может долгое время оставаться незамеченной.

Надо сказать, что у самого метода защиты при помощи пароля есть две слабые точки. Во-первых, пользователь должен назвать свой пароль при входе в систему, и в этот момент кто-то может попытаться его похитить. Самое простое — подсмотреть из-за вашего плеча, так работают визуальные хакеры. Например, когда вы пользуетесь телефоном в метро. Или это сделает программа-вирус, проникшая в ваш компьютер.

Во-вторых, провайдер должен хранить у себя пароли всех пользователей, а много секретов в одном месте — это настоящее пиршество для хакеров. Поэтому жулики обычно не охотятся за паролями отдельных пользователей, а стараются украсть всю базу целиком. Образно говоря, они предпочитают сначала вынести сейф, чтобы потом спокойно его распилить. Делать это надо предельно тихо и незаметно, иначе операция теряет смысл. Естественно, здесь на первый план выходит человеческий фактор: в любой компании всегда найдется сотрудник, который не откажется подзаработать на сливе информации, и задача преступников состоит только в том, чтобы выйти на него и договориться о цене.

Зная об этом риске, разработчики предпринимают встречные меры, которые призваны если и не остановить преступников, то осложнить

им задачу и дать атакованной структуре время, чтобы восстановить защиту — в том случае, если утечка была обнаружена.

Утечки паролей

В прессе регулярно появляются шокирующие заголовки об утечках миллионов паролей. Просто погуглите, чтобы ощутить масштаб бедствия. О крупнейшей базе украденных е-мейл адресов и паролей сообщил в начале 2019 года известный специалист по безопасности Трой Хант. Он следит за хакерскими форумами и покупает базы данных, выставленные на продажу (иногда эти базы ему присылают бесплатно). Но Хант никогда не видел, чтобы на продажу выставляли такую огромную базу, как нынешняя Коллекция №1 (Collection #1). Гигантский архив содержит 2 692 818 238 записей с адресами электронной почты и паролями.

Кстати, вы можете проверить, есть ли ваш е-мейл и пароль среди украденных хакерами. Для этого зайдите на сайт **https://haveibeenpwned.com/**, который уже несколько лет ведет Трой Хант[1].

Брутфорс — против лома нет приема

Чтобы взломать систему, когда нет никаких догадок насчет пароля, используют метод брутфорс (по-английски "brute

1 *Крупнейший дамп в истории: 2,7 млрд аккаунтов, из них 773 млн уникальных. // Habr.com, 17 января 2019.*

force" — буквально «грубая сила»), основанный на переборе всех возможных значений. Например, если у вас есть чемодан с кодовым замком, имеющим три лимба с цифрами от 0 до 9, то, чтобы его открыть, вам нужно перебрать всего тысячу комбинаций — с этим справится даже ребенок. Для четырех цифр уже потребуется перебрать 10 тысяч комбинаций, для пяти — 100 тысяч и так далее. Или можно увеличить число значений на лимбе, допустим, до 100, и тогда на трех лимбах мы уже имеем 100 * 100 * 100 = 1 000 000 — один миллион комбинаций.

Теперь вы понимаете, почему Фейнман так стремился выведать два числа из трех на замках шкафов с секретными документами. Перебирать вручную миллион комбинаций на механическом замке — задача нереальная, проще такой сейф просверлить. Но если замок электронный и перебор производит компьютер, то миллион вариантов — это пустяк.

> *Чтобы усложнить задачу взломщику, в паролях не только наращивают количество символов в длину, но также используют помимо цифр буквы, что значительно увеличивает число вариантов.*

Судите сами: если бы у нас был такой же трехлимбовый кодовый замок, но вместо цифр на его лимбах были бы буквы латинского алфавита, то число комбинаций было бы 26 * 26 * 26 = 17 576. Это гораздо больше, чем в случае с одними цифрами.

Допустим, что в пароле используются 36 различных символов (латинские буквы одного регистра + цифры), а скорость перебора составляет 100 тысяч паролей в секунду.

Кол-во знаков	Кол-во вариантов	Стойкость	Время перебора
1	36	5 бит	менее секунды
2	1296	10 бит	менее секунды
3	46 656	15 бит	менее секунды
4	1 679 616	21 бит	17 секунд
5	60 466 176	26 бит	10 минут
6	2 176 782 336	31 бит	6 часов
7	78 364 164 096	36 бит	9 дней
8	2,821 109 9x10^{12}	41 бит	11 месяцев
9	1,015 599 5x10^{14}	46 бит	32 года
10	3,656 158 4x10^{15}	52 бита	1 162 года
11	1,316 217 0x10^{17}	58 бит	41 823 года
12	4,738 381 3x10^{18}	62 бита	1 505 615 лет

Мы видим, что пароли длиной до 8 символов включительно, в общем случае, не являются надежными. Для современных компьютеров порог надежности гораздо выше. Так, 64-битный ключ (пароль) перебирается на современном компьютере примерно за два года, но перебор легко может быть распределен между множеством компьютеров, что существенно сократит сроки взлома.

Для повышения стойкости пароля важна даже не столько его длина, сколько разнообразие используемых символов.

Для повышения стойкости пароля важна даже не столько его длина, сколько разнообразие используемых символов. Именно поэтому сервисы, которые действительно заботятся о безопасности своих пользователей, требуют, чтобы пароль обязательно содержал буквы верхнего и нижнего регистра, цифры и специальные знаки.

Интересно, что длинные пароли, состоящие из 12 символов и более, ломаются ничуть не хуже, чем короткие. Дело в том, что для их составления люди используют фразы, состоящие из 3-4 обычных слов — такая задача легко решается с помощью перебора по словарю.

Также наивно будет использовать в качестве пароля русские слова, набранные латиницей. Например, конструкция «**JxtymCkj;ysqGfhjkm**» на самом деле в русской раскладке клавиатуры будет «**ОченьСложныйПароль**», что вскрывается программными средствами в два счета.

В реальных условиях брутфорс-атаке можно противостоять ограничением числа неправильных попыток ввода пароля и последующей блокировкой аккаунта. Например, если вы три раза неправильно ввели пин-код своей кредитной карты, банкомат ее «проглотит» и заблокирует. Точно также может быть заблокирован доступ к соцсети или электронной почте, если кто-то будет пытаться тупо угадать пароль методом перебора. Тем не менее такие атаки имеют место, особенно когда взламывается конкретно чей-то аккаунт.

> *Эффективность брутфорс-атаки прямо пропорциональна уровню беспечности пользователя. Чем надежнее ваш пароль, тем меньше шансов его взломать в лоб.*

Потому что хакер не сидит и не вводит данные вручную, для этого есть специальные утилиты, к которым подключаются словари известных паролей и настраиваются алгоритмы их перебора.

Шифр и хеш — в чем разница?

Сегодня только совсем безалаберные разработчики хранят пароли в открытом виде в базе данных. (Но такие еще встречаются.) И какой бы сложный пароль вы ни придумали, это ничем вам не поможет, если администратор базы данных управляет ей под логином «admin» с паролем «password». Такая база будет взломана с вероятностью 100%, и пароли будут похищены.

Ответственные программисты никогда не хранят пароли в открытом виде. Чтобы защитить своих пользователей, они применяют два метода: шифрование и хеширование. С точки зрения обывателя, разница почти незаметна — вместо вашего любимого пароля «vasya2006» в базе данных окажется какая-то абракадабра, и злоумышленник не сможет вместо вас получить доступ в систему. Но разница есть, и довольно существенная.

Все, что было зашифровано, можно расшифровать, зная секретный ключ.

Все, что было зашифровано, можно расшифровать, зная секретный ключ. И если кто-то добудет этот ключ, ему станут известны все пароли, хранящиеся в базе. А вопрос «Почему бы не купить этот ключ вместе с ворованной базой?» — риторический, как вы понимаете. Если бы можно было обезопасить систему от рисков, связанных с недобросовестным поведением сотрудников, то этот метод считался бы надежным, потому что взломать шифрованный пароль при текущем уровне развития компьютеров практически невозможно — для перебора вариантов потребуется много времени даже по астрономическим масштабам. (Именно по этой причине шла такая битва за передачу ключей шифрования мессенджера

Telegram спецслужбам — если у вас нет секретной лазейки, шифрование обеспечивает очень высокую надежность.)

Алгоритмов шифрования существует множество, и у нас нет цели познакомиться со всеми ними подробно. Одним из наиболее популярных является алгоритм AES — Advanced Encryption Standard, который, в частности, используется для шифрования паролей wi-fi. Этот алгоритм в настоящее время считается достаточно стойким.

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Даже суперкомпьютеру понадобилось бы неисчислимо огромное количество времени, чтобы получить доступ к информации под защитой AES посредством лобовой атаки. Для сравнения: возраст Вселенной — где-то между 13 и 14 миллиардами лет. Даже если предположить, что некий супер-суперкомпьютер мог быть справляться с более старым алгоритмом DES за одну секунду, то на взлом AES у него ушло бы около 149 триллионов лет. Как видите, размера ключа в 128 бит вполне достаточно, хотя совершенно секретная информация все равно шифруется с размером в 256 бит[1].

Однако все имеет обратную сторону. Алгоритмы шифрования математически очень сложны и потому работают медленно, что неудобно при повседневной работе: системе пришлось бы расшиф-

1 *Алгоритм шифрования AES. // Блог* ***OpenGsm.com***

ровывать пароль при каждом входе пользователя, а это вызывало бы заметную задержку. К тому же возникает тема с хранением ключей шифрования, а это отдельная и непростая история.

Поэтому сейчас для хранения паролей почти повсеместно используют хеширование[1]. Если не вдаваться в математические дебри, то хеширование — это алгоритм, который преобразует строку символов любой длины (ваш пароль) в другую строку фиксированной длины, называемую хешем.

> *Хеш обладает двумя свойствами. Во-первых, из него невозможно восстановить исходные данные — иначе говоря, расшифровать хеш нельзя, ключа в принципе не существует. Во-вторых, с очень высокой вероятностью каждому уникальному паролю соответствует уникальный хеш, что и позволяет использовать его вместо самого пароля.*

Тут нужно сделать оговорку — теоретически возможна коллизия, когда для двух разных паролей получится одинаковый хеш, но подбором параметров функции и длины самого хеша можно свести вероятность этого события почти к нулю. И, наконец, главное отличие от шифрования: хеш-функция работает очень быстро.

Как же преступники взламывают хешированные пароли, если ключа вообще нет? Да очень просто: они перебирают всевозможные комбинации символов, генерируют для них хеши и сравнивают

---

1 Hash (англ.) — мешанина, мусор, ненужная информация. В русском языке возможны два варианта транслитерации: хеш или хэш. Смысл термина можно трактовать так: зная только хеш, мы не получим никакой полезной информации, сам по себе хеш выглядит бессмысленным набором байтов.

с имеющимися в базе. Если совпали хеши, то и сами пароли совпадают. Например, хеш самого популярного пароля 123456 по алгоритму SHA-1 выглядит вот так: 7c4a8d09ca3762af61e59520943dc26494f8941b.

Само собой, жулики даром время не теряли и провели большую работу, чтобы составить так называемые радужные таблицы, которые позволяют не тратить время на вычисление хешей популярных паролей, — подобно тому, как раньше были таблицы Брадиса для квадратных корней, синусов, косинусов и других функций.

И как же быть? Ведь если по таблице запросто можно найти исходный пароль, значит, хеши бесполезны?

Не совсем так. Во-первых, полная таблица для всех возможных паролей получилась бы такого гигантского объема, что поиск по ней занял бы слишком много времени. Во-вторых, есть множество разных функций хеширования, и под каждую из них нужна своя радужная таблица.

Зачем пароли солят?

Чтобы они были вкуснее. Шутка! На самом деле, чтобы осложнить жизнь хешкрекерам (это хакеры, которые специализируются на подборе хешей), разработчики придумали перед вычислением хеша добавлять к исходному паролю некую случайную последовательность символов — на их жаргоне это называется «соль». Причем «соль» может динамически меняться, чтобы еще больше запутать взломщика.

«Соление» паролей полезно еще и потому, что, если два пользователя имеют один и тот же пароль, у них будет совпадать и хеш-код пароля.

> *Люди не склонны слишком напрягать фантазию, изобретая пароли. Например, в 2018 году на 23 месте в списке 100 худших паролей оказалось имя президента США Трампа — «Donald». Также часто используются имена других знаменитостей и популярных персонажей, названия культовых кинофильмов и музыкальных групп.*

Можете быть уверены, что хакеры провели предварительную работу и посчитали для них хеши, так что на сегодняшний день добавление «соли» является абсолютно необходимым элементом защиты паролей — и пока достаточно надежным.

Зачем это пользователю? Чтобы понимать, откуда взялось требование сложных и длинных паролей, и не ворчать по этому поводу. И еще: чтобы относиться с недоверием к ресурсам, допускающим короткие и простые пароли.

> *Но откуда нам знать, насколько ответственно разработчики относятся к защите паролей? Увы, на этот вопрос ответа нет. Именно поэтому важно использовать разные пароли к разным сервисам.*

Вполне вероятно, что ваши любимые пароли уже утекли, и продолжать ими пользоваться небезопасно. Национальный центр кибербезопасности Великобритании в мае 2019 года опубликовал список из 100 тысяч паролей, известных хакерам, и это лишь малая часть того, что можно найти в интернете. «Соль»

задержит злоумышленников на какое-то время, но не остановит совсем, так что к составлению паролей лучше подойти креативно.

Как придумать хороший пароль?

Итак, насчет плохих паролей все понятно — не использовать дни рождения, номера телефонов, вообще любые комбинации только из цифр; не годятся простые слова — все, которые есть в словаре; ни в коем случае пароль не должен совпадать с логином (именем пользователя) и его электронной почтой, не быть его вариацией типа логин «user123», пароль — «user321». Не годятся в качестве пароля и «прогулки по клавиатуре» — так называемые keyboard-walks пароли — например, «qwerty», «qazwsx», даже с добавлением цифр типа «qwerty123456» и тому подобное. Не остановят хакеров и такие банальные хитрости, как заменить букву «o» на ноль, «s» на $, «i» на 1 и так далее.

Может быть, взять строку из песни или из стихотворения? Вот, например, «Tobeornottobe», или «Strawberryfieldsforever», или уж «BewaretheJabberwockmyson!» — уберемпробелыиготово! Хакеры тоже не дураки, эти варианты они учли. К тому же выбранная вами фраза может оказаться очень длинной, а у многих сервисов есть ограничение на количество символов в пароле. Да и намучаетесь вводить его. Разумная длина пароля должна быть порядка десяти знаков, больше не имеет смысла.

Разумная длина пароля должна быть порядка десяти знаков, больше не имеет смысла.

И как же быть? Придется проявить фантазию.

> *Нужно придумать алгоритм, который лично вам будет понятен и логичен, чтобы по нему можно было не только составить надежный пароль, но и вспомнить его, когда понадобится.*

И еще одно важное замечание: многие сервисы устанавливают политики, требующие регулярной смены паролей. То есть ваш алгоритм должен позволять генерировать новые пароли, которые можно будет легко запомнить.

Можно призвать на помощь приемы мнемотехники. Вкратце суть мнемотехники можно передать следующим образом: нам сложно запомнить абстрактные и/или разрозненные данные (в нашем случае это пароли, удовлетворяющие требованиям безопасности) и легче запомнить связи между объектами, между новой информацией и уже имеющейся, ассоциации, наши эмоции по отношению к чему-либо. Иными словами, намного проще запомнить логические, ассоциативные, образные и другие связи между объектами, а не сами объекты. В случае с паролями нам потребуется провести обратное действие — из чего-то хорошо знакомого сделать абстрактный набор символов.

Намного проще запомнить логические, ассоциативные, образные и другие связи между объектами, а не сами объекты.

Вы же помните, как заучивали последовательность цветов спектра? «Каждый охотник желает знать, где сидит фазан» — вот вам и пароль: «kozzgsf». Семь букв маловато, но это не беда, можно взять по две буквы от каждого слова и чередовать заглавные и строчные: «KaOhZhZnGdSiFa».

О, теперь это похоже на перечисление химических элементов! А почему бы не попробовать таблицу Менделеева как генератор паролей? Там и цифры есть. Возьмем, к примеру, инертные газы: «He2Ne10Ar18» — осталось добавить специальные символы, и дело в шляпе. Пусть будет так: «He2!Ne10@Ar18#» — немного банально: символы «!», «@» и «#» идут подряд на клавиатуре, но это не страшно. Теперь проверим его в анализаторе паролей **https://howsecureismypassword.net/** — и увидим, что стойкость этого пароля 204 миллиона лет! А когда понадобится обновить пароль, в следующий раз возьмем, допустим, щелочные или щелочноземельные металлы, галогены, драгоценные металлы, редкоземельные элементы — да что угодно! Можете ходить по периодической таблице хоть по диагонали или даже буквой «Г», как конь в шахматах, — каждый ход будет давать вам прекрасные пароли. Органическая химия тоже может послужить источником вдохновения для придумывания хитрых паролей, если вдруг это ваше хобби.

Если вы не в ладах с химией, можете придумать себе другой способ генерации паролей, — главное, чтобы предметная область была вам хорошо знакома и ассоциации рождались легко. Но будьте осторожны с историей!

— Не понимаю, как они смогли взломать пароль у меня на ноуте?
— А что у тебя за пароль был?
— Год канонизации святого Доминика папой Григорием IX.
— А это какой год?
— 1234

Не хотите попробовать придумать свой алгоритм составления надежных паролей, чтобы он содержал не менее 8 символов — буквы верхнего и нижнего регистра, цифры и специальные символы? Поле широчайшее: можно использовать мелодии, запись шахматных партий, географические координаты, стихи (не слишком известные), физические формулы, счет в теннисном матче и вообще что угодно.

Бывает так, что фантазия нас покинула, а новый пароль придумать надо. Чтобы не ломать голову, можно воспользоваться генераторами паролей, коих в интернете есть великое множество. Один клик — и готово. Например, «w0v2X4%(dA», еще клик — «Yw4ite#3(&7h%9Ms» и так далее. Можно задавать длину пароля, наличие цифр и спецсимволов, гласные или согласные буквы, верхний или нижний регистр — в общем, любой каприз.

> *Человеку психологически трудно самому сгенерировать случайный набор символов, причем удовлетворяющий критериям надежности пароля, если просто наобум тыкать по клавиатуре. Лучше поручить это программе.*

Понятное дело, что запомнить такой пароль нет никаких шансов. Но зато надежно!

Должны ли все пароли быть уникальными?

Согласитесь, если бы ключ от квартиры подходил к машине, банковскому сейфу и шкафчику в раздевалке фитнес-клуба, то это было бы слишком рискованно, не правда ли? Однако люди часто исполь-

зуют одинаковые пароли к разным сервисам — к электронной почте, социальной сети, интернет-банку и случайному сайту, где вдруг потребовалась регистрация, чтобы скачать какой-то файл.

> *В идеальном мире у пользователя должны быть уникальные сложные пароли для каждого сервиса, но мы живем в реальном мире и понимаем, что так делать никто не станет, даже обладая удобной схемой генерации.*

Пожалуй, разумным компромиссом будет использование какого-то одного пароля, который легко запомнить, для регистрации на разных случайных сайтах, когда нужно прочитать какую-то статью или скачать документ, и где не требуется вводить персональные данные. Придумывать и хранить уникальные надежные пароли для каждого из таких сайтов было бы слишком утомительно.

В обязательном порядке вам нужны разные пароли для наиболее важных сервисов: основной электронной почты, социальной сети и банковских приложений. Электронная почта используется как универсальный логин, и на нее же завязана функция восстановления забытых паролей. Получив доступ к вашей почте, злоумышленник может завладеть почти всем вашим цифровым достоянием, поменяв пароли учетных записей.

Обязательно нужны разные пароли для наиболее важных сервисов: основной электронной почты, социальной сети и банковских приложений.

То же самое справедливо и относительно социальных сетей — кроме ущерба для репутации и выпрашивания денег у ваших друзей, преступник может получить доступ ко многим сайтам и приложениям, в которых вы зарегистрированы через ваш аккаунт в соцсети. Это

действительно очень удобно, когда можно нажать всего одну кнопку и сразу начать пользоваться новым сервисом вместо того, чтобы каждый раз заполнять анкету. У этого удобства есть и обратная сторона — более высокий риск при потере контроля над своим аккаунтом.

Про банковские приложения, наверное, понятно и без комментариев. Деньги — это главное, что интересует всех преступников и в интернете, и в обычной жизни. Если у вас несколько банковских приложений, то придется придумать уникальные пароли к каждому из них.

> *В июле 2019 года интернет-магазин Ozon сообщил об утечке логинов и паролей 450 тысяч пользователей. Все скомпрометированные пароли были сброшены сразу после обнаружения утечки, о чем компания уведомила пользователей. «Судя по всему, эти данные попали в Сеть потому, что пользователи из списка использовали одинаковые пароли для разных сервисов. Мошенники также могли получить их в разное время при помощи вирусной атаки на компьютеры пользователей», — добавили в Ozon.*

Вот вам и цена беспечности — взломают что-то одно, а под угрозой окажутся многие ваши аккаунты. Так что думайте сами, решайте сами. Но лучше все-таки не рисковать.

Пароли и дети

Если взрослые испытывают трудности с запоминанием и использованием сложных паролей, то что уж говорить о детях! Было бы наивно полагать, что дети справятся с такой задачей.

В школах Норвегии, где у детей были iPad'ы, они использовали для доступа к своим устройствам как отпечатки пальцев, так и индивидуальные пароли. У них также были пароли для подключения к образовательным платформам и к различным приложениям. Министерство образования Норвегии выдало школьникам индивидуальные пароли, позволяющие им безопасно получить доступ к некоторым учебным платформам. Однако другие платформы и приложения требуют использования дополнительных паролей. В общем, дети изо всех сил пытались запомнить эти различные пароли. В одной из школ однажды утром потребовалось 45 минут, чтобы начать урок, потому что дети забыли свои пароли. В другой школе пароли детей были автоматически обновлены в ночь перед тем, как они должны были пройти тест по математике. Это изменение вызвало проблемы и задержки, когда некоторые из детей пытались получить доступ к тестовым заданиям[1].

Увы, простого ответа на этот вопрос нет. Чтобы безопасно пользоваться интернетом, нужно помнить свои пароли, и при этом они должны быть надежными. Киберпреступники не делают скидок на возраст. Но и требовать от детей, чтобы они всегда помнили все свои пароли — просто глупо, ибо это требование невыполнимо. Наверное, разумным выходом будет записывать детские пароли и хранить их дома в надежном месте.

Требовать от детей, чтобы они всегда помнили все свои пароли — глупо, ибо это требование невыполнимо.

Дети не всегда понимают важность паролей и последствия их компрометации (то есть ситуации, когда пароль становится известен кому-то

1 *Digital Natives or Naïve Experts? Exploring how Norwegian children (aged 9-15) understand the Internet. // EU Kids Online 2018.*

еще). Согласно данным исследования Teen Angels из организации Wired Safety, 75% детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам, в этом же признались 66% девочек в возрасте 7-12 лет[1].

> *Задача взрослых — научить детей хранить свои пароли так же бережно, как ключи от квартиры, и никогда не сообщать их даже друзьям. А если такое все же случилось, то немедленно менять пароль.*

Нельзя отправлять пароли по электронной почте или в SMS, если кто-то попросил, потому что настоящие владельцы веб-сайтов никогда не спрашивают пароли у своих пользователей — так делают только мошенники.

Не вводите пароли на компьютерах, которые вы не контролируете. Не пользуйтесь для входа в соцсети, мессенджеры, электронную почту и другие сервисы, защищенные паролем, общедоступными компьютерами в школе, библиотеке, в интернет-кафе или компьютерных лабораториях. На таких компьютерах можно только посмотреть открытые сайты или поиграть.

- *Не вводите пароли на компьютерах, которые вы не контролируете*

Имеют ли родители право знать пароли детей? Если спросить психологов и юристов, их мнения разойдутся. Ребенок до 14 лет с юридической точки зрения вообще не может иметь мобильного телефона. А психолог скажет, что у ребенка должно быть личное пространство, и его нельзя нарушать. При этом оба они будут правы[2].

---

1 *Памятка по безопасности детей в Сети интернет // Сайт* ***Docplayer.ru.***

2 *Немецкие родители знают пароли своих детей. // RusVerlag.de, 25 ноября 2014.*

Менеджеры паролей

Итак, коль уж мы договорились, что пароли ко всем аккаунтам должны быть разные, но при этом сложные и длинные, и что хранить их где попало небезопасно, самое время задать вопрос — а где и как?

Ричард Фейнман хранил свою шпаргалку с кодами ко всем шкафам в лаборатории Лос-Аламос в замке своего шкафа — он вполне разумно предполагал, что если кто-то вскроет сам шкаф, то вряд ли будет разбирать замок на части. Но чтобы добраться до этих кодов, ему приходилось каждый раз разбирать и собирать замок, что было не очень удобно.

> *С точки зрения безопасности самый надежный вариант хранения пароля — записать его на бумаге и положить в сейф. С особо ценными паролями — например, от криптокошелька, где лежат биткойны на сотни миллионов долларов — именно так и поступают.*

Первые биткойн-миллиардеры братья-близнецы Уинклвоссы (те самые, что судились с Марком Цукербергом)[1], разработали сложную систему хранения и защиты своих персональных ключей. Они разрезали распечатки ключей на части и поместили фрагменты в конверты, хранящиеся в надежных депозитных боксах по всей Америке. Таким образом, если вор и похитит один из конвертов, то не получит весь ключ.

---

1 *Кэмерон Ховард Уинклвосс и Тайлер Ховард Уинклвосс (англ. Cameron Howard Winklevoss, Tyler Howard Winklevoss; род. 21 августа 1981, Саутгемптон, Нью-Йорк) — близнецы, американские гребцы и предприниматели. Братья являются основателями социальной сети ConnectU и долгое время судились с Марком Цукербергом, настаивая на том, что он украл идею их сайта для своей сети.*

Если у вас нет сейфа — не беда. Запишите свой пароль на бумаге и уберите дома в надежное место.

Если у вас нет сейфа — не беда. Запишите свой пароль на бумаге и уберите дома в надежное место. Киберпреступник до ваших записей не доберется, а обычному вору нужны деньги и ценные вещи, а не какие-то бумажки, пусть это и идет вразрез с большинством советов про хранение паролей, которые вы можете найти в интернете. Дело не в том, что пароль записан на бумаге, а в возможности доступа к нему посторонних. Если вы приклеите бумажку с паролем на монитор или положите в открытый ящик письменного стола на работе, это одно. А если уберете в папку с документами дома — то совсем другое.

Однако для повседневного пользования этот способ вряд ли подойдет, ведь пароли для входа в социальные сети или игры нужны каждый день и не только дома. Записывать все пароли в текстовый файл и держать их на рабочем столе или в заметках на телефоне — так себе идея. Их может похитить не то что неведомый хакер, а просто не в меру любопытный друг, которого пустили поиграть на компьютере. Ему достаточно просто вставить флешку или перекинуть ваш файл с паролями себе на почту.

Лучше всего использовать специальную программу — менеджер паролей. Это будет ваш цифровой сейф. Как и все цифровые вещи, в отличие от своего железного собрата он обладает новыми полезными свойствами. Пароли в нем можно не только безопасно хранить, но и использовать. Менеджер паролей работает и как заполнитель форм, и сам подставит нужный пароль, когда вы зайдете на соответствующий сайт.

Дополнительно менеджеры паролей могут работать как защита от фишинга. В отличие от людей, программа не ведется на визуальные имитации, которые похожи на настоящие веб-сайты. То есть после перехода по сомнительной ссылке на фишинговый сайт менеджер паролей не подставит ваши данные в форму ввода, а сообщит, что сайт является подделкой. Это весьма ценное свойство, особенно с учетом того, что человек не может быть постоянно бдительным, и вероятность попасться на удочку мошенников достаточно велика. С таким бонусом использование специальной программы становится выгодным, даже если у вас имеется всего несколько паролей, которые можно было бы и так запомнить.

Человек не может быть постоянно бдительным, и вероятность попасться на удочку мошенников достаточно велика.

Практически все современные браузеры имеют встроенный менеджер паролей. Почему бы не воспользоваться этой их функцией? Профессионалы в области информационной безопасности непременно скажут, что это дурной тон и небезопасно, что такие менеджеры не могут заменить полноценных приложений для управления паролями, но... тем не менее согласятся, что менеджеры паролей на основе браузера лучше, чем ничего. Для не слишком искушенного в технологиях пользователя это, в целом, приемлемый вариант. Ибо, во-первых, это удобно — благодаря функции синхронизации в браузере, ваши пароли будут с вами на любом устройстве, как только вы войдете в свой аккаунт.

Во-вторых, они активно совершенствуются. Еще недавно браузерным менеджерам паролей ставили в упрек неумение автоматически генерировать сложные пароли, состоящие из букв, цифр и специальных символов, но это уже в прошлом. Chrome и Firefox уже умеют создавать пароли, отвечающие требованиям безопасности.

Что касается возможностей взлома, этот риск существует для всех систем. Но чаще всего для реализации такой атаки все-таки сначала нужно установить на компьютер или телефон жертвы шпионское ПО. Чтобы этого избежать, не давайте свои устройства посторонним, используйте антивирусы и другие средства защиты — будьте начеку.

Не давайте свои устройства посторонним, используйте антивирусы и другие средства защиты — будьте начеку.

В качестве аргумента против использования Chrome для хранения паролей упоминают еще и то, что Google следит за пользователями в попытке показывать им более точно таргетированную рекламу. Да, это факт, но безопасности ваших паролей это не угрожает. (Подробнее о механизмах слежки и способах противодействия мы поговорим в главе об анонимности в интернете.) То есть если вы так или иначе пользуетесь продуктами «корпорации добра», как иронически называют Google, то в целом нет особых причин отказываться и от их менеджера паролей.

> *В браузере Chrome от Google появилось расширение под названием PasswordCheckup, которое автоматически проверит, были ли пароли раскрыты в результате взлома данных. После установки расширение проверяет все используемые данные для входа в систему Google по базе данных, насчитывающей около четырех миллиардов имен пользователей и паролей, и предупреждает вас, если найдет совпадение*[1].

1 *Google's new Chrome Extension automatically checks your passwords are still secure // The Verge, 5 февраля 2019.*

Кроме встроенных в браузеры программ есть еще множество специального ПО для управления паролями — платного и бесплатного, от известных производителей и не очень. Все они очень разные, ситуация на рынке постоянно меняется, поэтому нужно следить за обзорами, чтобы выбрать тот продукт, который вам подойдет больше.

Опасайтесь стилеров и кейлоггеров

А не слишком ли опасно хранить все пароли в одном месте? Если основной пароль будет похищен или взломан, это поставит под угрозу все хранимые пароли.

Да, такая опасность существует, и разработчики менеджеров паролей об этом знают. Поэтому они настоятельно рекомендуют соблюдать следующие правила:

- Основной пароль должен быть сложным, и его надо запомнить. Ни в коем случае не держите его записанным на компьютере или на бумажке рядом с ним;

- Используйте двухфакторную аутентификацию для входа в аккаунт браузера, если вы пользуетесь встроенным менеджером паролей;

- Настройте безопасный вход в менеджер паролей в соответствии с инструкциями производителя, если вы используете специальное ПО;

- Используйте антивирус, он может заметить подозрительную активность и пресечь атаку на вас;

- Не давайте свои устройства посторонним и всегда блокируйте, если вам нужно отойти.

> *Что такое стилер? Это шпионская программа, предназначенная для того, чтобы находить и воровать с устройства жертвы ценные данные — пароли, номера банковских карт и тому подобное.*

Название происходит от английского слова «steal» — «воровать». Обычно эти данные хранятся в определенных местах на диске, и стилер просто пытается скопировать нужные файлы и отправить их своему хозяину. Простейший стилер может написать даже школьник, но чтобы его внедрить на чей-то компьютер, нужен физический доступ. Более сложные программы-шпионы могут проникнуть к вам по сети. Однако на диске пароли, как правило, хранятся в зашифрованном виде, и далеко не факт, что вору удастся их расшифровать.

Даже если все ваши данные надежно зашифрованы и лежат в секретном месте, есть один момент, когда система очень уязвима — это момент ввода пароля. Вот здесь-то и вступают в игру кейлоггеры.

> *Кейлоггер — другая разновидность шпионского ПО, также нацеленная, в основном, на кражу паролей. Этот шпион после внедрения на компьютер записывает нажатия клавиш на клавиатуре и передает их преступникам.*

Потому он так и называется — от английского «keylogging», что значит «вести журнал нажатий клавиш». Разумеется, кейлоггер записывает не все подряд, иначе объем передаваемых данных

был бы слишком заметным. Он умеет определять, что́ в данный момент показывается на экране, и ждет, когда появится окно ввода пароля. Этот вид шпионов широко распространен, у них даже есть свои рейтинги. В их функции входит получение случайных снимков экрана, запись звука, отправка записанных нажатий клавиш на указанный адрес электронной почты, мониторинг других активных приложений и посещенных веб-сайтов. Многие программные кейлоггеры работают незаметно, никогда не появляясь в диспетчере задач как работающие приложения.

Существуют также и аппаратные кейлоггеры — их можно вполне открыто приобрести на Amazon примерно за 50 долларов. Однако, чтобы их использовать, нужно каким-то образом получить доступ к компьютеру жертвы.

Есть кейлоггеры и для телефонов с ОС Android. Их кто-то может скрытно установить на ваш телефон и следить за вами.

Акустический криптоанализ: немного из настоящей шпионской жизни

Как можно догадаться из названия, это метод получения секретных данных на основе изучения шумов, издаваемых при печати текста. Его использовали еще с 1950-х годов, когда все печатающие механизмы сильно шумели. Например, в ходе операции в 1956 году в Лондонском посольстве Египта были размещены прослушивающие устройства, которые перехватывали шумы, издаваемые шифромашинами. Это позволило британским разведчикам получить секретную информацию, что повлияло на позицию Великобритании в Суэцком кризисе.

И сейчас этот метод стоит на вооружении хакеров и спецслужб, потому что мы все еще используем механические клавиатуры, и они издают шумы. (В этом месте начинающий параноик должен подумать хотя бы о том, чтобы отключить звук тональных сигналов при наборе телефонного номера.) Несмотря на прогресс шпионских технологий, атака подобным методом все-таки довольно сложна и ее еще надо «заслужить» — против обычных пользователей вряд ли кто-то станет ее использовать.

Снизить риск от такого рода угрозы можно путем использования экранной клавиатуры — эта функция обычно есть в продвинутых менеджерах паролей. Можно воспользоваться и стандартной экранной клавиатурой Windows.

Что надо запомнить про пароли

Итак, подведем итоги. Что грамотный пользователь должен знать про пароли?

Длинный и сложный пароль — это не каприз разработчиков, а реальная необходимость. Чтобы пароль мог считаться безопасным, его длина должна составлять не менее 8 символов и включать буквы верхнего и нижнего регистров, цифры и специальне символы.

Для придумывания и запоминания сложных паролей можно использовать различные мнемотехники — это не так трудно, как кажется.

Графический пароль на Android должен включать не менее 8 узлов, не начинаться из угла и иметь пересечения, чтобы считаться надежным.

Иметь одинаковые пароли для всего слишком рискованно. По крайней мере, для всех важных сервисов пароли должны быть уникальными.

Пароли надо регулярно менять, потому что происходят утечки данных, возможно и ваших тоже.

Использовать отпечаток пальца или снимок лица можно, но не в качестве основного пароля.

Двухфакторная аутентификация, то есть подтверждение входа в систему или важных действий по SMS или другому каналу, обязательна для всех важных сервисов.

Менеджер паролей — полезная вещь, нужно выбрать и научиться им пользоваться, если вы еще этого не сделали.

В общем, к своим паролям нужно относиться максимально трепетно, заботиться об их сохранности, и тогда у вас будет меньше поводов волноваться о сохранности своих данных, денег и репутации.

Контрольные вопросы

1. Что такое пароль?
2. Как паролем пользовались древние римляне?
3. Что такое ПИН-код?
4. Что такое двухфакторная аутентификация?
5. Что такое биометрия?
6. Какие виды биометрических показателей вы знаете?
7. Можно ли защищать ценные данные только отпечатком пальца?
8. Почему обязательно нужно менять пароли по умолчанию?
9. Какой пароль считается надежным?
10. Что нельзя использовать как пароль?
11. Зачем надо регулярно менять пароли?
12. На каких домашних устройствах могут быть пароли?
13. Почему нельзя использовать один пароль на все?
14. Как можно хранить свои пароли?

15. Что такое брутфорс?

16. Что такое капча и зачем она нужна?

17. Сколько комбинаций на кодовом замке с тремя лимбами по 20 чисел?

18. Что такое хеш пароля?

19. Для чего нужны менеджеры паролей?

20. Что такое стилеры паролей?

21. Что такое кейлоггеры?