DOI: 10.25728/iccss.2023.57.93.037

Логинова Л.Н., Резников Р.М.

Символьная парольная аутентификация как средство повышения информационной безопасности

Аннотация: В работе показаны особенности обеспечения информационной безопасности с помощью некоторых способов аутентификации, проведен анализ символьных паролей, биометрической и двухфакторной аутентификации, даны рекомендации пользователям по эффективному использованию двухфакторной аутентификации.

Ключевые слова: информационная безопасность, утечка данных, защита информации, аутентификация, биометрия, двухфакторная аутентификация

В современном мире вопросы аутентификации, авторизации и идентификации при использовании вычислительных средств встают особо остро [1, 2]. Аутентификация по символьному паролю – это один из наиболее распространенных методов подтверждения личности пользователей в цифровом мире. Как и многие другие универсальные, рассчитанные на максимально широкое применение системы, символьная парольная аутентификация обладает рядом значительных преимуществ и недостатков. К главным плюсам такой системы можно отнести:

– принцип пароля в виде слова или словосочетания существовал задолго до появления компьютерных систем. Символьные пароли хорошо знакомы рядовому пользователю и не будут вызывать сложностей у сотрудников при внедрении;

– пароли могут быть использованы практически на всех устройствах и веб-сервисах, что делает их универсальным методом аутентификации. Отдельно нужно отметить, что они не требует использования аппаратных средств;

– пароль можно легко и оперативно сменить при угрозе компрометации. Пользователь может справиться с такой процедурой самостоятельно.

Парольная аутентификация имеет следующие недостатки.

– Уязвимость паролей к взлому может вырасти от множества факторов. Уязвимы слишком короткие, простые и повторяющиеся символьные пароли для разных учетных записей одного пользователя. Утечка повторяющегося пароля ставит под угрозу сразу множество систем, к которым имеет доступ пользователь. Именно так произошла одна из самых масштабных атак в 2021 году. Повторяющийся для разных сервисов пароль от *VPN*-решения одного из сотрудников оператора крупнейшего трубопровода в США *Colonial Pipeline* попал в руки киберпреступников [3]. Этот недостаток особенно важен, т.к. пользователи склонны использовать настолько простые пароли, насколько позволяет политика безопасности. Согласно исследованию *NordPass*, в 2022 году самыми популярными комбинациями оставались «*password*», «123456» и «123456789» [4].

– Уязвимость символьных паролей к социальной инженерии. Злоумышленники придумали множество способов похищения учетных данных. Исследователи Positive Technologies сообщают, в 2022 году 93% атак на частных лиц и 43% атак на организации использовали социальную инженерию. Утечка же конфиденциальных данных стала самым распространенным последствием атак. В 41% атак на частных лиц и в 14% атак на организации похищали именно учетные данные [5].

– Пароль легко забыть, особенно если он длинный и сложный, состоящий из случайных символов. Чем сложнее пароль, тем больше соблазн для пользователя записать комбинацию, часто на ненадежном носителе.

– Парольная аутентификация удобна и широко используется, но только ее недостаточно для обеспечения надежной защиты, потому ее часто комбинируют с другими методами безопасности, такими как биометрическая и двухфакторная аутентификация (*2FA*).

Одной из самых часто встречающихся альтернатив парольной аутентификации является биометрическая аутентификация. Наиболее распространен вариант аутентификации по отпечатку пальца, именно этот вариант чаще всего используется в смартфонах. Существуют варианты биометрической аутентификации по строению лица, радужке глаза, геометрии ладони и голосу.

Независимо от варианта биометрическая аутентификация обладает рядом преимуществ перед парольной аутентификацией. К ним можно отнести скорость ввода, значительно меньшее время, затрачиваемое на ввод символьной комбинации, неотчуждаемость идентификатора у пользователя и устойчивость к основным методам фишинга: злоумышленник не сможет обманом получить, например, отпечаток пальца. Благодаря вышеперечисленным преимуществам биометрическая аутентификация получила большее распространение при использовании на личных устройствах.

Вместе с тем на данный момент биометрическая аутентификация не может полностью заменить парольную аутентификацию из-за некоторых минусов. Главная проблема заключается в необходимости аппаратного решения для считывания биометрического идентификатора. При этом для обеспечения большей степени защиты необходимо использовать сканеры с расширенными возможностями, например, сканер отпечатка пальца должен определять температуру идентификатора для защиты от аутентификации по скопированному злоумышленником отпечатку на неодушевленном объекте. Исследователям из Университета штата Мичиган удалось доказать действенность такого метода еще в 2016 году [6]. Сканер геометрии лица должен быть усилен определением *3D* параметров лица для защиты от аутентификации по фотографии. При этом программного решения идентификации не только по геометрии лица, но и определению по проявлениям эмоций может быть недостаточно. Развитие технологии *deepfake*, позволяющей не только создать реалистичную фотографию, но и в режиме реального времени подменять лицо человека на видео позволит обойти такое решение. Существенным недостатком всех видов биометрических аутентификаций стало дублирование системой парольной защиты. Являясь неотчуждаемыми, биометрические параметры все же подвержены изменению и кратковременной недоступности. Для таких случаев биометрическую аутентификацию дублируют возможностью зайти по символьному паролю, что полностью нивелирует дополнительную защиту биометрии. Злоумышленник сможет продолжить обходить аутентификацию привычными методами атаки на парольную защиту.

Дополнительно нужно отметить, что часть биометрических данных, например, отпечатки пальцев остаются неизменными. Пользователь никогда не сможет сменить подобные идентификаторы, а значит, их утечка будет особенно критична. Из-за этого во многих странах биометрические данные особо охраняются законодательно, а значит, их хранение и обработка требуют сложных и дорогостоящих систем защиты. Одним из самых ярких примеров утечки биометрических данных стала компрометация 5,6 миллионов отпечатков пальцев федеральных служащих США, часть которых имеют секретные допуски в 2015 году [7].

Двухфакторная аутентификация (2FA*)* представляет собой, в классическом смысле, подтверждение личности пользователя перед предоставлением доступа с помощью дополнительной проверки одноразового пароля, высылаемого пользователю во время аутентификации. Постепенно двухфакторная аутентификация становится обязательным дополнением к парольной защите. Требования начинают появляться и на законодательном уровне, например, ГОСТ 57580.1 ввел обязательное использование *2FA* при аутентификации эксплуатационного персонала (администраторов и других привилегированных пользователей) и пользователей удаленного доступа для финансовых организаций. Применение двухфакторной аутентификации значительно усложняет взлом учетной записи, делает простой фишинг менее эффективным, т.к. теперь киберпреступнику недостаточно просто получить пару логин-пароль. Для успешной атаки злоумышленнику придется либо выходить на прямой контакт с целью в момент атаки, либо использовать более сложные инструменты и вредоносное программное обеспечение. Не смотря на указанную сложность злоумышленники активно разрабатывают и применяют подобные инструменты. Например, шпионское программное обеспечение (ПО) *KingsPawn*, ориентированное на устройства под управлением *iOS*, может не только собирать конфиденциальную информацию о жертве, но и генерировать одноразовые коды для *iCloud (time-based one-time password, TOTP*) на произвольные даты [8].

Разнообразие методов обеспечения *2FA* аутентификации позволяет выбрать наиболее удобный для конкретной задачи.

Одноразовые коды могут приходить пользователю в *SMS*, специальном приложении или на электронную почту.

Несмотря на множество преимуществ, у двухфакторной аутентификации есть и недостатки.

– Усложнение процесса аутентификации, при добавлении в него нового звена. Пользователи могут счесть *2FA* неудобной и слишком долгой для каждого входа, отключать ее, если двухфакторная аутентификация не является обязательной.

– Пользователи могут не иметь доступа к устройству или сервису, в который приходит одноразовый код, что вызовет проблемы при аутентификации. Это может произойти как по вине пользователя, например, потерявшего телефон, так и из-за проблем со связью, ограничивающих доставку *SMS* или ошибки на стороне сервера приложений для двухфакторной аутентификации.

– Двухфакторная аутентификации не является абсолютной защитой. Даже правильно настроенная система может быть взломана, в том числе с помощью социальной инженерии. Например, активно эксплуатируемая в 2023 году фишинговая платформа *EvilProxy*, распространяемая по модели *Phising-as-a-Service*, нацелена на *cookie* файлов [9]. Поскольку пользователю уже приходилось проходить проверку *2FA* при входе в учетную запись, злоумышленники смогут обойти двухфакторную аутентификацию.

Несмотря на указанные минусы, в большинстве случаев *2FA* остается дополнительным средством обеспечения безопасности учетных записей. Для эффективного использования двухфакторной аутентификации пользователям можно рекомендовать выполнение следующих правил: изучить и научиться узнавать базовые приемы социальной инженерии, всегда оставаться бдительным в Интернете; использовать надежные резервные пароли, и ни в коем случае никому их не сообщать; по возможности отдавать предпочтение двухфакторной аутентификации с помощью приложений, а не SMS-сообщений; для критически важной информации применять трех- и более факторную аутентификацию, рассмотреть возможность использования дополнительных физических ключей.

Литература:

1. *Минаков В.А*. Анализ эффективности аутентификации с помощью графических паролей // Вестник ВГТУ. – 2009. – № 11. –

URL: https://cyberleninka.ru/article/n/analiz-effektivnosti-autentifikatsii-s-pomoschyu-graficheskih-paroley (дата обращения 01.10.2023).

2. *Фатхи Д.В., Галушка В.В*. Повышение сложности пароля – пользователя на основе комплексирования символов пароля и временных интервалов между ними // ИВД. – 2019. – № 1 (52). – URL: https://cyberleninka.ru/article/n/povyshenie-slozhnosti-parolya-polzovatelya-na-osnove-kompleksirovaniya-simvolov-parolya-i-vremennyh-intervalov-mezhdu-nimi (дата обращения 07.10.2023).

3. Хакеры атаковали Colonian Pipeline с помощью «утекшего» пароля. – URL: https://www.securitylab.ru/news/520905.php (дата обращения 01.10.2023).

4. Самый популярный пароль у пользователей в 2022. – URL: https://www.ixbt.com/news/2022/11/15/password-2022-123456.html (дата обращения 01.09.2023).

5. Актуальные киберугрозы: итоги 2022 года. – URL: https://ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения 01.10.2023).

6. All you need to dupe a fingerprint sensor is a paper, conductive ink, and a inkjet printer. – URL: https://slate.com/technology/2016/03/michigan-state-university-research-shows-how-easy-it-is-to-trick-a-fingerprint-scanner.html#:~:text=Researchers%20at%20Michigan%20State%20University,conductive%20ink%2C%20and%20regular%20paper./ (дата обращения 01.10.2023).

7. Злоумышленники похитили отпечатки пальцев 5,6 млн американских госслужащих. – URL: https://www.securitylab.ru/news/474804.php (дата обращения 01.10.2023).

8. Системный календарь iPhone «приглашает» пользователей установить израильское шпионское ПО. – URL: https://www.securitylab.ru/news/537525.php (дата обращения 01.10.2023).

9. Набор фишинговых инструментов EvilProxy позволяет киберпреступникам обходить двухфакторную защиту. – URL: https://www.securitylab.ru/news/533766.php?clear_cache=Y (дата обращения 01.10.2023).