ПРИМЕНЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ С АППАРАТНЫМ КЛЮЧОМ В ВЕБ-РАЗРАБОТКЕ

Д. В. Иванов

Белорусский государственный университет, г. Минск;
d.ivanov1243@gmail.com;
науч. рук. – Е. В. Кремень, канд. физ.-мат. наук, доц.

В данной статье рассмотрим двухфакторную аутентификацию, а также особенности двухфакторной аутентификации с аппаратным ключом. Определим, как преимущества предоставляет использования такого способа аутентификации для обычных пользователей и для бизнеса. Рассмотрим применение аппаратного ключа в веб-разработке в связке с программной средой Node.js.

Ключевые слова: защита данных; двухфакторная аутентификация; аппаратный ключ; Node.js.

Защита пользовательских данных – далеко не новая проблема. Наиболее уязвимыми являются данные аутентификации, ведь насколько эффективными бы не были методы шифрования хранимых и передаваемых данных, такие методы окажутся бесполезными, как только будет скомпрометирован логин и пароль.

Для усиления степени защиты используется двухфакторная аутентификация – комбинация из пароля и ключа-подтверждения. Наиболее часто используемые методы двухфакторной аутентификации работают по номеру телефона или электронной почте. Такие методы предоставляют больший уровень безопасности, чем однофакторная аутентификация, однако все еще могут быть подвержены фишингу и могут быть неудобны в ряде ситуаций (например, подтверждение по номеру телефона, когда вы находитесь в роуминге).

Более безопасным вариантом многофакторной аутентификации является аппаратный ключ – небольшое устройство, оснащенное криптопроцессором и интерфейсом Bluetooth, NFC или USB. Аппаратный ключ является быстрым и надежным способом защитить пользовательские данные. Такой способ защиты подойдет для людей, работающих с конфиденциальной и личной информацией, таких как администраторы баз данных, системные администраторы, сетевые администраторы и администраторы безопасности, разработчики приложений, сотрудники, работающие с финансами, топ-менеджеры и сотрудники отдела кадров.

Аппаратный ключ позволяет улучшить безопасность как устаревших, так и современных способов многофакторной аутентификации, таких как FIDO2 или WebAuth. Аппаратный ключ использует микрочип для генера-

ции секретных ключей и такой алгоритм генерации не может быть скопирован или украден удаленно, что делает его наилучшим решением для привилегированных пользователей.

Фишинг – один из способов добычи персональных данных, логины и пароли зачастую являются главными мишенями таких атак. По данным Google [3], 68% фишинговых атак (рис. 1) – новые вариации писем, никогда не наблюдаемых ранее, из чего можно сделать вывод что такой тип угроз продолжает расти и развиваться.

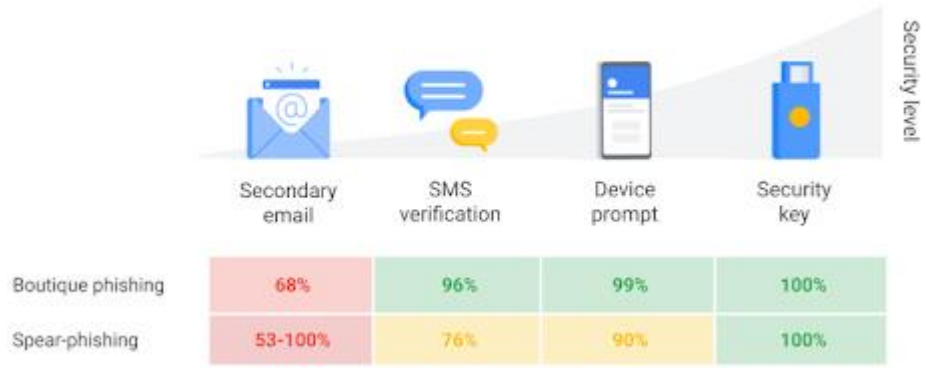

Рис. 1. Степень защиты различных методов двухфакторной аутентификации

Аппаратные ключи надежно защищают от таких угроз и предоставляют самый надежный способ защиты от захвата аккаунтов путем таргетированных фишинг-атак. Даже в случае, когда персональные данные скомпрометированы, защиту аппаратным ключом не получится обойти, так как учетные данные привязаны к реальному сайту и новая кодовая комбинация генерируется при каждой новой попытке авторизации.

От использования аппаратного ключа могут выиграть разные типы пользователей. Компании могут снизить затраты на обслуживание аккаунтов в случае утери или кражи данных авторизации. Исходя из отчета компании Yubico за 2019 год, от 20% до 50% звонков в службу поддержки представляли из себя запросы на сброс пароля [4]. Такие запросы могут обходится компаниям в среднем по $70 за каждый. Использование аппаратных ключей значительно снижает необходимость обслуживания паролей.

Обычные пользователи, также могут воспользоваться преимуществами аппаратных ключей, крупные платформы на аппаратных ключах поддерживают двухфакторную аутентификацию на многих платформах, куда входять социальные сети (Facebook, Twitter, Instagram), все сервисы Google (Google Диск, Gmail, YouTube), менеджеры паролей, прочие почтовые клиенты и облачные хранилища. Также поддерживается аутентификация в системах Windows, MacOS и Linux.

Многие производители предоставляют API и SDK для интеграции аппаратных ключей в приложения для персональных компьютеров, мобильных устройств, а также веб-сервисы, поддерживая языки Python, Java и C [1].

Применение ключа Yubikey в WEB на примере Node.js

В данном случае двухфакторная аутентификация была реализована при помощи библиотеки «yubikey-client» [2]. Ключ Yubikey позволяет реализовать как подтверждаемую онлайн, так и оффлайн аутентификацию используя OTP (одноразовый пароль). Ключ может использоваться как для подтверждения пользовательской сессии, так и для выполнения различных чувствительных к атакам действий.


```
{
    t: '2013-08-31T07: 13: 27Z0111',
    otp: 'cccaccbtbvkwjjirhcctvdgbahdbijduldcjdurgjgfi',
    nonce: '50fb8a88a327b4af16e6e7bd9ec4e4e6c692f2e5',
    sl: '25',
    status: 'OK',
    signatureVerified: true,
    nonceVerified: true,
    identity: 'cccaccbtbvkw',
    serial: 123456,
    valid: true
}
```


Рис. 2. Пример данных yub.verify библиотеки yubikey-client

Для онлайн-аутентификации сервис должен быть зарегистрирован в сервисе Yubico, с получением API ключа. При онлайн-аутентификации клиент-модуль считывает секретную комбинацию аппаратного ключа, затем комбинация передается на сервер, а затем на сервер Yubico для подтверждения. При оффлайн-авторизации параметр nonceVerified (рис. 2) всегда равен false, что означает что сгенерированный ключ не был подтвержден сервером Yubico.

Таким образом, аппаратный ключ предоставляет повышенный уровень защиты пользовательских данных и большую простоту использования по сравнению с другими методами двухфакторной аутентификации, позволяет уменьшить затраты на обслуживание пользовательских аккаунтов для больших компаний и унифицировать способ авторизации для обычных пользователей без потери степени безопасности.

Библиографические ссылки

1. Youbico Developers [Electronic resource]. URL: https://developers.yubico.com/ (date of access: 12.05.2020).
2. Yubikey-client – npm [Electronic resource]. URL: https://www.npmjs.com/package/yubikey-client (date of access: 12.05.2020).
3. Google Online Security Blog: Understanding why phishing attacks are so effective and how to mitigate them [Electronic resource]. URL: https://security.google-blog.com/2019/08/understanding-why-phishing-attacks-are.html (date of access: 12.05.2020).
4. The 2019 State of Password and Authentication Security Behaviors Report [Electronic resource]. URL: https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf (date of access: 12.05.2020).