УДК 621.382

Каримов М.М., Арзиева Ж.Т., Худойкулов З.Т.

Анализ метода аутентификации на основе одноразовых паролей

Аннотация. В данной статье анализированы методы генерации одноразовых паролей и методы передачи их пользователю. Хотя, почти все аутентификаторы базированные на основе одноразовых паролей, которые основаны на синхронизации времени, из-за возможности извещения временной метки и исчерпания времени применимости паролей они сталкиваются с проблемами безопасности и использования. Считается, что передача паролей на основе SMS самый распространенный метод, но передача в открытом виде сообщений, делает безопасность мобильной среды менее эксплуатируемым. Кроме того, в результате анализа определены не существование методов аутентификации, основанные на одноразовые пароли, которые являются стойкими к атакам типа «человек в середине», «просмотр через плечо».

Ключевые слова: одноразовый пароль (One Time Password, OTP), DOS-атака, схема Лемпорта, HOTP (An HMAC-Based One-Time Password Algorithm), TOTP (Time-Based One-Time Password Algorithm), TAN-кодом (Transaction authentication numbers).

В условиях постоянного увеличения доли онлайн-сегмента бизнеса все острее нужда в том, чтобы защита данных была особенно надежной. Если еще можно “пережить” взлом личной странички в социальное сети, то потери информации в бизнесе могут привести не только к утрате репутации и доходов, но и к закрытию компании.

Одним из самых уязвимых моментов в информационное безопасности является надежная аутентификация пользователя, пытающегося получить доступ к своему аккаунту на том или ином веб-ресурсе.

Знакомые всем многоразовые, обычные пароли при современном уровне хакерских угроз практически бесполезны. Они не в состоянии выдержать напор злоумышленников, оснащенных такими “инструментами” как кейлоггеры, перехват данных, методы социальной инженерии. На порядок более высокий уровень защиты может обеспечить применение одноразового пароля.

OTP является механизмом основанная на одноразовых паролях для применения в сетях или услуг, который гарантирует не использование логин/пароля при утрате. В данном случае логин пользователя не меняется, но пароль будет меняться при каждом обращении пользователя к системе для входа.

В настоящее время при генерации одноразовых паролей применяется следующие методы:

1. Основанная на синхронизации времени

В OTP основанные на синхронизации времени обычно используют маленькое устройства, называемое как токен безопасности (с помощью данного токена OTP генерируется). Внутри данного токена существует очень точно работающий часы, которые синхронизированы с сервером аутентификации. На основе данного метода используется синхронное время и распределенный ключ для генерации OTP. При этом с использованием данных двух параметров на основе необратимых односторонних функций (например, код аутентификации сообщений – Message authentication code, MAC) генерируется OTP. Явным примером можно привести алгоритм TOTP (Time-Based One-Time Password Algorithm [18]). В данном алгоритме во избежание существующих проблем с зонами времени, использованы метки UNIX времени, которые представлены на секундах, начиная с 1 января 1970 года. Данный временное значение из-за представления в секундах T параметр ($T = [(\text{UNIX время})/30]$) для TOTP алгоритма генерируется на каждые 30 секунды.

Принцип работы TOTP алгоритма аналогичен к ниже приведенному принципу работы HOTP (An HMAC-Based One-Time Password Algorithm), но вместе перечисления используется T параметр времени. В практике во многих приложениях используется алгоритм TOTP (например, Google Authenticator, Microsoft Authenticator). В качестве токена может использована мобильные устройства, в котором установлена специальное программное средство.

2. Основанная на математических алгоритмах (основанные на предыдущих значений)

На основе данного метода следующий OTP генерируется с использованием предыдущего. При этом заранее будет определена последовательность необходимых функций. Схема Лемпорта [1] играет особую роль при генерировании OTP, которые подлежат к данной группе.

Таблица 1

Анализ методов генерации OTP основанные на математических алгоритмов

Методы	Сервер		Пользователь		Пользователь →Сервер	
	Количество хешированный	Хранимые данные	Количества хешированный	Хранимые данные	Количества передач	Длина передаваемого сообщения
S/Key [7]	1	Seed, n	M-n	n	2	L(Seed)+ L(M-n) +L(h)
Лампорт [1]	1	n	M-n	n	1	L(h)
SAS-R [5]	2	ID, V_n	5	n_i	1	L(ID)+ 2L(h)
SAS-2 [8]	1 (2)	ID, V_n	3 (4)	n_i	1	L(ID)+ 2L(h)
Хеа С.Ж. [6]	1	ID, V_n, P_n	3	Токен (K, Seed)	2	L(ID)+ 2L(h)+ L(N_i)

Методы аутентификации, основанные на схеме Лампорта, являются простыми, но требуют многоразового использования операции хеширования от пользователя в каждом сессии аутентификации. Это в свою очередь требуют много потребления времени и возможностей устройства [2].

Метод аутентификации SAS (Simple and Secure), разработанное М. Сандиригамой и др. [3] не требует хранения, высоких выполняемых операций передачи через сеть и позволяет снизить риск проведения атаки «Человек в середине», но при этом является не стойким к атакам повторения и DoS [4]. Вышеприведенные проблемы решены в алгоритме OSPA (Optimal Strong-Password Authentication) [4] и в модифицированной версии SAS протокола [5], но аппаратная реализация, которые имеют малые возможности являются очень трудным (модифицированная версии протокола SAS требует 5 кратного хеширования в каждом (SAS-R) сессии). Хоть и разработан протокол SAS-2 и его вид основанные на «вопрос-ответ», в котором сделаны попытки снизить количества использования односторонних функций и позволяющий обеспечивать двухстороннюю аутентификацию [8] (секретное значение, например, случайное значение), но они до сих пор требуют хранения разных данных и определенных вычислений. Кроме того, можно увидеть таких проблем и в других [6, 7] методах аутентификации, которые аналогичны к схемам Лампорт, SAS и др. (Таблица 1).

3. Основанный на математическом алгоритме (основанный на синхронном счетчике или “вопрос” у)

Данный метод генерации OTP использует некоторое вводимое случайное значение (“вопрос” или значение счетчика) и распределенный ключ. В качестве примера, который входит в данный тип можно привести алгоритм HOTP (An HMAC-Based One-Time Password Algorithm [17]). HOTP алгоритм работает если у двух сторон существует распределенный ключ K и одинаковое состояние счетчика C. Последовательность выполнения данного алгоритма приведена ниже:

a. Вычисление HMAC-SHA1: $HS = HMAC - SHA1(K, C)$. Данное заничение является 160 битным или 20 байтным ($HS[0], \dots, HS[19]$) информацией.

b. Вычисление 4 байтной строки на основе значения HMAC-SHA1 (с помощью динамического сокращения (Dynamic Truncation, DT)): $Sbits = DT(HS)$. Динамическое сокращение вычисляется следующим образом:

I. Выделение самого маленького 4 бита $HS[19]{:}offset = HS[19]\&0xF$. При этом в 10 системе счисления будет в диапазоне $offset \epsilon [0,15]$.

II. После того вычисляется $P = HS[offset]||\ HS[offset + 1]||\ HS[offset + 2]\ ||\ HS[offset + 3]$.

III. Последний 31 бит значения P составляетSbits.

c. Sbits бит переводится в 10 системе счисления (Snum).

d. Пароль с требуемой длиной (digit) соответственно вычисляется следующим уравнением $D = Snum \bmod 10^{digit}$.

Обычно OTP основанные на математических алгоритмах, также называются основанные на событии (Event based). В таблице 2 приведены результаты анализа методов генерации OTP основанные на синхронизации времени и математических алгоритмов и здесь является целесообразным выбрать их по мере среде использования. Например, алгоритм TOTP является эффективным в средах где существует возможность синхронизация времени, а при не существовании данных возможностей в среде целесообразно использовать подходы, основанные на математических алгоритмах.

Пароли, полученные с помощью данных методов генерирования OTP не всегда дает достаточный уровень случайности. В частности, определены, что OTP генерированная в приложении Google Authenticator никогда не начинается с 0 и в результате диапазон ключа для 6 злачных паролей попадает от 106 по 10^6-10^5[9].

OTP генерированная на токене с помощью различных методов, может передаваться на сервер аутентификации и OTP генерированная в сервере аутентификации тоже может различными путями передаваться в пользователь. Широко распространённые методы передачи OTP являются следующие:

Таблица 2

Анализ методов генерации OTP

Метод генерации OTP	Безопасность	При использовании
Основанные на времени	Преимущества: существование OTP значения за короткое время.	Преимущества: Легкость прочтения OTP в экране устройства.
	Недостаток: значение OTP с легкостью может получен со стороны наблюдателя.	Недостаток: Возможность изменения OTP до его использования.
Основанные на математических алгоритмах	Преимущества: для генерации OTP требуется управления токена со стороны злоумышленника.	Преимущества: OTP генерируется по запросу пользователя; через определенное время его значение не измениться.
	Недостаток: Возможность использования OTP до генерации нового OTP.	Недостаток: для генерации OTP требуется нажатие кнопки “генерирование” со стороны пользователя.

1. Через мобильный телефон. Одним из широко применяемых методов передачи, генерированной OTP это сообщения в виде текста. Основной причиной этого является то, что сообщения в виде текста возможно передавать с помощью мобильных устройств через все существующие каналы связи. Кроме того, передача сообщения в виде текста не требуют больших затрат (в многих случаях никакой затраты). Сообщения в виде текста обычно передается с помощью сервиса SMS (Short Message Service). SMS сообщения отправляются в открытом виде [16], кроме того существует проблемы безопасности в протоколе маршрутизации SS7, из-за таких проблем, со стороны злоумышленника OTP легко может быть получен.

2. Частные токены. Данный метод передачи OTP применяет специальные токены, явным примером на данный тип можно привести устройства SeccurID компании RSA Security [15]. Данные токены основаны на синхронизации времени и требует от пользователя безопасного сохранения. В них существует дисплей для отображения OTP. По причине синхронизации времени OTP через определенное время автоматически меняется и дисплей будет отображать OTP для текущего времени. Эти токены тоже,

как и другие могут быть украдены, потеряны и испорчены. Кроме того, существует возможность перезарядки (поменять батарейки).

Однако, существует и программные виды токенов, которые не имеют проблемы, связанные с зарядкой их. Программные виды токенов в основном предназначены для мобильных телефонов, по необходимости может быть и существуют и для персональных компьютеров. Данный вид частных токенов может выполнять аналогичные функции с токенами основанными на устройств, по при этом из-за использования вычислительных ресурсов третей стороны (мобильные устройства) степен безопасности низкая. Явными примерами для таких средств можно привести Google Authenticator или Microsoft Authenticator OTP приложений.

3. Веб-основанные методы. В настоящее время методы передачи OTP, которые предоставляются со стороны провайдеров не требует добавочных токенов и устройств. Данный метод основывается на способность распознавания заранее выбранных изображений, которые предоставляются с случайными. Пользователь сначала выбирает секретную группу (животные, машины, цветы и т.д.) при регистрации. В процессе проведения аутентификации система предлагает выбрать из случайных изображений (обязательно, среди случайно формированных изображений будет существовать изначально выбранные тоже). У каждого предоставленного изображения на заднем фоне, находиться неповторимая цифра. Со стороны пользователя указывается изначально выбранные изображения среди случайных и на основе полученных цифр из заднего фона изображения формируется OTP [14].

Кроме того, в системе OTP основанная на вебе, которая разработана со стороны компании Confident Technologies, при проведении аутентификации на мобильный телефон отправляется ссылка, позволяющая открыть изображения для выбора соответствующего. Когда производиться обращение к данной ссылке из открывшегося окна пользователь выбирает необходимых изображений и таким образом генерируется OTP [11].

4. Напечатанные на бумаге. В некоторых странах одноразовые пароли используются для удалённого использования банков. В некоторых из этих систем банк посылает пользователю, пронумерованный список одноразовых паролей, напечатанный на бумаге. Иногда пользователям даются карты в виде пластиковых карт и требуется выключение для определения OTP. Обеих случаях существующие OTP могут применятся случайно или последовательно по требованию банка. В Германии, Бразилии и Австрии эти OTP обычно называют TAN-кодом (Transaction authentication numbers). Некоторые банки отправляют TAN-коды пользователю с помощью SMS, и в этом случае они называются mTAN-коды (от «mobileTANs») [13].

Таблица 3

Анализ методов передачи OTP

Метод передачи OTP/ Свойства	Через мобильный телефон (SMS)	Личный токены (в виде устройства)	Личные токены (в виде программы)	Методы, основанные на вебе	Напечатанные на бумаге	Отправка с помощью почты
Недостаток	Требует мобильного устройства	Постоянно имеет при себе, высокая стоимость, ограниченный период работы	Требует мобильного устройства	Требует сохранить памяти	Постоянно имеет при себе	Знание пароля почтовой системы
Преиму-щества	Удобства пользования, низкая стоимость	Удобства пользова-ния, высокая безопасность	Средняя стоимость, неограниченный период работы	Не требует личных устройств, низкая стоимость	Не требует личных устройств, низкая стоимость	Не требует личных устройств, низкая стоимость
Проблемы безопасности	Небезопасность систем мобильных устройств, небезопасность среди передачи SMS	Постоянное безопасное хранения и иметь при себе	Небезопасность систем мобильных устройств	Небезопасность систем мобильных устройств (если применялся)	Постоянное безопасное хранения и иметь при себе	Не постоянное безопасное хранения учетной записи почтовой системы
Существующие атаки	Физический контроль устройства, слушание мобильной сети, атаки на основе вредоносных программ, атака “просмотр через плечо”	Не полное безопасность из-за потери или утери, атака “просмотр через плечо”	Атаки на основе вредоносных программ, спуфинг атаки, атака “просмотр через плечо”	Спуфинг атаки, атака “просмотр через плечо”	Фишинг, атака “человек в середине”, утеря, атака “просмотр через плечо”	Спуфинг атаки, атака “человек в середине”, атака “просмотр через плечо”
Примеры	Telegram, WhatsApp	SecurID	Google Authenticator	Confident Multi-Factor-Authentication[11]	Классик TAN	SmartSign [12]

5. Отправка с помощью почты. Почти во всех системах двух факторной аутентификации генерированные OTP отправляются на электронную почту пользователя. В частности, SmartSign продукт, разработанный компанией Microcosm для передачи OTP используют электронную почту пользователя [12].

Сравнительный анализ методов передачи OTP приведена в 3 таблице. Хот и является наиболее удобным метод передачи с помощью SMS или почта, из-за недостаточной защищенности сети передачи не может обеспечит высокий уровень безопасности [10]. Использование токенов в виде устройства обеспечивает высокий уровень безопасности, но и имеет ограниченный период использования и высокий стоимость. Токены в виде программного средства характеризуются такими преимуществами, как удобностью применения, низкая цена и не имеют проблемы с питанием. Однако из-за небезопасности среди мобильных устройств и существования много вредоносных программ, существует возможность проведения атак против них. Напечатать на бумаге OTP хот и не требует лишних затрат, но всегда требует безопасного сохранения и позволяет реализовать множества атак при процессе использования.

Методы передачи генерированного OTP на основе SMS и почты широко применяются в финансовой сфере (в банках) и личных целях, а в узкой деятельности целесообразным является использовать методов основанные на токены [10].

В результате анализа существующих методов генерации OTP и передачи их были получены следующие выводы:

1. Приветствуются со стороны пользователей применение OTP отправленные с помощью SMS или почты.
2. OTP передаваемые с помощью SMS или почты не защищены.
3. OTP основанные на вебе являются стойкими для атак “человек в середине”, “просмотр через плечо” и различных вредоносных программ.
4. При передаче OTP с помощью токенов в виде программы или в виде SMS требуется создать безопасную среду в мобильном устройстве.
5. Ряд паролей, созданных из генераторов OTP не имеют высокой случайностью.

В следующих научное работе приводиться данные по решению приведенных проблем и недостатков.

Использованная литература

[1] L. Lamport, “Password Authentication with Insecure Communication”, In: Comm. ACM, vol. 24, No 11, 1981, pp. 770-772.

[2] Takasuke TSUJI. A One-Time Password Authentication Method. Master’sthesis. January 31, 2003.

[3] M.Sandirigama, Shimizu A., Noda M. T. Simple and secure password authentication protocol (SAS) //IEICE Transactions on Communications. – 2000. – Т. 83. – №. 6. – С. 1363-1365.

[4] Lin C. L., Sun H. M., Hwang T. Attacks and solutions on strong-password authentication //IEICE transactions on communications. – 2001. – Т. 84. – №. 9. – С. 2622-2627.

[5] T. Kamioka. The examination of the security of SAS one-time password authentication //IEICE Technical Report. – 2001. –Т. 435. – С.53-58.

[6] Jo H. S., Youn H. Y. A secure user authentication protocol based on one-time-password for home network //International Conference on Computational Science and Its Applications. – Springer, Berlin, Heidelberg, 2005. – С. 519-528.

[7] N.HallerBellcore, “The S/KEY One-Time Password System”, Network Working Group, February 1995.

[8] T. Tsuji, T. Kamioka, and A. Shimizu, “Simple and secure password authentication protocol, ver.2 (SAS-2)”, IEICE Technical Report, OIS2002-30, vol.102, no.314, September 2002.

[9] Dmitrienko A. et al. Security analysis of mobile two-factor authentication schemes //Intel Technology Journal. – 2014. – Т. 18. – №. 4.

[10] De Cristofaro E. et al. A comparative usability study of two-factor authentication //arXivpreprint arXiv: 1309.5344. – 2013.

[11] http://confidenttechnologies.com/confident-multi-factor-authentication-demo/

[12] https://www.microcosm.com/products/smartsign/authentication-methods/email-otp

[13] https://www.commerzbank.de/portal/en/englisch/products-offers/services/secure-internet-banking/banking.html

[14] https://www.darkreading.com/risk/images-could-change-the-authentication-picture/d/d-id/1134705

[15] https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access/securid-hardware-tokens

[16] https://www.pymnts.com/news/security-and-risk/2017/o2-confirms-hack-that-wiped-out-german-customers-bank-accounts-mobile/

[17] https://tools.ietf.org/html/rfc4226

[18] https://tools.ietf.org/html/rfc6238

Каримов Маджит Маликович
Директор Государственный центр тестирования при кабинете министров Республики Узбекистан, д.т.н., профессор
Тел.: (+99871) 234-72-50
Эл. почта: m.karimov@tdtu.uz
Арзиева Жамила Тилеубаевна
Каракалпакский государственный университет,
Кафедра прикладной математики, ассистент
Тел.: (+99891)3992744
Эл. почта: jamka-1980@mail.ru
Худойкулов Зариф Туракулович
PhD, заведующие кафедры «Криптология», ТУИТ
Тел.: (+99897) 729-60-47
Эл. почта: zarif.xudoyqulov@mail.ru

Karimov M.M., Arziyeva J.T., Khudoykulov Z.T.

Analysis of authentication method based on one-time passwords

In this article, methods of one time password generation and delivery it to users are analyzed. Even majority one-time password based authenticators are time-based; it caused problems in security and performance since possibility of knowing time stamp and changing while it is being entered. Even SMS based one-time password delivery methods is most common one, messages that is plaintext form and insecurity of mobile environment are causes serious problems. Besides that, onetime password based authentication methods in current works, did not provide security against man-in-the middle attack and shoulder face attacks.

Keywords: One Time Password (OTP), DOS-attack, Lemport scheme, HOTP (An HMAC-Based One-Time Password Algorithm), TOTP (Time-Based One-Time Password Algorithm), TAN-code (Transaction authentication numbers).