УДК 621.382

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

Атаки направленные на методы аутентификации по паролю

Аннотация. В данной статье приведены результаты анализа атак, направленные на методы аутентификации, основанные на паролях. Кроме того, приведены необходимые мероприятия и подходы для предотвращения рассмотренных атак. В результате анализа обосновано, что атаки направленные на методы аутентификации, основанные на паролях, фокусируются на процесс аутентификации и на определение пароля. Также определена высокая эффективность использования одноразовых паролей для предотвращения многих существующих атак, направленных на методы аутентификации.

Ключевые слова: пароль, аутентификация, атака, одноразовый пароль, spoofing, «человек по середине», «браузер в середине (Man-In-The-Browser attack).

Использование открытых каналов при передачи данных создаёт потенциальные возможности для злоумышленных действий. Поэтому, одна из основных задач обеспечения информационной безопасности это использование методов и средств, функционирующих для взаимодоверия сторон. Для предотвращения этих проблем используются специальные методы, позволяющие удостовериться в подлинности сторон.

Аутентификация – это процесс проверки подлинности пользователя, устройства или процесса, который произвел обращение, которая служит гарантией пользователя (устройства или процесса) в подтверждении того, за кого он себя выдает. При данной процедуре производится обмен данными определенного типа между пользователем и системой, который состоит из идентификатора, пользователя и информации, которую никто не знает (например, пароль или сертификат) [1].

Данная статья посвящена анализу существующих атак, направленных на методы аутентификации, а также предложены методы защиты для предотвращения существующих атак.

По той причине, что процесс аутентификации является важным процессом удостоверения подлинности прав доступа пользователей, он должен быть защищен от атак, которые направлены на получения персональных данных пользователей. Поэтому перед злоумышленником ставится цель - получить без разрешения данные пользователя, для чего он может воспользоваться разными методами. При этом атаки, нацеленные на методы аутентификации, которые основаны на знание чего-либо, можно разделит на две группы [2]:

- атаки, направленные на управления учетными записями;
- атаки, направленные на поиск пароля.

Атаки, направленные на управления учетными записями

Атаки данной группы характеризуют себя целенаправленностью непосредственно получить пароль. Существуют следующие атаки, которые относятся к данной группе:

– *Основанные на вредоносных программах*. Вредоносные программы — это любая не разрешенная программа, которая без разрешения пользователя устанавливается в системе. Основной целью является накопление конфиденциальной информации пользователя, и к этим программам относятся перехватчики информации, введенные с помощью клавиатуры (keylogger), регистрирующие движения мыши, копирующие текущее состояние экрана и копирующие из текущего состояния памяти.

В качестве примера можно привести ограбление около 3 миллионов информации учетных записей пользователей Индийской компании Zoho в 25 сентября 2018 года [3]. Для этого со стороны злоумышленников было использовано программное средство типа keylogger. Кроме того, в 2010 году в Великобритании впоследствии использования keylogger программы по имени Zeus было похищено около 31млн.$ денежных средств клиентов банка [4].

– *Основанные на атаках «спуфинга (spoofing)».* Спуфинг атаками являются действия злоумышленника, который выдаёт себя за другого и успешно маскируется для получения незаконных привилегий. Для реализации вышеприведенной атаки требуется инфицирование вредоносной программой компьютера «жертвы». Явными примерами таких атак является фишинг (Phishing) и фарминг (Pharming).

В фишинг атаках злоумышленник из своего (фиктивный) сервера отправляет «жертве» спам сообщение, состоящее из URL, который позволяет выполнить обращение к своему серверу. Через данный URL “жертве” предоставляется сервис, требующий конфиденциальную информацию (например, пароль и логин) пользователя. Таким образом, можно сказать что, фишинг атака является комбинированным видом социальной инженерии и атаки «человек по середине», целью которых является получение персональных данных пользователя. Причиной реализации данной атаки является уязвимость решения организованной аутентификации в целом, а не уязвимость метода криптографической аутентификации (например, протокол TLS/SSL) [16, 18].

Самыми крупными фишинг атаками 2018 года, которые были направлены на ограбление почтовых данных (логин и пароль) являются “MailChimp”, “Social Network”, “Account Verification”, “ICO”, “Tax W2” и “Gmail Scam”. В частности, в результате фишинг атаки “ICO” для компании “Bee Token” ущерб составил 85 000$ США [5].

Фарминг используют для обманного обращения “жертвы” на веб-сайт злоумышленника. При этом он применяет инфицированный сервис DNS-серверов. Для этого, изначально платформа пользователя инфицируется (например, случайно загрузив какие-то приложе-ния JavaScript и JavaApplet), и выполненные все обращения в данной платформе через ин-фицированный DNS перенаправляются на сайт злоумышленника.

Фарминг атака входит в тип, который приносит большой вред для компаний или организаций. В частности, в феврале 2017 году зафиксированы фарминг атаки на более 50 финансовых организаций США, Европы и Азии. В составе таких организаций банк Barclays, Шотландский банк, PayPal, eBay, Discover Card и American Express [5].

Атака «человек по середине». Данный тип атаки выполняется при передаче пароля в незащищенном виде через сеть. В данном случае злоумышленник перехватывает передающуюся информацию между

клиентом и сервером и на основе анализа контента может получить важные данные, такие как, пароль, логин, информацию или почтовые данные. Данная атака очень эффективна при использовании небезопасных протоколов аутентификации PAP или Telnet. Однако, существует возможность применения данной атаки на протоколы, у которых уровень безопасности выше (например, SSL/TLS).

Проведенные исследования показывают, что использование одних протоколов SSL/TLS недостаточно для защиты от атак “человек по середине”. Потому что во многих веб-серверах не использованы свойства HTTP Strict Transport Security (HSTS), который позволяет предотвратить атаки фишинг и «человек по середине» [6].

Атака повторения. В данном типе атак злоумышленник наблюдает процесс аутентификации легального пользователя и копирует все данные сеанса. Через определенное время на основе повторной отправки скопированных данных проходит успешную аутентификацию от имени настоящего пользователя. Данный вид атаки дает результат даже если использованные пароли были в хешированном виде.

Атака «браузер в середине (Man-In-The-Browser attack, MITB)». Данный вид атаки входит в тип Интернет атак, и очень похож н атаки «человек в середине», но отличает реализацией угрозы на платформе «жертвы». В MITB атаке вредоносный файл, целью которого является браузер, помещает себя между пользователем и браузером. Основной целью MITB атаки является создание или модификация финансовых транзакций онлайн банковских систем, таким образом, что ни пользователь и ни сервер провайдера сервиса не были информированы об этом. При этом атака не выполняется до того времени, пока сессия аутентификации не завершена. Данная атака может выполняться даже при использовании безопасных протоколов (например, SSL/TLS). Филип Гухринг привел 5 причин, которые приводят к реализации данной атаки [17].

1. Browser Helper Objects – в операционной системе Windows по причине загрузки со стороны Internet Explorer динамических библиотек (Dynamically Loaded Libraries, DLL), злоумышленник может обеспечивать полный контроль.
2. Extensions – данная причина отличается от первой тем, что она доступна для других браузеров, например, FireFox.
3. Скрипты пользователя (UserScripts) – загружаемые скрипты в браузер со стороны пользователя.
4. API-Hooking – данная атака выполняется между браузером и DLL файлом браузера (Extensions и DLL файлы операционной системы). Например, на основе данной атаки может быть модифицирована связь между браузером и ме-ханизмами заднего фона SSL при процессе протокола SSL.
5. Вертуализация – при загрузки операционной системы в виртуальной среде, будет возможным обход всех механизмов безопасности.

Для разных веб браузеров существуют различные вредоносные программы, нацеленные на реализацию MITB атаки. В частности, в ОС Windows созданные для веб-браузеров Internet Explorer и Firefox с помощью Agent.DBJP [7], Bugat [8], Carberp [9], Gozi [10] программ возможно выполнить MITB атаку.

Атака «Отказа в обслуживании (Denial of Service attack, DOS)». В результате данной атаки вместо попытки получения учетных записей пользователя, ставится цель сделать недоступными системы для пользования клиентами.

Обычно в методах аутентификации, основанных на паролях, в целях предотвращения атак, основанных на «Brute Force» и на основе словаря производится временное блокирование системы, если произведено несколько неудачных попыток атак. Другими словами, злоумышленник производит несколько неуспешных попыток от имени пользователя и после этого учетная запись блокируется. В данном случае, при правильном введении пароля в систему она не будет доступной пользователю.

Атаки, направленные на поиск пароля

В отличие от вышеприведенных типов атак, целью, данной атаки, направленной на поиск пароля является только определение пароля пользователя. Атаки, направленные на поиск паролей, основываются на гипотезе паролей, и восстановление при передачи или хранении. Самый распространенный вид - введение пароля случайным образом. Поэтому необходимо рассмотреть методы атак, относящиеся к данному типу.

Использование уязвимой криптографической системы. При использовании уязвимого криптографического протокола в процессе передачи паролей через сеть или в процессе сохранения возникает возможность определения пароля со стороны злоумышленника. Например, протоколы типа Telnet, из-за открытой передачи пароля пользователя возникают серьезные проблемы. Кроме того, недостаточное внимание на криптостойкость сохраненных хэш значений паролей приводит к увеличению вероятности определения паролей.

Атака, основанная на гипотезе. Обычно пользователи избегая проблемы хранения пароля в памяти стараются использовать персональную информацию в качестве пароля. При этом они используют такие данные, как номер телефона, дата рождения, и другую персональную информацию. При проведении данной атаки злоумышленник для получения персональных данных «жертвы» пользуется способами социальной инженерией.

Атака, основанная на словаре. Данный метод определения пароля основывается на вероятности. При этом у злоумышленника существует список широко распространенных паролей, которые он будет использовать по очереди. Из-за использования пароля одного типа со стороны многих пользователей, данная атака в многих случаях реализуется успешно.

Каждый год во всем мире объявляется список паролей, которые очень часто применяются со стороны группы хакеров или организаций занимающийся анализом. 2018 году на основе представленных данных со стороны организации SplashData в высшую пятерку самых распространенных паролей входят следующие: “123456”, “password”, “123456789”, “12345678” и “12345” [11].

Атака «Полный перебор». В данном типе атак рассматриваются все комбинации пароля, которые возможны. При этом основными факторами являются длина пароля и тип использованных символов. Увеличение возможных символов и длины пароля приводит к снижению вероятности реализации данной атаки. Поэтому данный тип атаки широко применяется для определения паролей с малой длиной. Кроме того, применяются параллельные вычисления для сокращения времени на вычисления всех комбинаций паролей. Атака “Полный перебор” делится на офлайн и онлайн. Если злоумышленник реализует атаку не связываясь с защищенным ресурсом, то это офлайн атака, в обратном случае это онлайн атака. Предотвратить онлайн атаки “Полный перебор” легко, так как их можно просто

блокировать, если количество неуспешных попыток входа больше обычного.

Атаки, основанные на предварительной вычислении. В данном типе атак каждый пароль из словаря сохраняется со своим значением хэш-функций и кроме того, формируется таблица, состоящая из двух колонок, в каждую из которых вводится пароль и хэш значение соответственно. Если введено новое хэш значение, то в соответствие колонке хэш значения определяется пароль из соответствующей колонки. Данный вид атаки предотвращает от вычисления случайным образом.

Для предотвращения данной атаки необходимо обеспечить различность хэш значений, которые были сгенерированы. Для этого используется значения случайного ряда, которые называются «соль (salt)». По данному методу для каждого пароля генерируется «соль» значение и в случае объединения его с паролем, они хэшируется. В базе паролей сохраняется хэш значение и соответствующий «соль».

Данный метод усложняет реализацию атак, основанных на предварительном вычислении. Другими словами, не зная значения «соль», бесполезно вычислять хэш-значение пароля. В результате этого резко снижается эффективность реализации атаки предварительного вычисления, с практической точки зрения.

Существует множество средств для реализации данной атаки и среди них широко применяется следующие: RainbowCrack [12], Aircrack-ng [13], John the Ripper [14]. В частности, значения, полученные от LM, NTLM, MD5 и SHA1, хэш функций паролей различной длины и символов, предварительно сгенерированных с помощью средства RainbowCrack [15].

Атака «просмотр через плечо». Целью данной атаки является получения учетных записей пользователя непосредственно наблюдением введения данных или посредством записей из камеры. Данный тип атаки зависит от средств процесса и применения, так как они определяют эффективность атак.

В общем можно изобразить классификацию атак, направленных на методы аутентификации, основанные на знании чего-либо, как приведено на рисунке 1.

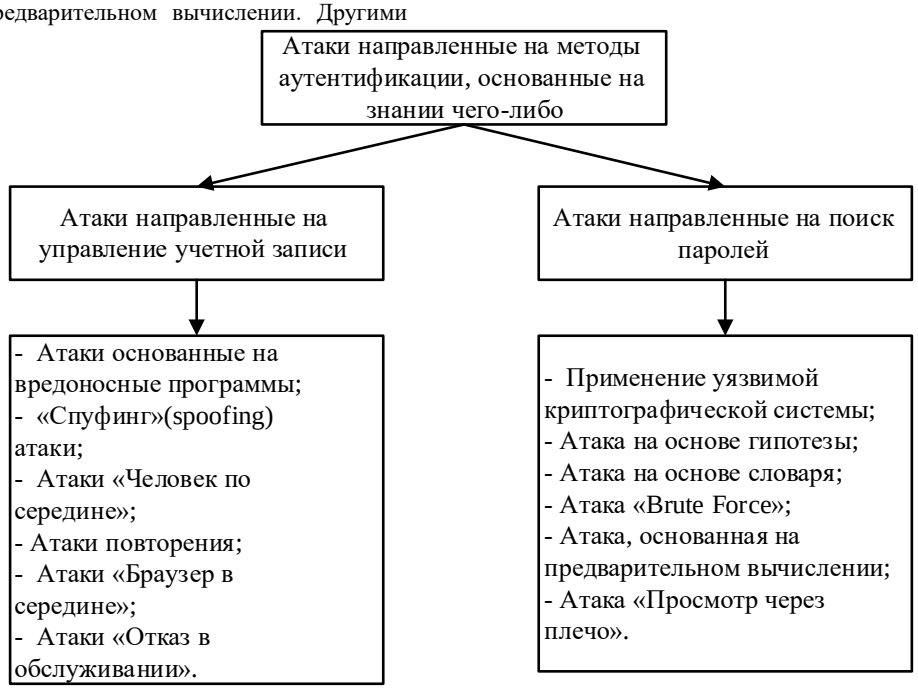

Рис.1. Классификация атак, направленных на методы аутентификации, которые основаны на знании чего-либо

Не существует определенного одного метода предотвращения атак, направленных на методы аутентификации, которые основаны на знании чего-либо. Потому что, при таких обстоятельствах квалификация злоумышленника, количество ущерба в соответствии с используемой средой, средствами и уровнем риска бывают разными. В таблице 1 приведены методы и мероприятия необходимые для предотвращения атак, направленных на методы аутентификации, основанные на знание чего-либо.

Таблица 1

Виды атак и методы противодействия им

№	Виды атак	Методы предотвращения атак
	Атаки, направленные на управления учетных записей	
1.	Атаки, направленные на вредоносные программы	Установление защиты против вредоносных программ, использование OTP.
2.	«Спуфинг» (spoofing) атаки	Применение аутентификации (OTP), которая не является статической.
3.	Атака «Человек по середине»	Применение шифрованных каналов связи.
4.	Атака повторения	Применение шифрования и случайной метки значение/время.
5.	Атака «браузер в середине»	Проведение аутентификации на уровне транзакции.
6.	Атака «отказ в обслуживании»	Комплекс мероприятий.
	Атаки, направленные на поиск пароля	
1.	Применение уязвимой криптографической системы.	Применение стойких криптографических хэш функций.

№	Виды атак	Методы предотвращения атак
2.	Атака на основе гипотезы	Использование OTP
3.	Атака на основе словаря	Автоматическое блокирование, ограничение неудачных попыток, применение «соль».
4.	Атака «Brute Force»	Использование многофакторной аутентификации, систем CAPTCHA и технологий «доверенный адрес».
5.	Атаки, основанные на предварительное вычисление.	Применение OTP, многофакторной аутентификации или «соль».
6.	Атака «Просмотр через плечо»	Применение графических паролей, OTP.

Заключение

Приведенные методы, которые направлены на предотвращение атак на методы аутентификации, основанные на знание чего-либо, не обеспечивают полную защиту. Но из приведенных методов аутентификации, основанных на OTP (One time Password) отличаются от других своей стойкостью к существующим атакам.

Использованная литература

[1] Shangin V. F. Informasionnaya bezopasnost kompyuternых sistem i setey: ucheb. Posobiye. — M.: ID «FORUM»: INFRA-M, 2011. — 416 s.

[2] Alzomai M.H. Identity management: strengthening one-time password authentication through usability: dis. – Queensland University of Technology, 2011.

[3] https://blog.360totalsecurity.com/en/hackers-use-keyloggers-to-steal-the-information-from-3-million-zoho-users/

[4] Hackers infected thousands of PCs with Zeus trojan to steal millions, http://news.techworld.com/security/3241594/police-arrest-gang-behind-20-million-online-bank-fraud/

[5] https://www.adaware.com/blog/50-banks-in-pharming-attack

[6] https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-mitm-attacks.html

[7] https://www.computerworld.com/article/2518665/trojan-writers-target-u-k--banks-with-botnets.html

[8] https://www.techworld.com/news/security/zeus-not-the-only-bank-trojan-threat-users-warned-3243894/

[9] https://www.techworld.com/news/security/facebook-users-targeted-in-carberp-man-in-browser-attack-3330728/

[10] https://www.securityweek.com/evolution-proxy-trojans

[11] https://www.teamsid.com/100-worst-passwords/

[12] http://project-rainbowcrack.com/

[13] http://www.aircrack-ng.org/

[14] http://www.openwall.com/john/

[15] http://project-rainbowcrack.com/table.htm

[16] A. Josang, P.M. Mollerud and E. Cheung. Web Security: The Emperors New Armour. In Proceedings of the Europian Conference of Information Systems (ECIS2001), Bled, Sloveniya, June 2001.

[17] Philipp Guhring. Concepts against Man-in-the-Browser Attacks. White paper: http://www.cacert.at/svn/sourcerer/CAcert/SecureClient.pdf

[18] Mohammad Mannan and P.C. van Oorschot. Security and usability: the gap in real-world online banking. In Proceedings of the 2007 Workshop on New Security Paradigims, NSPW'07, pages 1-14, New York, NY, USA, 2008. ACM.

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.
Attacks on Password Based Authentication Methods

Annotation. In this paper is given analysis of attacks on password based authentication methods. Furthermore, methods and approaches to prevent these attacks are described. Based on analysis result, attacks against password based authentication methods focus on authentication process and password guessing. One time password can used as countermeasure against majority of attacks on password based authentication.

Keywords: password, authentication, attack, one-time password, spoofing, "man in the middle", "Man-In-The-Browser attack".