УДК 004

И. А. Заярная, А. Р. Петрич
Новороссийский филиал ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации», Новороссийск, e-mail: aiamsem@mail.ru

АУТЕНТИФИКАЦИЯ: ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ

Ключевые слова: аутентификация, уязвимость, риски.

В последнее время наблюдается активизация процессов информатизации общества, что демонстрируется появлением большого количества вед- сервисов, ростом численности участников электронных коммуникаций, осуществляющих различные операции в сети Интернет, спектр которых включат поиск информации, рекламу товаров и услуг, финансовые операции и т.д. Для оказания услуг населению в рамках государственного управления экономикой создаются электронные правительства. Поскольку доверие к подобным веб-службам должно быть наивысшим необходимо формирование усиленной степени защиты пользователей. Мошенничество представляет серьезную опасность участникам электронных коммуникаций. Имеются примеры разработки и применения технологий изготовления муляжей биометрических признаков индивида. Благодаря этим технологиям злоумышленники совершают криминальные преступления, что является вполне вероятностным событием и вопросом соответствующей ситуации. В связи с обозначенной проблемой мошенничества защита пользователей электронных коммуникаций становится весьма актуальной задачей. При этом защита рассматривается в смысле сохранения конфиденциальности и целостности сведений о пользователях, а также выявлении степени доступности информации, для снижения негативных последствий, которые возможны в случае возникновения риска мошенничества. В числе методов защиты можно назвать аутентификацию. Основной целью аутентификации пользователя информационной системы является снижение угроз безопасности, а именно нарушение конфиденциальности и целостности информации. Несанкционированный доступ – один из самых распространенных видов нарушений, представляющий непосредственную угрозу работоспособности системы. Аутентификация используется для доступа к социальным сетям, электронной почте, интернет магазинам, интернет–банкингу, платежным системам и т.д. В данной статье рассматриваются теоретические аспекты такого понятия, как аутентификация. Синтезируя общие представления о аутентификации, встречающиеся в научной литературе, авторы статьи раскрывают смысл названной категории, представляют факторы и классификационные категории аутентификации и демонстрируют способы применения группы методов аутентификации для защиты информации путем установления истинности утверждения об идентичности чего-либо или кого-либо.

I. A. Zayarnaya, A. R. Petrich
Financial University affiliated to the Government of the Russian Federation,
Novorossiysk, e-mail: aiamsem@mail.ru

AUTHENTICATION: THEORETICAL ASPECTS

Keywords: authentication, vulnerability, risks.

Recently, there has been an intensification of the processes of informatization of society, which is demonstrated by the emergence of a large number of ved-services, an increase in the number of participants in electronic communications, carrying out various operations on the Internet, the spectrum of which will include information search, advertising of goods and services, financial transactions, etc. Electronic governments are being created to provide services to the population within the framework of state management of the economy. Since the trust in such web services must be the highest, it is necessary to form an increased degree of protection for users. Fraud poses a serious danger to participants in electronic communications. There are examples of the development and application of technologies for manufacturing dummies of biometric features of an individual. Thanks to these technologies, attackers commit criminal offenses, which is a completely probable event and a question of the corresponding situation. In connection with the identified problem of fraud, the protection of users of electronic communications becomes a very urgent task. At the same time, protection is considered in the sense of maintaining the confidentiality and integrity of information about users, as well as identifying the degree of availability of information in order to reduce the negative consequences that are possible in the event of a risk of fraud. Authentication is one of the security methods. The main purpose of information system user authentication is to reduce security threats, namely the violation of the confidentiality and integrity of information.Unauthorized access is one of the most common types of violations that poses a direct threat to system performance. Authentication is used to access social networks, e-mail, online shopping, online banking, payment systems, etc. This article discusses the theoretical aspects of such a concept as authentication. Synthesizing the general ideas about authentication found in the scientific literature, the authors of the article reveal the meaning of the named category, present the factors and classification categories of authentication, and demonstrate how to use a group of authentication methods to protect information by establishing the truth of a statement about the identity of something or someone.

Введение

С развитием цифровой экономики и повышением активности участников электронных коммуникаций к числу высокозначимых аспектов функционирования информационных систем можно аутентификацию пользователей, позволяющей разграничивать права доступа пользователей к системе и определять, действительно ли данные пользователи являются теми, за кого себя выдают.

Аутентификация дает возможность осуществлять контроль доступа к индивидуальной информации пользователя, что можно признать основой для формирования и реализации политики безопасности как в рамках домашнего хозяйства или отдельно взятой фирмы, так и в государственных масштабах.

Поскольку в настоящее время существуют риски мошеннических операций с использованием индивидуальных данных участников электронных коммуникаций, которые оказались в руках злоумышленников, исследование в области аутентификации являются актуальными.

Целью данной статьи является исследование теоретических аспектов аутентификации.

Материалы и методы исследования

В процессе исследования применены такие методы исследования как анализ информации, её изучение, классификация и обобщение, метод индукции используется для выделения наиболее важных характеристик объекта.

Результаты исследования и их обсуждение

Аутентификация – это процесс проверки личности данного пользователя или клиента. Другими словами, это включает в себя проверку того, действительно ли это те люди, за кого себя выдают. По крайней мере частично, веб-сайты доступны любому, кто подключен к Интернету Таким образом надежные механизмы аутентификации являются неотъемлемым аспектом эффективной веб-безопасности.

Существует три фактора аутентификации, по которым можно классифицировать различные типы этой категории:

- что-то, что человек знает, например, пароль или ответ на секретный вопрос. Их иногда называют «факторами знаний».

- что-то, что у есть у человека, то есть физический объект, такой как мобильный телефон или токен безопасности. Их иногда называют «факторами владения».

- что-то, чем является человек или что он делает, например, его биометрические данные или модели поведения. Их иногда называют «факторами инерции».

Ученые выделяют несколько способов использования аутентификации [4]:

1. Подтверждение личности пользователя.

Одной из самых больших угроз в современном мире кибербезопасности является кража личных данных. Традиционного имени пользователя и пароля больше недостаточно для защиты ваших данных и учетных записей от киберпреступников.

2. Соблюдение требований соответствия.

Помимо сохранения репутации компании, защита потребительских данных требуется многими нормативными актами по соблюдению требований в области ИТ. Например, стандарт PCI, или PCI DSS, требует, чтобы любой бизнес, обрабатывающий данные кредитных карт, должен был идентифицировать и аутентифицировать доступ к компонентам системы. Многофакторная аутентификация – это простой и высокоэффективный способ контроля доступа к конфиденциальным данным, таким как платежная информация.

3. Использование решений для единого входа (SSO).

Многие решения аутентификации совместимы с SSO. Вместо создания уникальной комбинации имени пользователя и пароля для каждой учетной записи можно использовать одну учетную запись единого входа с многофакторной аутентификацией, чтобы упростить доступ для авторизованных пользователей без ущерба для безопасности. Это может сэкономить время при одновременной проверке личности пользователя при попытке входа в систему

Механизмы аутентификации полагаются на целый ряд технологий для проверки одного или нескольких из этих факторов.

Аутентификация – это процесс проверки того, что пользователь действительно является тем, за кого себя выдает, в то время как авторизация предполагает проверку того, разрешено ли пользователю что-либо делать.

В контексте веб-сайта или веб-приложения проверка подлинности опреде-

ляет, действительно ли кто-то, пытающийся получить доступ к сайту с именем пользователя «Carlos123», является тем же человеком, который создал учетную запись.

Как только «Carlos123» проходит аутентификацию, его разрешения определяют, имеет ли он право, например, получать доступ к личной информации о других пользователях или выполнять такие действия, как удаление учетной записи другого пользователя [1].

Несмотря на, казалось бы, безупречную защиту пользователя, аутентификация имеет ряд уязвимостей, которые могут понести за собой серьезные риски как для сайта, так и для пользователей. Механизмы аутентификации слабы, поскольку они не обеспечивают адекватной защиты от атак методом перебора.

Так, например, логические недостатки или плохое кодирование в реализации позволяют злоумышленнику полностью обойти механизмы аутентификации. Это иногда называют «нарушенной аутентификацией».

Во многих областях веб-разработки логические ошибки просто приводят к неожиданному поведению веб-сайта, что может быть проблемой безопасности, а может и не быть. Однако, поскольку аутентификация настолько важна для безопасности, вероятность того, что некорректная логика аутентификации подвергает веб-сайт проблемам безопасности, явно повышена [2].

Последствия уязвимостей аутентификации могут быть очень серьезными. Как только злоумышленник либо обошел проверку подлинности, либо взломал учетную запись другого пользователя, он получает доступ ко всем данным и функциям, которые есть у скомпрометированной учетной записи. Если им удастся скомпрометировать учетную запись с высокими привилегиями, например, системного администратора, они могут получить полный контроль над всем приложением и потенциально получить доступ к внутренней инфраструктуре [3].

Большинство угроз, связанных с процессом аутентификации, связаны с паролями и методами аутентификации на основе паролей. Но нарушенная аутентификация также приводит к значительному количеству уязвимостей. Нарушенная аутентификация возникает, когда реализация процесса аутентификации имеет недостатки. К сожалению, обычно это трудно обнаружить, и это может быть более серьезным, чем риски, связанные с паролями [6].

Ниже перечислены основные источники рисков, которые порождают общие векторы атак при слабой аутентификации.

1. Уязвимая логика аутентификации.

2. Слабый процесс восстановления учетной записи/ пароля.

3. Использование уязвимой библиотеки аутентификации.

4. Небезопасная обработка сеансов.

5. Отсутствующие ограничители скорости и процесс блокировки

6. Небезопасная двухфакторная аутентификация [7].

В то время как некоторые уязвимости, такие как слабые пароли и известные уязвимые библиотеки зависимостей, легко использовать, использование логических недостатков является более сложной задачей и требует ручного процесса атаки. Но самым значительным риском может быть просто обман пользователей, заставляющий их выдавать свои учетные данные. Их можно классифицировать как векторы атак, наиболее часто используемые для компрометации процесса аутентификации, двумя способами [5]:

1. Компрометация паролей: Фишинг – это популярный противоборствующий метод, позволяющий обманом заставить пользователей выдавать учетные данные, такие как пароли и PIN-коды, и является одним из самых мощных векторов атак. Фишинг имеет более высокий процент успеха, чем многие другие векторы атак, что объясняет его популярность. Аналогичным образом, методы взлома паролей методом грубой силы не менее популярны. Атаки на основе словаря и атаки с использованием радужных таблиц также являются распространенными методами взлома паролей.

Ручная эксплуатация логических недостатков: Ручная эксплуатация включает в себя перехват необработанных HTTP-запросов и ответов и злонамеренное манипулирование перехваченными данными для использования логических недостатков.

2. SQL-инъекция: SQL-инъекция включает в себя вставку необработанных SQL-запросов, которые могут извлекать данные, не прошедшие проверку подлинности, несанкционированные данные или даже изменять логическое поведение приложения. В контексте проверки подлинности внедре-

ние SQL может привести к утечке учетных данных, хранящихся в базе данных, или повлиять на логику проверки подлинности, позволяя злоумышленнику входить в систему без проверки подлинности. Узнайте больше о том, как работает атака с использованием SQL-инъекций.

Хотя пароли и методы аутентификации на основе паролей вызывают большинство уязвимостей и угроз, связанных с аутентификацией, логические недостатки и небезопасная реализация также вызывают множество проблем. Помимо упомянутых рисков и уязвимостей, важно отметить, что небезопасные действия сотрудников могут быть серьезной уязвимостью, связанной с процессом аутентификации. В конце концов, сотрудники являются самым слабым звеном, и векторы атак, такие как фишинговые атаки, предназначены для использования этой уязвимости.

Наиболее безопасным видом аутентификации является двухфакторная. Двухфакторная аутентификация добавляет еще один фактор аутентификации к обычному процессу входа в систему поверх вашего пароля, отсюда и название. Как только пользователь вводит свое имя пользователя и пароль, будет предложено ввести код, отправленный в виде текстового сообщения или электронной почты, а иногда и в виде push-уведомления на телефоне.

Существует четыре основных типа двухфакторной аутентификации, ранжированных в порядке эффективности:

1. Код текстового сообщения:

Наиболее распространенной формой двухфакторной оплаты является код, отправленный по SMS. Для этого не требуется приложение или даже смартфон, но требуется сотовая связь. Он прост в использовании и настройке, но двухфакторный обмен текстовыми сообщениями – наименее безопасный метод. Хакеры могут легко использовать слабые места в телефонных сетях для кражи двухфакторных кодов SMS. Поскольку SMS-сообщения не шифруются, текстовые сообщения также подвержены утечке. Кроме того, если ваш телефон потерян или украден, злоумышленник может запросить двухфакторный код и получить доступ к вашим учетным записям. Код текстового сообщения намного лучше, чем вообще не использовать двухфакторный код, но есть гораздо более безопасные варианты [4].

2. Приложение-аутентификатор:

Это работает аналогично текстовому сообщению, за исключением того, что придется установить приложение на смартфон. В любое время, когда пользователю понадобится двухфакторный код, его можно получить из своего приложения. Приложения-аутентификаторы даже работают в автономном режиме и не требуют подключения к мобильному телефону или Интернету. Существует множество приложений для проверки подлинности на выбор, таких как Authy, Duo и Google Authenticator. Разница здесь в том, что они отправляются по зашифрованному соединению, что делает практически невозможным для кого-либо украсть ваш двухфакторный код до того, как вы его используете.

3. Использование биометрических данных.

Использование лица, глаза или отпечатка пальца является распространенным способом разблокировки устройств, но он также все чаще используется веб-сайтами для проверки того, что пользователь тот, за кого себя выдает. Часто эти двухфакторные параметры на основе биометрии встроены в устройство, например компьютер или телефон, для сканирования лица или отпечатков пальцев.

4. Физический ключ безопасности:

Физический ключ безопасности считается самым надежным из всех методов двухфакторной аутентификации. Ключи безопасности часто выглядят как устройства размером с USB-накопитель, которые достаточно малы, чтобы поместиться на связке ключей. Возможно, он даже не понадобится, поскольку новые устройства Android и iPhone имеют встроенную аппаратную функцию. И фишинговые страницы не будут работать, потому что только законные сайты поддерживают ключи безопасности. Эти ключи предназначены для того, чтобы помешать даже самым умным и изобретательным злоумышленникам, таким как хакеры национальных государств. Собственные данные Google показывают, что с момента предоставления ключей безопасности своим сотрудникам у компании не было ни одного подтвержденного взлома учетной записи.

Есть несколько ключей безопасности на выбор: у Google есть своя программа расширенной защиты для пользователей с высоким уровнем риска, таких как политики и журналисты, и свой ключ Google Titan для

всех остальных. Но многие эксперты по безопасности скажут, что Yubikeys – это золотой стандарт ключей безопасности.

Однако есть несколько вещей, на которые следует обратить внимание. Еще не все сайты поддерживают ключи безопасности, но большинство крупных компаний поддерживают их – например, Microsoft, Google и др.

Заключение

Таким образом, аутентификация действует как первая линия защиты, предоставляя доступ к ценным данным только тем, кому это позволено. Многие организации признают это и используют многофакторную аутентификацию в качестве дополнительного уровня защиты для аутентификации. Обеспечение безопасности этого процесса абсолютно необходимо, поскольку в 2021 году 29% сетевых взломов были связаны с кражей учетных данных.

Многие специалисты в области безопасности испытывают трудности в своей области, потому что они знают, что злоумышленники имеют преимущество над сетевыми защитниками. Необходимо постоянно обновлять программное обеспечение для сетевой аутентификации, чтобы быть уверенным, что данные будут под защитой.

Библиографический список

1. Иванов В.В., Лубова Е.С., Черкасов Д.Ю. Аутентификация и авторизация // Проблемы современной науки и образования. 2017. № 2. С. 31-33.

2. Нелсон Н. Риски аутентификации, обнаруженные в платформе Okta // Threat post. июль 2019. [Электронный ресурс]. URL: https://threatpost.com/risks-okta-sso/180249/ (дата обращения: 06.08.2022).

3. Сакшам Ш. Наиболее Распространенные Уязвимости Аутентификации. февраль 2022. [Электронный ресурс]. URL: https://goteleport.com/blog/authentication-vulnerabilities/ (дата обращения: 06.08.2022).

4. Уиттакер З. Как двухфакторная аутентификация может защитить от взлома учетных записей // TechCrunch. декабрь 2018. [Электронный ресурс]. URL: https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/ (дата обращения: 06.08.2022).

5. Уязвимости аутентификации // PortSwigger. 2020. [Электронный ресурс]. URL: https://portswigger.net/web-security/authentication (дата обращения: 06.08.2022).

6. Уязвимости в многофакторной аутентификации // PortSwigger. 2020. [Электронный ресурс]. URL: https://portswigger.net/web-security/authentication/multi-factor (дата обращения: 06.08.2022).

7. Многофакторная (двухфакторная) аутентификация // Tradviser. июль 2022. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Многофакторная_(двухфакторная)_аутентификация (дата обращения: 06.08.2022).