УДК 004 **Технические науки**

Акушуев Рамазан Тахирович, *студент 3 курса по направлению «Информармационная безопансость», Донской государственный технический университет Россия, г. Ростов-на-Дону*

АУТЕНТИФИКАЦИЯ И ИДЕНТИФИКАЦИЯ КАК МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация: В данной работе рассматриваются вопросы, касающиеся особенностей аутентификации и идентификации, их смысл и применение, а так же о фальсификации личности и проверки личности.

Ключевые слова: информационная безопасность, аутентификаци, идентификация, методы защиты информации.

Annotation: This paper discusses issues related to the features of authentication and identification, their meaning and application, as well as the falsification of identity and identity verification.

Keywords: information security, authentication, identification, methods of information protection.

При разработке мер безопасности, будь то в масштабе конкретного механизма или всей инфраструктуры, идентификация и аутентификация, скорее всего, будут ключевыми понятиями. Идентификация-это утверждение о том, что такое кто-то или что-то, и аутентификация устанавливает, является ли это утверждение истинным. Мы можем видеть, что такие процессы происходят ежедневно самыми разнообразными способами.

Один очень распространенный пример идентификации и аутентификации транзакции можно найти в использовании платежных карт, которые требуют личного идентификационного номера. Когда проводим

магнитной полосой по карте, мы утверждаем, что мы-человек, указанный на карте. На этом этапе мы дали идентификацию, но не более того. Когда нам предлагают ввести PIN-код, связанный с картой, мы завершаем аутентификацию части транзакции [1].

Некоторые из методов идентификации и аутентификации, которые используем в повседневной жизни, особенно хрупки и в значительной степени зависят от честности и усердия тех, кто участвует в сделке. Многие такие обмены, включающие предъявление удостоверений личности, такие как покупка предметов, ограниченных теми, кто старше определенного возраста, основаны на теории, что предъявляемая идентификационная карта является подлинной и точной. Мы также полагаемся на то, что лицо или система, выполняющие аутентификацию, компетентны и способны не только выполнять акт аутентификации, но и точно обнаруживать ложные или мошеннические действия.

Можно использовать различные методы идентификации и аутентификации, от простого использования имен пользователей и паролей до специальных аппаратных маркеров, которые служат для установления нашей личности несколькими способами.

Идентификация

Идентификация, — это просто утверждение того, кто мы есть. Это может включать в себя то, кем мы утверждаем себя как личность, важно отметить, что процесс идентификации не предполагает какой-либо проверки или подтверждения личности, которую мы утверждаем. Эта часть процесса называется аутентификацией и представляет собой отдельную транзакцию.

Можно идентифицировать себя по нашим полным именам, сокращенным версиям наших имен, изображениям самих себя, прозвищам, номерам счетов, именам пользователей, удостоверениям личности, отпечаткам пальцев, образцам ДНК и огромному разнообразию других методов. К сожалению, за некоторыми исключениями, такие методы идентификации не являются уникальными, и даже некоторые из предположительно уникальных

методов идентификации, такие как отпечаток пальца, могут быть продублированы или подделаны во многих случаях.

То, кем мы себя называем, во многих случаях может быть элементом информации, подлежащим изменению. Например, наши имена могут меняться, как в случае женщин, которые меняют свою фамилию после вступления в брак, людей, которые по закону меняют свое имя на совершенно другое имя. Кроме того, мы вообще можем очень легко менять логические формы идентификации, как в случае с номерами счетов, именами пользователей и т. п. Даже физические характеристики, такие как рост, вес, цвет кожи и цвет глаз, могут быть изменены. Один из наиболее важных факторов, который необходимо осознать, когда мы работаем с идентификацией, заключается в том, что недействительное утверждение об идентичности само по себе не является достоверной информацией.

Проверка личности

Верификация личности — это шаг за пределы идентификации, но это все еще шаг до аутентификации. Когда просят предъявить водительские права, карточку социального страхования, свидетельство о рождении или другую подобную форму удостоверения личности, это обычно делается с целью проверки личности, а не аутентификации. Это грубый эквивалент того, что кто-то утверждает личность [2].

Так же можно проверить форму идентификации - паспорт—по базе данных, содержащей дополнительную копию информации, которую она содержит, и сопоставить фотографию и физические характеристики с лицом.

Верификация личности используется не только в наших личных взаимодействиях, но и в компьютерных системах. Во многих случаях, например, когда отправлют электронное письмо, предоставленная идентификация считается истинной, без каких-либо дополнительных шагов. Такие пробелы в безопасности способствуют огромному количеству спам-трафика, который видим.

Фальсификация идентификации

Методы идентификации подвержены изменениям. Как таковые, они также подвержены фальсификации. В то время как многие водительские удостоверения теперь имеют голограммы или штрих - коды, которые делают их более трудными для подделки. Постоянная борьба между мерами безопасности и преступниками происходит и в виртуальном мире. На несколько более зловещей ноте, такие фальсифицированные средства идентификации также используются преступниками и террористами для различных задач гнусного характера. Некоторые первичные средства идентификации, такие как свидетельства о рождении, также предоставляют возможность получить дополнительные формы идентификации, такие как карточки социального страхования или водительские права, тем самым усиливая ложную идентификацию.

Кража личных данных, основанная на фальсифицированной информации, является сегодня серьезной проблемой. Этот тип атаки, к сожалению, распространен и прост в исполнении. При минимальном объеме информации-обычно достаточно имени, адреса и номера социального страхования—можно выдать себя за кого - то в достаточной степени, чтобы во многих случаях действовать как этот человек. Жертвы кражи личных данных могут обнаружить, что кредитные линии, кредитные карты, автокредиты, ипотечные кредиты на жилье и другие операции были совершены с использованием их украденных личных данных.

Такие преступления облегчаются из-за отсутствия требований к аутентификации для многих видов деятельности, в которых мы участвуем. В большинстве случаев единственной проверкой, которая имеет место, является проверка личности. Этот процесс в лучшем случае представляет собой небольшое препятствие, и его можно легко обойти, используя фальсифицированные формы идентификации. Чтобы исправить эту ситуацию, стоит завершить процесс идентификации и идентификации людей, вовлеченных в эти транзакции, чтобы, по крайней мере, более убедительно доказать, что действительно взаимодействуем с теми людьми [3].

Вполне возможно отправить электронное письмо с адреса, который отличается от фактического адреса отправки, и эта тактика используется спамерами и атаками на основе социальной инженерии на регулярной основе. Видим те же проблемы во многих других системах и протоколах, которые используются ежедневно и являются частью функциональности интернета.

Аутентификация

Аутентификация-это, в смысле информационной безопасности, набор методов, которые используется для установления истинности утверждения об идентичности. Важно отметить, что аутентификация лишь устанавливает, правильно ли было заявлено утверждение об идентичности. Аутентификация не предполагает и не подразумевает ничего о том, что аутентифицируемая сторона может делать; это отдельная задача, известная как авторизация. Факторы

С точки зрения аутентификации существует несколько методов, которые можно использовать, причем каждый из них называется фактором. В рамках каждого фактора существует ряд возможных методов. Чем больше факторов используется, тем более позитивными будут результаты. Различные факторы-это то, что вы знаете (пароль), то, что вы есть (сканирование радужной оболочки глаза), что-то, что вы делаете (распознавание походки), и место, где вы находитесь (в определенном терминале).

То, что вы знаете, является очень распространенным фактором аутентификации. Это могут быть пароли, пин-коды, парольные фразы или почти любая информация, которую человек может запомнить. Чаще всего именнно эти данные и используются для входа в учетные записи на компьютерах. Это несколько слабый фактор, потому что если информация, от которой зависит фактор, будет раскрыта, это может свести на нет уникальность нашего метода аутентификации [4].

Библиографический список:

1. Советов Б.Я., Информационные технологии Высшая школа, 2009г.

2. Мельников В.П. Информационная безопасность и защита информации. 3-е изд. Академия. 2008г.

3. Грушо А.А., Применко Э.А., Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс лекций. 2000г.

4. Варлатая, С.К., Аппаратно-программные средства и методы защиты информации. 2007г.