ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ СИСТЕМ

INFORMATION SUPPORT SYSTEM

УДК 004

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Шибанов С.В., Карпушин Д.А.

Аннотация. Рассматривается понятие процесса аутентификации и его видов с целью исследовать современные методы аутентификации, применяемые в вычислительной технике. В качестве основных были выделены три типа аутентификации: аутентификация на основе знания чего-либо, на основе владения чем-либо и на основе биометрических характеристик. Приведены примеры выделенных типов аутентификации. Выявлены достоинства и недостатки каждого метода, приведены принципы работы каждого из методов, перечислены основные виды атак них, а так же предложены способы понижения уровня компрометации рассмотренных методов аутентификации. Выделены факторы, влияющие на выбор того или иного метода аутентификации, на основе которых сделаны выводы о применимости каждого из методов аутентификации. Многофакторные биометрические системы аутентификации на данный момент являются наиболее перспективными для организации доступа к информационным системам, как с точки зрения удобства, так и с точки зрения безопасности. Стоимость таких систем всё ещё является довольно высокой, поэтому решая вопрос о применении того или иного вида аутентификации необходимо руководствоваться не только соображениями безопасности, но и вопросом стоимости конечного решения.

Ключевые слова: аутентификация, пароль, токен, биометрия, нейронная сеть, компрометация.

COMPARATIVE ANALYSIS OF MODERN METHODS OF AUTHENTICATION

Shibanov S.V., Karpushin D.A.

Abstract. Considering the concept of authentication process and it's species to explore modern methods of authentication used in computing. Identified three general types of authentication: authentication by knowledge, authentication by ownership and authentication by characteristic. Considered examples of authentication methods. Identified advantages and disadvantages of considered authentication methods, given the principles of each method, types of attacks on them, also suggested methods of decreasing of compromise level for considered authentication methods. Considered factors which influenced on choice of particular method of authentication. Basing on it made conclusions of applicability of each authentication method. Multifactor biometric authentication systems are currently the most promising for the organization of access to information systems, both in terms of facilities and in terms of security. The cost of such systems is still fairly high, so when deciding on the use of a particular type of authentication should be guided not only security concerns but also the question of the cost of the final solution.

Keywords: Athentication, password, token, biometrics, neural network, compromising.

Введение

Процедура аутентификации придумана человеком очень давно и успешно используется по сей день. Важность процесса аутентификации в принципе неоспорима. Аутентификация – это процедура, позволяющая одной сущности проверить объявленные свойства другой [1]. Т.е. аутентификация позволяет одной сущности проверить, что вторая сущность является именно той сущностью, за которую себя выдаёт.

Первыми средствами аутентификации были голосовые пароли. Затем появились первые печати и замки. Сейчас же, в связи с бурным развитием вычислительной техники, процесс аутентификации проводится и в виртуальном пространстве, где он не потерял своей изначальной важности. Целью данной работы является исследование современных методов аутентификации, применяемых в информационных системах и автоматизированных системах управления, основанных на применении вычислительной техники.

Представление аутентификации

Современные методы аутентификации согласно [6] можно разбить на три больших семейства: аутентификация на основе знания чего-либо (парольная аутентификация); аутентификация на основе биометрических характеристик (биометрическая аутентификация); аутентификация на основе обладания чем-либо (основанная на применении т.н. «токенов»).

Парольная аутентификация – это аутентификация, основанная на знании некоторой секретной информации. В настоящее время данный вид аутентификации является самым распространённым в связке т.н. логином – идентификатором пользователя. Достоинством

данного метода аутентификации является то, что аутентификационная информация не хранится на материальном носителе, а находится в «голове» у пользователя. Это достоинство зачастую является главным недостатком – пользователь не хочет запоминать длинные и сложные последовательности символов, полагаясь в этом вопросе либо на какой-нибудь носитель информации, либо на выбор в качестве пароля осмысленных или простых данных, таких как дата своего рождения или кличка своей собаки. Отсюда и появляются основные методы атак на данный метод аутентификации. Это, во-первых, «социальная инженерия»: если в информационной системе есть возможность посмотреть подсказку к паролю, то злоумышленник этим непременно воспользуется, либо осмотрит рабочее место пользователя на предмет наличия «записки», содержащей пароль, либо попробует подобрать пароль со словарём, исходя из того, что пользователь мог полениться использовать сложный пароль [7]. В данном классе атак есть ещё одна интересная атака. Она основана на том, что пользователь пользуется не одной информационной системой, а несколькими, что в наше время не является редкостью. Атакующий подразумевает, что пользователь пользуется одним и тем же паролем во всех информационных системах. И, подобрав тем или иным способом пароль от одной из них, атакующий автоматически подбирает пароль к остальным. Ещё одним видом атаки является внедрение вирусов типа «троян» или «кейлоггер», которые крадут сохранённые пароли и перехватывают вводимые символы с клавиатуры соответственно. При работе в компьютерных сетях распространение получила атака типа *Man in the middle* – «Человек посередине». Данная атака основана на том, что между двумя абонентами или между клиентом и сервером возникает прослушивающий узел. Этот вид атаки относится не только к парольным системам аутентификации. Т.е. если канал связи не зашифрован – злоумышленник с лёгкостью может узнать логин и пароль пользователя.

Компания *SplashData* опубликовала список самых популярных паролей, используемых пользователям на сайтах [2]. Данные были получены из разнообразных источников, содержащих украденные файлы с паролями. Пятёрка самых популярных паролей в 2014 году: 123456, *password*, 12345, 12345678, *querty*. Согласно статистике, 80% инцидентов в области информационной безопасности связаны с компрометацией парольной защиты [9]. Существует множество рекомендаций по выбору паролей, разработанных как на уровне конкретной фирмы, так и на уровне государства, оформленных виде инструкций и стандартов.

В случае, когда пароль формируется генератором псевдослучайной последовательности символов, сложность пароля можно рассчитать с помощью понятия информационной энтропии, предложенного К. Шенноном. Под информационной энтропией понимается мера неопределённости информации. Информационная энтропия парольной системы определяется по формуле [3]:

$$H(A^*) = log_2|A|^n = n \cdot log_2|A|,$$

где $|A|$ – мощность используемого алфавита; n – длина пароля.

Полученное значение характеризует степень случайности пароля при его генерации. Например, при использовании в пароле только латинских символов в нижнем регистре (26) и длине пароля в 8 символов энтропия составит 37,6, а при использовании ещё и заглавных букв энтропия увеличится до 45,6. Отсюда следует, что стойкость пароля напрямую зависит от используемого при его генерации алфавита и от длины сгенерированного пароля.

Рис. 1. Простейший токен, отображающий сгенерированный пароль на дисплей

К сожалению, человеческий мозг устроен так, что ему довольно-таки трудно или неохотно запоминаются длинные, устойчивые пароли. Данную проблему попытались решить с помощью таких устройств, как токены.

OTP (*One-Time Passwords*) токен – это устройство (или программа), генерирующее одноразовые пароли для аутентификации конкретного пользователя (рис. 1, 2). В данном случае человек идентифицирует себя тем, что он имеет в своём распоряжении некий прибор [8]. В данном методе аутентификации решается

основная проблема классической парольной аутентификации: пользователю не нужно ничего запоминать – для каждой процедуры входа в систему используется новый пароль, генерируемый устройством. Если же для использования токена необходимо ввести пин-код – аутентификация превращается в многофакторную, что значительно уменьшает степень компрометации. Для генерации паролей в токенах используются хэш-функции или криптографические алгоритмы [4].

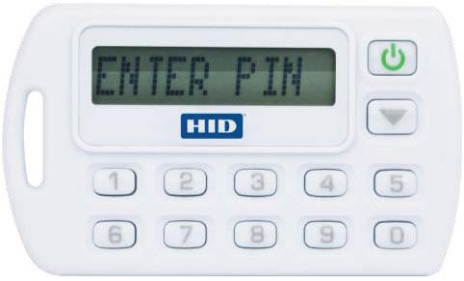

Рис. 2. Токен, защищённый пин-кодом

Тем не менее, как и в случае с парольной аутентификацией, сильная сторона данного метода так же является и самой слабой стороной. Если при использовании парольной аутентификации пароль (в идеальном случае) хранится в «голове» у пользователя, то здесь имеет место быть привязка к конкретному устройству или программе. Отсюда возникают и способы атаки на дынный вид аутентификации – банальная кража токена, с последующим применением реверс-инжениринга (с целью понять логику работы системы), либо не менее банальная аутентификация с помощью этого украденного токена, если он не защищён пин-кодом. Этой же «болезнью» страдают и альтернативные токенам системы аутентификации, основанные на применении смарт-карт или двухфакторной авторизации с паролем, высылаемым на мобильный телефон с помощью *SMS*. Ещё одним видом атаки на токены является обычный подбор пин-кода, защищающего токен от несанкционированного доступа, поскольку длина пин-кода обычно не превышает 4-6 символов. Следовательно, данный вид аутентификации является более удобным по сравнению с парольным. Уровень компрометации здесь зависит от внимательности и рассеянности пользователя, а так же от степени защищённости самого токена. Защитить токен можно путём превращения аутентификации в двухфакторную. Например, разместив на токене клавиатуру для ввода пин-кода или биометрического сканера отпечатка пальцев, которые будут использоваться для организации доступа непосредственно к самому токену.

Следующим видом аутентификации является биометрическая аутентификация. Биометрическая аутентификация – это аутентификация пользователя, осуществляемая путём предъявления им своего биометрического образа [5].

Классифицировать биометрические характеристики человека можно по-разному. Один из вариантов классификации разделяет биометрию на статическую и динамическую. В качестве статических (физиологических) биометрических характеристик применяются отпечаток пальца, форма лица, венозный рисунок руки, радужка и сетчатка глаза. В качестве динамических (поведенческих) биометрических характеристик применяются голос человека и его подпись. Различие между первым и вторым видом биометрических характеристик в том, что характеристики первого вида практически неизменны в течение всей жизни человека, а характеристики второго вида могут меняться по воле человека. Другой вид классификации – это разделение на открытую и закрытую биометрию. Открытая биометрия – это биометрия, доступная для всеобщего обозрения (н.р. радужная оболочка глаза, лицо, отпечаток пальца). Закрытая (тайная) биометрия – это биометрия недоступная для всеобщего обозрения (н.р. сетчатка глаза или венозный рисунок руки).

Биометрическая аутентификация работает следующим образом. На первом этапе специальное устройство (преобразователь некоторой физической величины) считывает определённую биометрическую характеристику человека (например – отпечаток пальца). Считанные данные в дальнейшем (после первичной обработки) формируют биометрический образ человека. Под первичной обработкой здесь понимается оцифровка биометрических данных и выделение из них вектора биометрических параметров, что в совокупности даёт нам на выходе биометрический образ человека. Полученный образ сопоставляются с образами, хранящимися в базе аутентификационных данных. Аутентификация считается успешной, если в

базе найден образ, очень близкий к введённому (при каждой процедуре аутентификации входные данные немного, но отличаются от эталонных, хранящихся в базе данных).

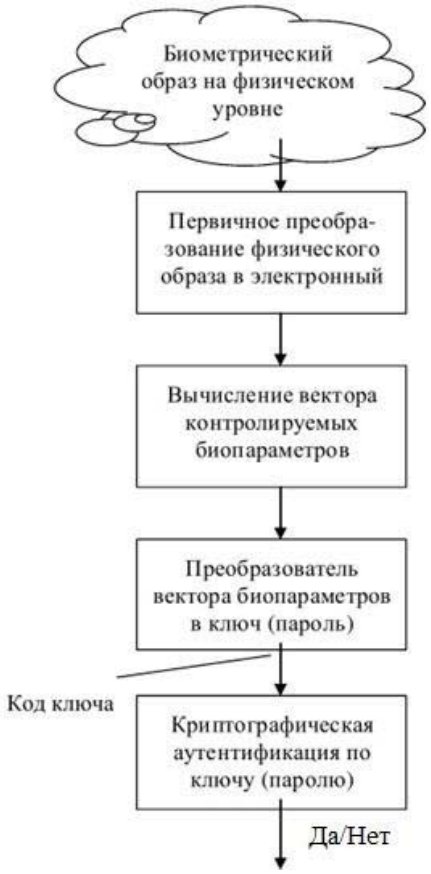

Рис. 3. Структурная схема обработки информации в средствах высоконадёжной биометрической аутентификации [5]

В системах высоконадёжной биометрической аутентификации применяется преобразователь биометрия-код (ПБК). Это преобразователь, предназначенный для преобразования вектора нечётких, неоднозначных биометрических параметров «Свой» в чёткий однозначный код ключа (пароля) [5]. В данном случае система генерирует на основе предоставленного биометрического образа некоторый «код», который можно использовать в информационной системе в качестве пароля. Схема работы обработки информации в системе с высоконадёжной биометрической аутентификацией представлена на *рис. 3*.

В нейросетевых преобразователях биометрия-код (НПБК) используется нейронная сеть, обученная таким образом, что при вводе биометрических данных «Свой» преобразователем будет предоставлен конкретный код, а в противном случае – набор случайных символов. Применение данных преобразователей снижает вероятность ошибок первого (отказ «своему») и второго (пропуск «чужого») рода. К тому же, при использовании НПБК, реализованных согласно пакету стандартов ГОСТ 52633, решается проблема обезличивания биометрии пользователей. В данном случае база аутентификационных данных представляет собой набор т.н. биометрических контейнеров, которые, по своей сути, являются набором значений весов нейронной сети, параметров и порядка преобразований, проводимых над данными, полученными в результате первичной обработки. Т.е. биометрия в «сыром» виде вообще отсутствует в информационной системе. В купе с шифрованием базы применение НПБК позволяет поддерживать уровень компрометации на достаточно высоком уровне.

На первый взгляд, системы биометрической аутентификации лишены недостатков, присущих парольным и основанным на использовании токенов систем аутентификации. Т.е. не нужно полагаться ни на свою память, ни на какой-либо носитель информации – пользователь сам по себе является носителем информации. Подделать открытый биометрический образ, принимая во внимание текущий уровень развития первичных преобразователей физической величины, с каждым годом становится всё труднее. А подделать закрытый биометрический образ без непосредственного сотрудничества (возможно, против своей воли) в принципе невозможно. Но и в данном методе аутентификации присутствуют свои недостатки. Первым недостатком является хрупкость человеческого тела. Не смотря на то, что биометрия является частью пользователя, она теряет смысл, если она испорчена (н.р. имеется значительный шрам на пальце или радужке глаза). Конечно, в распоряжении человека имеется два глаза и 20 пальцев и не так уж и страшно, если какой-то из них будет испорчен. Другим недостатком систем биометрической аутентификации является то, что человек, исходя из религиозных или каких-либо других соображений, не хочет предоставлять подобную информацию о себе. Данная проблема решается, как было описано выше, путём обезличивания данных, в т.ч. с применения НПБК.

Существует несколько типов атак на биометрические системы аутентификации. Они основаны либо на подделке биометрической черты, используемой при аутентификации, либо на перехвате данных в канале связи. Хорошим решением в плане безопасности является

применение биометрических токенов – токенов, в которых вопрос несанкционированного доступа решён с помощью биометрии, а не с помощью пин-кода. Во-первых, потому что налицо имеется многофакторная аутентификация (биометрия + устройство генерации одноразовых паролей). Во-вторых, потому что ключ (код), полученный из биометрии, не покидает доверенную вычислительную среду (токен).

Заключение

Основываясь на вышесказанном, можно сделать вывод, что многофакторные биометрические системы аутентификации на данный момент являются наиболее перспективными для организации доступа к информационным системам, как с точки зрения удобства, так и с точки зрения безопасности. Но стоимость таких систем всё ещё является довольно высокой [10], поэтому решая вопрос о применении того или иного вида аутентификации необходимо руководствоваться не только соображениями безопасности, но и вопросом стоимости конечного решения. К тому же, если информационная система используется для обработки персональных данных, то на неё налагается действие федерального закона РФ «О персональных данных» и связанных с ним нормативно-правовых актов и методических указаний ФСТЭК и ФСБ России, в которых классифицируются виды информационных систем и устанавливаются требования к обработке и защите персональных данных.

Список используемых источников

1. Мао, В. Современная криптография: теория и практика. / В. Мао. – М. : Издательский дом «Вильямс», 2005. – 768 с. – ISBN 5-8459-0847-7.
2. "123456" Maintains the Top Spot on SplashData's Annual "Worst Passwords" List [Электронный ресурс]: статья. – Режим доступа: http://splashdata.com/press/worst-passwords-of-2014.htm.
3. Марков, А. С. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов., А.В. Барабанов. – М. : Радио и связь, 2012. – 192 с. – ISBN 5-89776-015-2.
4. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие для вузов / А.А. Афанасьев [и др.] – М. : Горячая линия-Телеком, 2009. – 552с.
5. Защита информации. Техника защиты информации. Требования к средствам высоконадёжной биометрической аутентификации : ГОСТ Р 52633-2006 – 2007. – Введ. 2007-04-01.
6. A Guide to Understanding Identification and Authentication in Trusted Systems [Электронный ресурс]: стандарт. – Режим доступа: http://ftp.fas.org/irp/nsa/rainbow/tg017.htm.
7. Касперски, К. Техника сетевых атак / К. Карсперски. – М. : Солон-Р, 2001. – 400 с. – ISBN 5-93455-078-0.
8. Смит, Р.Э. Аутентификация: от паролей до открытых ключей. / Р.Э. Смит – М. : Издательский дом «Вильямс», 2002 – 432 с. – ISBN 5-8459-0341-6.
9. Марков, А.Г. Метрики стойкости парольной защиты. [Электронный ресурс]: молодёжный научно-технический вестник. / ФБГОУ ВПО «МГТУ им. Н.Э. Баумана». – Электронный журнал. – Режим доступа: http://www.cnpo.ru/doc/psw-metrics.pdf/
10. Современные биометрические методы идентификации [Электронный ресурс]: статья. – Режим доступа: http://habrahabr.ru/post/126144/.

Шибанов Сергей Владимирович – канд. техн. наук, доцент кафедры «Математическое обеспечение и применение ЭВМ» ФГБОУ ВПО «Пензенский государственный университет». E-mail: *serega@pnzgu.ru*.
Карпушин Дмитрий Александрович – магистр ФГБОУ ВПО «Пензенский государственный университет». E-mail: *kolobchanin@gmail.com*.

Шибанов С.В., Карпушин Д.А. Сравнительный анализ современных методов аутентификации пользователя // Математическое и программное обеспечение систем в промышленной и социальной сферах. – 2015. – №1. – С. 33-37.

Shibanov, S.V. and Karpushin D.A. (2015). Comparative analysis of modern methods of authentication. Software of systems in the industrial and social fields, 5 (1): 33-37.