Математические структуры и моделирование
2012, вып. 26, с. 124–134

УДК 612.087.1:004.056.523

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ЛИЧНОСТИ: ОБЗОР ОСНОВНЫХ БИОМЕТРИЧЕСКИХ МЕТОДОВ ПРОВЕРКИ ПОДЛИННОСТИ ПОЛЬЗОВАТЕЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ

А.Б. Лысак

В статье рассматриваются основные биометрические методы, применяемые в современных компьютерных системах в целях идентификации и аутентификации пользователя. Приводится базовая классификация методов и описываются сферы их применения и ключевые отличия.

Введение

Необходимость разграничения доступа к постоянно возрастающим объёмам информации в современном мире остро ставит проблему проверки подлинности пользователя. Рост компьютерных сетей и интенсивности их использования также упрощает задачу злоумышленника по получению несанкционированного доступа к данным или определённым сервисам, предоставляемым компьютерными системами.

Помимо обеспечения разграничения прав доступа к конфиденциальной информации современные автоматизированные комплексы решают ряд смежных задач. Двумя основными процедурами, выполняемыми подобными комплексами, являются идентификация и аутентификация субъекта доступа. В общем случае таким субъектом для компьютерной системы может являться не только человек, но и любой процесс, выполняемый удалено или локально [1].

Однако по данным анализа статистики экспертами в области компьютерной безопасности большинство случаев, связанных с утечками информации связаны с факторами, к которым напрямую причастен человек. Причинами доступа третьих лиц к конфиденциальной информации на порядок чаще становилась работа инсайдеров и хакеров, нежели действия зловредного программного обеспечения [2, 3]. Таким образом, выводы экспертов подтверждают первостепенную значимость проблемы идентификации и аутентификации личности в области компьютерной безопасности.

В большинстве современных компьютерных систем проверка личности пользователя осуществляется с помощью ввода логина и пароля. В настоящее время

Омский НИИ приборостроения
E-mail: antonlysak@gmail.com

существуют и другие методы, которые, хотя и не получили такого широкого распространения, потенциально являются намного более надёжными. В частности, существует целый класс перспективных биометрических подходов.

Целью данной статьи является нахождение способа надёжной защиты от несанкционированного доступа к информации путём применения современных биометрических технологий.

Для достижения данной цели необходимо:

1. Проанализировать существующие подходы к идентификации и аутентификации личности.

2. Рассмотреть современные биометрические технологии, их сильные и слабые стороны.

3. Найти приемлемую технологию или их комбинацию, которые бы обеспечили более надёжную защиту конфиденциальной информации.

1. Современные подходы к идентификации и аутентификации

В первую очередь необходимо определить различия между идентификацией и аутентификацией.

Процесс идентификации заключается в предъявлении пользователем идентификатора и сопоставления его с образцами идентификаторов всех пользователей в системе (сравнение 1:m). Наибольшее распространение чистая идентификация получила областях, где непосредственный контакт человека с системой не предусмотрен, например, в системах распознавания лиц. В качестве проверки личности пользователя при доступе к ресурсам современных компьютерных систем идентификация не используется по причинам значительно меньшей надёжности по сравнению с аутентификацией.

В процессе аутентификации пользователь также должен предъявить системе идентификатор, заявляя о том, кто он, и подтвердить свою личность. Для этого в дополнение к идентификатору используется нечто, называемое не получившим широкого распространения термином *аутентификатор*. После нахождения в базе данных требуемой записи о пользователе с помощью идентификатора, система выполняет сравнение аутентифакотора, хранящегося в ней с тем, который предъявил пользователь. При аутентификации последовательно выполняется сравнение 1:m идентификаторов и 1:1 аутентификаторов.

Таким образом, для того, чтобы система функционировала с требуемыми уровнями быстродействия и надёжности, необходимо правильно выбирать, что использовать в качестве идентификатора, а что — в качестве аутентификатора.

Три основных подхода, с помощью которых возможно осуществить как идентификацию, так и аутентификацию, описаны ещё в 1994 году [4]:

1. С использованием собственности — пользователь предъявляет системе некоторый физический предмет, например, смарт-карту или usb-токен.

2. С использованием знаний — пользователь вводит в систему какую либо секретную фразу, например, пароль или PIN-код.

3. С использованием характеристик — пользователь предъявляет системе свои физиологические или поведенческие параметры.

Автор статьи, Бенджамин Миллер, рассматривая эти три подхода, говорил об их совместном использовании. Например, при доступе к своему банковскому счету с помощью банкомата пользователь использует пластиковую карту (собственность) в качестве идентификатора и PIN-код (знания) в качестве аутентификатора. В настоящее время первые два подхода широко применяются как в комбинации, так и по отдельности. Помимо специализированных систем аутентификация с использованием собственности в виде USB-брелока возможна на персональном компьютере с операционной системой общего пользования [5]. Тем не менее, наиболее широкое распространение получил подход с использованием знаний в чистом виде. Связка: логин в качестве идентификатора и пароль в качестве аутентификатора — ежедневно используется сотнями миллионов пользователей глобальной сети Интернет по всему миру. В качестве основной причины повсеместного распространения данного подхода можно, в первую очередь, выделить отсутствие необходимости в дополнительном аппаратном обеспечении для проведения процедуры аутентификации и, как следствия этого, отсутствие дополнительных материальных затрат и более высокий уровень удобства пользователя.

Несмотря не невысокую распространённость биометрических характеристик, неоспоримыми преимуществами их использования является то, что их, в отличие от собственности и знаний, невозможно намеренно передать другому, потерять или украсть. Данные свойства биометрических характеристик делают их практически идеальными для использования в качестве аутентификатора, поскольку надёжность системы аутентификации напрямую зависит от возможности его попадания в руки злоумышленника.

В это же время использование биометрических характеристик в качестве идентификатора сопряжено с некоторыми трудностями. Проблема заключается в том, что в отличие от знаний и собственности предъявляемый пользователем биометрический идентификатор никогда не будет с абсолютной точностью совпадать с идентификатором из базы данных. В процессе экстракции свойств из биометрического образца они подвергаются искажению и наложению шума [6]. Это приводит к тому, что при поиске соответствующего биометрического идентификатора в базе данных используется не простое сравнение цифрового представления информации, а более сложный алгоритм:

1. К образцу, предъявляемому пользователем B_1, и хранящемуся в базе данных B_2 применяется функция экстракции — $f(B_1)$, $f(B_2)$.

2. Вычисляется величина, выражающая степень сходства между образцами $s(f(B_1), f(B_2))$.

3. Получившаяся величина сравнивается с заранее заданным пороговым значением T. В случае $s > T$ процедура завершается успешно, в случае $s < T$ — неудачно.

Эффективность работы алгоритма применительно к выбранному биометрическому параметру обычно оценивают по двум критериям:

1. FAR(False Acceptence Rate) — коэффициент ложного доступа, процентный показатель случаев, при которых проверка личности оказалась ошибочно успешной.

2. FRR(False Rejection Rate) — коэффициент ложного отказа в доступе, процентный показатель случаев, при которых проверка личности ошибочно завершилась неудачей.

Для использования биометрического идентификатора в системе аутентификации необходимо применение биометрического параметра B, функций экстракции f и сравнения s, для которых требования к вычислительным ресурсам будут минимальными при достаточно низком уровне FRR. Это должно обеспечить быстрое и успешное определение личности пользователя. При этом требование по минимизации FAR не является критичным, поскольку надёжность аутентификации практически полностью зависит от аутентификатора, а не от идентификатора. Для повышения удобства процедуры аутентификации также возможно использование нескольких различных типов идентификаторов для каждого пользователя. Внедрение гибридных систем аутентификации, в которых пользователь может использовать биометрические параметры по своему выбору вместо традиционного ввода логина не влияет на безопасность и при этом позволяет совершить плавный переход к широкому использованию биометрии.

Если для идентификатора наиболее важным параметром является FRR, то при выборе подходящего аутентификатора критичную роль играет значение FAR. Помимо этого, рост применения биометрических аутентификаторов также возможен только при выполнении определённых требований, которые будут рассмотрены далее.

2. Основные биометрические методы и их классификация

Все биометрические параметры можно разделить на две большие группы:

1. Физиологические — физические характеристики человека, измеряемые в определённый момент времени;

2. Поведенческие — определённые действия, совершаемые человеком на протяжении промежутка времени.

В настоящее время подавляющее большинство систем аутентификации использует в качестве биометрических параметров физиологические признаки.

Причиной этого можно назвать значительно более высокую надёжность по сравнению с поведенческими характеристиками при достаточно несложных алгоритмах экстракции и вычисления сходства. В то же время, наибольшее распространение получили не самые эффективные подходы по показателям FAR/FRR. Проанализировав ситуацию, можно выделить следующие основные факторы, влияющие на применимость того или иного биометрического метода:

1. Стоимость оборудования для получения требуемой биометрической характеристики.

2. Возможность подделки биометрического образца злоумышленником.

3. Удобство, которое складывается из среднего времени, занимаемого процедурой, и перечнем действий, совершаемых в её процессе.

4. Отношение общества к использованию данной характеристики.

Поскольку при достаточно большом разнообразии подходов дать количественную оценку по каждому из данных факторов не представляется возможным, необходимо попытаться качественно оценить основные биометрические методы, используемые в настоящее время и имеющие потенциальную применимость в ближайшем будущем. В статье принципиально не рассматриваются такие методы как использование ДНК или сетчатки глаза, поскольку оборудование для их получения настолько дорогостоящие, что не приходится предполагать рост распространения данных подходов.

Отпечатки пальцев

Использование отпечатков пальцев берет своё начало в конце XIX века и основывается на гипотезе Уильяма Гершеля о том, что папиллярные линии на поверхности ладоней и пальцев являются уникальными для каждого человека. Несмотря на то, что это предположение до сих пор не имеет научного обоснования, с начала XX века и по настоящее время данный биометрический признак получил широкое распространение в целях идентификации преступников. Кроме того, сейчас он также является наиболее часто используемым биометрическим признаком для предоставления доступа к компьютерным системам. Более 12% моделей современных ноутбуков имеют встроенные аппаратные и программные средства для получения и обработки отпечатков пальцев.

В настоящее время для получения отпечатка пальца используются специальные сканеры. Все существующие сканеры можно разделить на три группы [7]:

1. Оптические.

2. Полупроводниковые.

3. Ультразвуковые.

Оптические сканеры основаны на использовании оптических методов получения изображения. Существует несколько способов реализации данного метода, но общий принцип заключается в том, что небольшая камера или набор фотодатчиков фиксируют изображение на специальной полупрозрачной поверхности, получаемое в результате освещения пальца с одной или нескольких сторон. Стоимость таких сканеров на рынке начинается с 15$. Процедура получения отпечатка занимает не более секунды и производится в одно касание. К минусам данных устройств можно отнести отсутствие защиты от муляжей и быстрое загрязнение сканера, резко понижающее его надёжность.

В основе работы полупроводниковых сканеров лежит использование особых свойств полупроводников, изменяющихся в местах контакта гребней папиллярного узора с поверхностью сканера. Можно выделить следующие типы данных устройств:

1. Ёмкостные.
2. Радиочастотные.
3. Пьезоэлектрические.
4. Термические.

Ёмкостные и пьезоэлектрические сканеры имеют сопоставимые с оптическими сканерами стоимость и надёжность. Радиочастотные и термические являются гораздо более устойчивыми к атакам с использованием муляжей, но имеют более высокую стоимость.

Ультразвуковые сканеры являются относительно новыми на рынке устройств получения отпечатков пальцев. Они используют ультразвуковые волны для облучения поверхности пальцев и определяют папиллярный узор по отражённому эху. Качество получаемых изображений в несколько раз выше, чем у оптических и полупроводниковых сканеров. Данный способ практически полностью защищён от муляжей и устойчив к загрязнению пальцев. Существенным недостатком является высокая стоимость подобных устройств по сравнению с оптическими и полупроводниковыми сканерами.

Вне зависимости от применяемых устройств отпечаток пальца, как и практически любой другой физиологический признак, может без особого труда быть получен злоумышленником. Изготовить муляж также не представляет особой технической сложности, в особенности для обмана широкораспространенных недорогих моделей сканеров. Второй проблемой является то, что в случае компрометации сменить изображение отпечатка пальца в отличие от пароля не представляется возможным. Кроме того реакция современного общества на повсеместное использование отпечатков пальцев определённо является негативной по причине применения данного признака в криминалистике.

Лицо

Методы проверки подлинности с использованием изображения лица стали стандартом де-факто ещё до широкого распространения компьютерных систем.

Так практически все документы, удостоверяющие личность, содержат фотографию лица аутентифицируемого субъекта. Этот способ распознавания является наиболее естественным для человека и поэтому не встречает никакого сопротивления со стороны общества.

Достаточно надёжные системы базируются на применении нескольких камер, расположенных под разными углами и обеспечивающих формирование трёхмерной модели лица. В них также используется дополнительная подсветка для снижения влияния освещения на получаемый результат. Подобные системы находят применение на контрольно-пропускных пунктах предприятий. В то же время применение таких систем обычными пользователями в повседневных условиях невозможно по причине их высокой стоимости, сложности установки и использования.

Наиболее распространёнными устройствами, позволяющими получить двухмерное изображение лица пользователя являются веб-камеры. В настоящее время около 95% моделей ноутбуков, представленных на рынке, имеют встроенную камеру. Стоимость внешней веб-камеры для персонального компьютера составляет от 10$. Использование недорогого оборудования негативно сказывается на надёжности системы. Отрицательное влияние также оказывает изменяющееся освещение.

Современные алгоритмы способны компенсировать наличие очков, усов и бороды, а также дополнительных аксессуаров на лице исследуемого индивида даже на двумерном изображении. Однако основной проблемой использования двумерных изображений является уязвимость к атакам с использованием муляжей. Для обмана таких систем достаточно использование фотографии субъекта.

Соответственно, можно сделать вывод о том, что широкое распространение может получить только подход с использованием двумерного изображения лица в качестве идентификатора.

Ладонь

С руки человека возможно собрать до 90 информационных признаков [8]. Однако не все они в настоящее время используются.

Существует два подхода при использовании изображения ладони:

1. Первый, существующий с 1976 года, основан исключительно на геометрических характеристиках кисти.

2. Второй, современный, использует кроме геометрических ещё и рисунки на сгибах между фалангами пальцев и узоры кровеносных сосудов.

Современные сканирующие устройства не требуют непосредственного контакта ладони с поверхностью сканера. Соответственно, при их использовании не предъявляется жёстких требований к чистоте, влажности, температуре рук. Процедура сканирования занимает несколько секунд, удобна для пользователя, а сам метод не встречает негативной реакции со стороны общества.

Получение данных злоумышленником и изготовление муляжа, особенно для систем, использующих исключительно геометрические характеристики, не является неразрешимой задачей, хотя и более сложно, чем в случае с отпечатками пальцев или изображением лица. Существенным недостатком также является высокая стоимость устройств сканирования — около 300$, не включая затрат на программное обеспечение [9]. В настоящее время это является важнейшим сдерживающим фактором для распространения данного биометрического метода.

Радужная оболочка глаза

Радужная оболочка глаза является уникальной характеристикой человека. Её рисунок формируется на восьмом месяце внутриутробного развития, окончательно стабилизируется в возрасте около двух лет и практически не изменяется в течение жизни, кроме как в результате сильных травм или резких патологий. Данный метод в настоящее время является одним из наиболее точных [10].

Качество современных устройств получения изображения радужной оболочки в совокупности с разработанными алгоритмами позволяет достигать достаточной надёжности для использования данного метода в режиме чистой идентификации. [11] Однако стоимость устройств, позволяющих получить настолько качественные изображения, составляет несколько тысяч долларов США и ограничивает их применение организациями, в которых предъявляются очень высокие требования к безопасности. Также существуют реализации систем на базе простых и дешёвых цифровых фотокамер с высоким разрешением, однако их надёжность является более низкой.

С точки зрения удобства для пользователя такие системы также нельзя назвать идеальными. Несмотря на то, что снимок делается практически мгновенно, пользователю необходимо занять правильное положение по отношению к считывающему устройству таким образом, чтобы расстояние до глаз составляло определённую величину. Это значение может быть различным для разных устройств, но в общем случае составляет несколько десятков сантиметров.

Кроме того, как и любой другой физиологический признак, изображение радужной оболочки не защищено от копирования и воспроизведения злоумышленником. Достаточно качественное изображение радужной оболочки возможно получить с помощью фотографии, а затем использовать в системе, не предусматривающей физический контроль процедуры проверки.

Рукописная подпись

Рукописная подпись — один из классических способов проверки личности, применяемый уже несколько столетий в юридической практике, банковском деле и торговле. Относительно долгая история использования подписи обеспечивает лояльность со стороны общества к этому биометрическому параметру.

Существует два подхода к использованию подписи:

1. Статический, при котором сравниваются изображения подписей. Он является классическим и выполняется человеком на протяжении нескольких столетий.

2. Динамический, при котором используются сведения о колебаниях пишущего пера, силе нажатия, наклоне пера как функции времени [12]. Данный современный подход возможен исключительно для использования компьютерными системами.

Для получения информации о биометрических характеристиках подписи при динамическом подходе всеми современными системами используются графические планшеты (дигитайзеры). Стоимость такого устройства зависит от его характеристик и начинается приблизительно от 100$. Более дорогие дигитайзеры позволяют получать больше признаков, например, угол наклона пера относительно планшета.

Удобство использования подписи варьируется в зависимости от того, как часто человек использует её в повседневной жизни. Люди, привыкшие подписывать десятки документов в день не испытывают какого-либо дискомфорта от данной процедуры. Время её совершения также может быть различным, но в общем случае можно говорить о том, что оно составляет несколько секунд и не существенно отличается от времени ввода пароля с использованием клавиатуры. Недостатком является то, что в существующих системах, применяющих динамический подход, пользователю приходится расписываться пером графического планшета, которое достаточно сильно отличается от привычной авторучки.

Большим преимуществом является то, что при использовании динамического подхода злоумышленник не может скопировать подпись, за исключением случаев, когда информация о динамике воспроизведения передаётся по незащищённым каналам связи. Повторить подпись с теми же характеристиками невозможно даже в том случае, если злоумышленник неоднократно наблюдал процесс её воспроизведения.

Уникальность использования подписи в качестве биометрического аутентификатора заключается в возможности смены аутентификатора по желанию пользователя. Это полезно, если она все же будет каким-либо образом скомпрометирована. Таким образом, подпись можно рассматривать как гибрид подходов с использованием знаний и биометрических характеристик.

Голос

Идентификация человека по голосу также является одним из традиционных способов распознавания, применяемым повсеместно. Можно легко узнать собеседника по телефону, даже не видя его.

Использование голоса является одним из наиболее удобных для пользователя методов. Произнесение требуемой фразы не требует непосредственного контакта пользователя с каким-либо элементом системы. Встроенные устройства звукозаписи присутствуют практически во всех моделях ноутбуков и других

цифровых устройств. Внешний микрофон для персонального компьютера имеет стоимость в несколько долларов США. В целом можно говорить о том, что по стоимости и удобству данный метод определённо можно назвать наиболее привлекательным.

Несмотря на данные преимущества, голосовые методы обладают невысокой надёжностью. Негативно на ней сказывается ещё и то, что голос меняется с возрастом, а также при различных заболеваниях и нарушениях в организме.

Как и в случае с подписью, применение голосового метода в реальной системе не является чисто биометрическим. Пользователю также необходимо знать парольную фразу. Однако в отличие от случая с подписью, в данном методе это является существенным минусом, поскольку злоумышленник может легко подслушать её во время процедуры. Более того не существует особых преград для того, чтобы записать и в дальнейшем использовать реальную голосовую запись для получения несанкционированного доступа. Таким образом, можно говорить о том, что использование голоса возможно в современных биометрических системах исключительно в роли идентификатора.

Заключение

Большинство физиологических биометрических признаков не может получить широкое применение, в первую очередь, по причине нежелания большей части пользователей компьютерных систем передавать в базы данных свои уникальные и неизменяемые параметры. Ситуация обостряется тем, что при их утечке и попаданию к злоумышленнику пользователь не сможет их изменить.

Физиологические параметры, к использованию которых общество относится терпимо, например, изображение лица, не могут обеспечить надёжность распознавания, достаточную для того, чтобы заменить традиционные методы с использованием знаний и собственности. Их применение в системах аутентификации возможно только в роли идентификатора при условии применения программно-аппаратных средств, обеспечивающих быструю и не требующую дополнительных действий со стороны пользователя идентификацию в совокупности с невысокой стоимостью.

В то же время огромные перспективы использования в качестве аутентификатора имеют поведенческие параметры, в частности, рукописная подпись. Несмотря на многочисленные преимущества, данный метод все ещё не получил широкого распространения по причинам, рассмотренным в основной части статьи. Можно выделить следующие направления, в которых необходимо вести работу для того, чтобы подпись стала реальной заменой аутентификации с использованием пароля:

1. Разработка недорогих специализированных аппаратных средств для получения образцов рукописной подписи.

2. Разработка быстрых и надёжных алгоритмов экстракции и сравнения биометрических характеристик рукописной подписи.

3. Разработка удобных для пользователя аутентификационных протоколов с возможностью использования в качестве идентификатора других биометрических признаков.

Литература

1. ФСТЭК России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. URL: http://www.fstec.ru/_docs/doc_3_3_002.htm (дата обращения: 29.06.2012).
2. Утечки корпоративной информации и персональных данных в 2010 году. URL: http://www.anti-malware.ru/node/3632 (дата обращения: 26.08.2012).
3. Что реально угрожает персональным данным? URL: http://www.anti-malware.ru/personal_data_leaks (дата обращения: 26.08.2012).
4. Benjamin Miller Vital signs of identity // IEEE Spectrum. 1994. N. 2. C. 22–30.
5. Rutoken. Российское средство аутентификации. URL: http://www.rutoken.ru/ (дата обращения: 26.08.2012).
6. Болл Р.М. Руководство по биометрии. М. : Техносфера, 2007. 368 с.
7. Сканеры отпечатков пальцев. Классификация и способы реализации. URL: http://habrahabr.ru/post/116458/ (дата обращения: 30.08.2012).
8. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. СПб. : Политехника, 2001. 240 с.
9. PalmSecure Palm Vein Sensor. URL: http://www.amazon.com/PalmSecure-Palm-Vein-Sensor-biometric/dp/B007Y7YU12 (дата обращения: 02.09.2012).
10. Современные биометрические методы идентификации. URL: http://habrahabr.ru/post/126144/ (дата обращения: 02.09.2012).
11. Технологии распознавания радужной оболочки глаза в аэропортах (По материалам доклада «Биометрия в авиационной безопасности», подготовленного для конференции ITE&AIA) // Системы безопасности. 2006. № 5. С. 140–144.
12. Ложников П.С., Еременко А.В. Идентификация личности по рукописным паролям // Мир измерений. 2009. № 4. С. 1–13.