Разрабатываемое приложение является системой отслеживания и анализа поведенческой биометрии.

На всемирном рынке в свободном доступе существуют десятки систем, работающих с биометрическими параметрами, но лишь единицы из них рассматривают их с поведенческой точки зрения. Чаще всего рассматриваются отпечатки пальцев, сетчатка глаза, анализ голоса и лица пользователя, что неприменимо к нашему случаю.

ЛИТЕРАТУРА

1. Интернет-портал Devprom [Электронный ресурс] / Инструменты проектирования: Enterprise Architect. – Режим доступа: http://devprom.ru/news-Enterprise-Architect. Дата доступа: 15.09.15.

УДК 004.023

АНАЛИЗ СУЩЕСТВУЮЩИХ СРЕДСТВ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

М.А. КВЕТИНСКИЙ
(Представлено: М.В. МАТЮШ)

Рассмотрены общие понятия, методы и технологии биометрической идентификации, как это работает и для чего нужно. Приведен обзор нескольких разрабатываемых и уже готовых проектов.

Биометрия – это методы автоматической идентификации человека и подтверждения личности человека, основанные на физиологических или поведенческих характеристиках. Примерами физиологических характеристик являются отпечатки пальцев, форма руки, характеристика лица, радужная оболочка глаза. К поведенческим характеристикам относятся особенности или характерные черты, либо приобретенные или появившиеся со временем, то есть динамика подписи, идентификация голоса, динамика нажатия на клавиши.

Все биометрические системы работают практически по одинаковой схеме. Во-первых, система запоминает образец биометрической характеристики (это и называется процессом записи). Во время записи некоторые биометрические системы могут попросить сделать несколько образцов для того, чтобы составить наиболее точное изображение биометрической характеристики. Затем полученная информация обрабатывается и преобразовывается в математический код.

Идентификация по любой биометрической системе проходит четыре стадии:

– запись – физический или поведенческий образец запоминается системой;

– выделение - уникальная информация выносится из образца и составляется биометрический образец;

– сравнение – сохраненный образец сравнивается с представленным;

– совпадение/несовпадение – система решает, совпадают ли биометрические образцы, и выносит решение.

Подавляющее большинство людей считают, что в памяти компьютера хранится образец отпечатка пальца, голоса человека или картинка радужной оболочки его глаза. Но на самом деле в большинстве современных систем это не так. В специальной базе данных хранится цифровой код длиной до 1000 бит, который ассоциируется с конкретным человеком, имеющим право доступа. Сканер или любое другое устройство, используемое в системе, считывает определенный биологический параметр человека. Далее он обрабатывает полученное изображение или звук, преобразовывая их в цифровой код. Именно этот ключ и сравнивается с содержимым специальной базы данных для идентификации личности.

Биометрические данные можно разделить на два основных класса:

– физиологические – относятся к форме тела. В качестве примера можно привести: отпечатки пальцев, распознавание лица, ДНК, ладонь руки, сетчатка глаза, запах, голос;

– поведенческие – связаны с поведением человека. Например, походка и речь. Иногда для этого класса биометрии используется термин англ. behaviometrics.

Идентификация по отпечаткам пальцев – самая распространенная, надежная и эффективная биометрическая технология. Благодаря универсальности этой технологии она может применяться практически в любой сфере и для решения любой задачи, где необходима достоверная идентификация пользова-

телей. В основе метода лежит уникальность рисунка папиллярных узоров на пальцах. Отпечаток, полученный с помощью специального сканера, датчика или сенсора, преобразуется в цифровой код и сравнивается с ранее введенным эталоном. Надежность данного способа идентификации личности, состоит в невозможности создания идентичного отпечатка. Наиболее совершенную технологию идентификации по отпечаткам пальцев реализуют оптические сканеры.

Технология распознавания радужной оболочки глаза была разработана для того, чтобы свести на нет навязчивость сканирования сетчатки глаза, при котором используются инфракрасные лучи или яркий свет. Ученые также провели ряд исследований, которые показали, что сетчатка глаза человека может меняться со временем, в то время как радужная оболочка глаза остается неизменной. И самое главное, что невозможно найти два абсолютно идентичных рисунка радужной оболочки глаза, даже у близнецов.

Для получения индивидуальной записи о радужной оболочке глаза черно-белая камера делает 30 записей в секунду. Еле различимый свет освещает радужную оболочку, и это позволяет видеокамере сфокусироваться на радужке. Одна из записей затем оцифровывается и сохраняется в базе данных зарегистрированных пользователей. Вся процедура занимает несколько секунд, и она может быть полностью компьютеризирована при помощи голосовых указаний и автофокусировки.

В аэропортах, например, имя пассажира и номер рейса сопоставляются с изображением радужной оболочки, никакие другие данные не требуются. Размер созданного файла, 512 байт с разрешением 640 x 480, позволяет сохранить большое количество таких файлов на жестком диске компьютера.

Очки и контактные линзы, даже цветные, никак не повлияют на процесс получения изображения. Также нужно отметить, что произведенные операции на глазах, удаление катаракты или вживление имплантатов роговицы не изменяют характеристики радужной оболочки, ее невозможно изменить или модифицировать. Слепой человек также может быть идентифицирован при помощи радужной оболочки глаза. Пока у глаза есть радужная оболочка, ее хозяина можно идентифицировать.

Голосовая биометрия, позволяющая измерять голос каждого человека, незаменима при удаленном обслуживании клиентов, когда основным средством взаимодействия является голос, в первую очередь, в автоматических голосовых меню и контакт-центрах.

Традиционные способы аутентификации клиента при удаленном обслуживании проверяют знания клиента (для этого клиента просят ввести какой-то пароль или ответить на вопросы безопасности - адрес, номер счета. девичью фамилию матери и пр.) Как показывают современные исследования в области безопасности, злоумышленники относительно легко могут добыть персональные данные практически любого человека и таким образом получить доступ, например, к его банковскому счету. Голосовая биометрия решает эту проблему, позволяя при удаленном телефонном обслуживании проверят действительно личность клиента а не его знания. При использовании голосовой биометрии клиенту при звонке в IVR или в контакт-центр достаточно произнести парольную фразу или просто поговорить с оператором (рассказать о цели звонка) - голос звонящего будет автоматически проверен.

Классическая верификация (идентификация) человека по почерку подразумевает сличение анализируемого изображения с оригиналом. Именно такую процедуру проделывает например оператор банка при оформлении документов. Очевидно, что точность такой процедуры, с точки зрения вероятности принятия неправильного решения (см. FAR & FRR) невысокая. Кроме этого, на разброс значений вероятности принятия правильного решения оказывает и субъективный фактор.

Принципиально новые возможности верификации по почерку открываются при использовании автоматических методов анализа почерка и принятия решения. Данные методы позволяют исключить субъективный фактор и значительно снизить вероятность ошибок при принятии решения (FAR & FRR).

Одним из факторов, которые определяет преимущество автоматических методов идентификации путем анализа почерка по сравнению с классическими методами верификации, является возможность использования динамических характеристик почерка. Автоматические методы идентификации позволяют принимать решение не только путем сличения изображения верифицируемого и контрольного образца, но и путем анализа траектории и динамики начертания подписи или любого другого ключевого слова [1].

В свободном доступе можно найти информацию лишь о некоторых проектах.

В Курском государственном университете под руководством Леонида Крыжевича, кандидата технических наук, доцента кафедры математического анализа и прикладной математики разрабатывается программа с подобным функционалом. По словам ученого , путем сложных математических преобразований, основанных на теории вероятности и статистике, коллективу КГУ удалось разработать программный продукт, который идентифицирует пользователя компьютера с точностью до 96%. Для успешной работы программы, по словам Крыжевича, достаточно набора четырех-шести символов. Ожидается, что демонстрационный программный продукт появится на рынке уже в следующем году [2].

DARPA Active Authentication Program: Behavioral Biometrics также схожий по функционалу продукт. В 2013 году на RSA Conference Asia Pacific были представлены некоторые его концепты и результаты его тестирования. Также были приведены математические формулы расчета и анализа «доверия» анализируемому пользователю. Данный программный продукт опирается на большое количество разнообразных критериев оценки и поведенческих параметров. По результатам тестирования, программа может определить неверного пользователя в течении 10 секунд использования компьютера (6 взаимодействий, в среднем 3 нажатия клавиш) или же менее чем за 3,5 минут использования мыши [3].

SilentSense, мобильное приложение, считывающее действия пользователя за устройством и с высокой точностью определяющее, является ли он владельцем телефона. Считывая нажатия на экран, различные движения, и показания акселерометра, программа за 10 действий может определить валидность пользователя с вероятностью ошибки меньше 1%. К сожалению, данный программный продукт не подходит для персональных компьютеров, но использованные в нем математические функции для расчета вероятности и «доверия» к пользователю, лежащие в свободном доступе, могут прилично поспособствовать разработке системы идентификации [4].

Разрабатываемое нами приложение предназначено для идентификации пользователя на базе поведенческой биометрии. Оно наглядно показывает работоспособность системы идентификации пользователя на базе поведенческой биометрии, позволяет создать профиль пользователя с параметрами поведенческой биометрии и в дальнейшем использовать его для анализа.

ЛИТЕРАТУРА

1. Свободная энциклопедия – Википедия [Электронный ресурс] / Распространенные технологии биометрии - Режим доступа: https://en.wikipedia.org/wiki/ Biometrics#Adaptive_biometric_systems. Дата доступа: 10.09.15.
2. Интернет-портал Хакер [Электронный ресурс]/ Человека можно идентифицировать после 4-6 нажатий клавиш - Режим доступа: https://xakep.ru/2014/12/18/keyboard-id/ . Дата доступа: 12.09.15.
3. Официальный сайт RSA Conference [Электронный ресурс]/ DARPA Active Authentication Program - Режим доступа: http://www.rsaconference.com/. Дата доступа: 12.09.15.
4. Свободная энциклопедия - Cornell University Libriary [Электронный ресурс]/ SilentSense - Режим доступа: http://arxiv.org/pdf/1309.0073.pdf Дата доступа: 12.09.15.

УДК 004.492

АНАЛИЗ ПРИНЦИПОВ ВНЕДРЕНИЯ, НАЗНАЧЕНИЯ, УПРАВЛЕНИЯ ПРОГРАММНЫХ ЗАКЛАДОК. ХАРАКТЕРНЫЕ ПРИЗНАКИ И КЛАССИФИКАЦИЯ ПРОГРАММНЫХ ЗАКЛАДОК

А.Е. РАМАШКА
(Представлено: канд. техн. наук, доц. К.Я. РАХАНОВ)

Рассмотрена возможная классификация программных закладок по принципам внедрения, назначения и управления. Проанализированы характерные признаки программных закладок.

Программная закладка – это внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию (недокументированные возможности программного обеспечения) [1].

В настоящее время проблема программных закладок является актуальной и требует немедленного решения. Таким образом, возникает потребность в методах и программных продуктах, способных успешно противодействовать подобным угрозам. Современное предприятие представляет собой сложноорганизованную систему со своими управляющими органами и объектами информатизации. Поскольку любое современное рабочее место уже трудно представить без компьютера, которые практически всегда объединены в общую вычислительную сеть, необходимо полностью обезопасить их от возможных утечек секретных данных и конфиденциальной информации.

Как правило, многие крупные компания скрывают факт взлома и получения конфиденциальной информации злоумышленниками. Но даже без этой большой части всеобщей статистики, можно провести анализ известных кибер-атак, которые, к слову были произведены с помощью программных закладок.

Самым ярким примером действия программной закладки является военный конфликт в Персидском заливе. Тогда при проведении операции «Буря в пустыне» система ПВО Ирака оказалась заблоки-