

УДК 004.35

Актуальность мультибиометрических методов идентификации

Ванжа Роман Николаевич ,11-Р,

Рук: Абашин В.Г.

Актуальность: в связи с активным внедрением мультибиометрических технологий в различных средах деятельности человека.

Цель: в целях расширения кругозора.

Обозреватели индустрии считают, что объем рынка биометрических систем увеличится в течении следующих нескольких лет. Это касается технологий анализа отпечатков пальцев, голоса, формы лица, рисунка вен ладони и пальцев, радужной оболочки глаза.

На первый взгляд повсеместное применение биометрической идентификации выглядит весьма перспективно. Не нужно запоминать никаких паролей, нет риска потерять смарт-карту или иное средство доступа, идентификация обычно проходит быстро и просто. Все эти достоинства аннулируются недостатком биометрической информации — будучи хорошим идентификатором, она является никуда не годным ключом.

Хранение конфиденциальной информации сопровождается растущей угрозой ее раскрытия, следствием чего может стать вмешательство в частную жизнь или совершение незаконных операций с частной собственностью.

Компании, которые сканируют радужную оболочку для выдачи идентификационного бэйджа, могут также позволить правительственным структурам или коммерческим субъектам использовать биометрические данные для пополнения баз данных без согласия индивидуума как в законных, так и в незаконных целях. Поэтому эксперты сходятся во мнении, что информация такого характера требует шифрования.

У биометрических технологий есть свои уязвимые места. Некоторые из них считаются неэтичными. Например, высокой надежностью характеризуется

технология идентификации по сетчатке глаза. Но этот метод может показать признаки многих заболеваний, таких как диабет или некоторые виды рака. Полученная информация может привести к дискриминации по состоянию здоровья при получении страховки или приеме на работу. А так же самое серьезное из них — канал связи между сканером и базой данных пользователей информационной системы. Ведь именно сканер преобразует, например, отпечаток пальца человека в набор чисел, которые потом передаются на компьютер с управляющим ПО. Таким образом, злоумышленник может попытаться получить доступ к каналу связи, перехватить шаблон, а в будущем использовать его в своих целях.

Биометрические устройства защиты запоминают определенные уникальные особенности человека, свойственные только данной конкретной личности, например отпечатки пальцев, и используют эту информацию для сравнения при последующей аутентификации. Самыми надежными являются сканеры радужной оболочки или сетчатки глаза; незначительно отстают от них сканеры отпечатков пальцев, лиц или отпечатков ладони. Надежность этих устройств выше, чем у сканеров голоса или подписи, но ниже, чем у защиты с помощью паролей или аутентификационных жетонов.

Проблема заключается в том, что любая биометрическая система сравнивает между собой не объекты реального мира, а результаты измерений. Отсюда целый ряд отличных возможностей для введения ее в заблуждение. Скажем, раздобыв чужие результаты измерений, можно заранее сохранить их в уже готовом для обработки виде и, получив доступ к аппаратуре, ввести в систему в обход биометрических сенсоров. Доступ к программному обеспечению позволит подменить хранящиеся в системе данные другого пользователя своими. Но и без всякого доступа можно легко обмануть биометрическую проверку, предъявив сенсорам муляж, например, чужого пальца.

Принципиальное отличие скопированного отпечатка пальца от украденной смарт-карты или подсмотренного пароля заключается в том, что последние легко заменить, а пальцев у человека всего 10. И поскольку люди не слишком часто

работают в перчатках, заполучить чей-либо отпечаток пальца без его ведома — дело нехитрое. Довольно убедительно это продемонстрировала известная немецкая хакерская группа ССС, «украдя» отпечаток пальца министра внутренних дел Германии Вольфганга Шойбле, который активно выступал за внесение отпечатков пальцев в электронные паспорта. Во время публичного выступления в университете он имел неосторожность прикоснуться к стакану с водой, и теперь рисунок его собственного пальца стал публичным достоянием и широко растиражирован в Интернете. Несложно заполучить и рисунок радужной оболочки — достаточно обычной фотографии глаза в хорошем качестве. А уж образцы своей ДНК люди оставляют просто повсюду — для их получения достаточно невымытой кофейной чашки или выпавшего волоса. Другими словами, биометрические данные ни в коем случае нельзя считать секретными, они легкодоступны, и относиться к ним надо так, как если бы они были представлены для всеобщего обозрения.

Конечно, с муляжами и другими подделками пытаются бороться. Так называемая «проверка на живость» (liveness check) позволяет биометрическому устройству определить, имеет оно дело с живым человеком или ему подсовывают фальшивку. К сожалению, обойти эти проверки часто не сложнее, чем украсть сами данные. Например, в сканерах отпечатков пальцев есть температурные сенсоры и емкостные датчики. Первые легко обмануть полиэтиленовым пакетом с теплой водой или подогретым воском, вторые — специальным щупом или просто другим пальцем.

Книги и фильмы, в которых биометрические системы с удовольствием применяют банки и военные организации, создают впечатление, что это окончательное решение вопроса о безопасном доступе к данным. На практике же часто оказывается, что результатам их работы можно доверять не более чем подписи под документом, отправленным по факсу.

Технология аутентификации с применением биометрических устройств выглядит очень привлекательно. Однако, перед тем как окончательно остановиться на ней свой выбор, стоит принять во внимание и некоторые ее недостатки.

В фильме “Особое мнение” есть такой эпизод: для прохождения авторизации на право доступа к секретным документам использовалось препарированное глазное яблоко. Этот эпизод демонстрирует, что любой сканер можно обмануть, и это один из самых крупных недостатков технологии биометрической аутентификации.

Некоторые ситуации, однако, как будто специально создаются для применения биометрических устройств. Например, если ваша служба поддержки завалена запросами пользователей, забывших свои пароли, вам как раз и стоит обратиться к технологии биометрической аутентификации.

На биометрические устройства аутентификации могут влиять условия окружающей среды. Оптические сканеры имеют небольшие размеры, и их лучше использовать в офисах. Однако они, вероятно, не подойдут для применения в помещениях, где много пыли, высокая влажность или присутствуют другие загрязнения. Грязные, жирные или неправильно позиционируемые по отношению к объективу пальцы, руки или лица могут привести к некорректному считыванию устройством информации. Очки, контактные линзы, специфическое освещение и неправильное расположение видеокамеры способны отрицательно сказаться на надежности работы сканеров радужной оболочки или сетчатки глаза. Фоновые шумы и изменение голоса человека из-за болезни или стресса приводят к ошибкам в системах распознавания голоса.

Помимо этого, создатели всех биометрических устройств предъявляют специфические требования к программным и аппаратным средствам. Проверьте, есть ли у вас необходимые ресурсы для поддержки избранного вами устройства и сможет ли это устройство работать с вашим сетевым ПО. Кроме того, выясните, требуется и имеется ли в наличии внешний источник питания или порт USB.

Всевозможные страхи и культурные и религиозные предрассудки тоже могут работать против человека.

И конечно, “специалисты” уже нашли способы обманывать биометрические устройства. Отпечатки пальцев можно снять с любой гладкой поверхности, даже прямо со сканера отпечатков пальцев, с помощью графитового порошка и куска клейкой ленты или желатина. Сканеры радужной оболочки несложно обмануть, используя фотографию глаза пользователя, сделанную с высоким разрешением. Чтобы обнаружить обман, новейшие устройства регистрируют “признаки жизни”, в частности пульсацию кровеносных сосудов.

Для биометрических устройств приемлемый порог неудач в распознавании устанавливается на основе процента ложных разрешений на допуск (False Acceptance Rate — FAR) и процента ложных отказов в допуске (False Rejection Rate — FRR). FAR соответствует вероятности того, что биометрическое устройство ошибочно признает пользователя, а FRR — что оно ошибочно отвергнет его.

Если администратор занижает порог отказа в допуске, то система будет более “снисходительно” оценивать совпадение хранимого в устройстве биометрического образца с данными пользователя, и, естественно, увеличится вероятность, что она по ошибке разрешит вход постороннему.

Вывод: На сегодняшний день придумано немало технологий аутентификации пользователей в информационных системах, однако у каждой есть свои недостатки. Некоторые имеют слишком малую надежность, и способы их обхода хорошо известны злоумышленникам. Взлом систем, основанных на других технологиях, также возможен, просто требует более высокой квалификации. В полной мере это относится и к биометрии. Существенно уменьшить риск можно только с помощью многофакторной мультибиометрической аутентификации, когда для идентификации личности используется сразу два и более способов, и чем сильнее каждый из них, тем надежнее будет результат.

Литература

1. Денис Б. Биометрическая защита несёт угрозы.-URL:http://www.3dnews.ru/news/biometricheskaya_zashita_neset_ugrozi/. Дата обращения: 26.08. 2009.
2. Оксана К. Универсальная биометрия.-URL:<http://www.bytemag.ru/articles/detail.php?ID=6851>. Дата обращения: 25.08.2009.
3. Елена П., Александр Т. Эра биометрии или сумерки свободы.-URL:<http://www.vokrugsveta.ru/vs/article/6580/>.Дата обращения: 26.08. 2009.
4. Попов М. Биометрические системы безопасности.-URL:<http://www.rasi.ru/news.php?id=566&category=2>. Дата обращения: 26.08.2009.
5. Андрей С. Биометрия в зоне боевых действий.-URL: http://www.infox.ru/hitech/weapon/2009/08/26/Biomyetriya_print.phtml. Дата обращения: 26.08. 2009.
6. Майк Ф. Сильные и слабые стороны биометрических устройств.-URL:http://www.ccc.ru/magazine/depot/03_08/read.html?0502.htm. Дата обращения: 26.08.2009.
7. Райнбоу Т. Технология биометрической аутентификации Precise Biomatch.-URL: http://isup.ru/index.php?option=com_content&task=view&id=541&Itemid=58. Дата обращения: 26.08.2009.