Биометрическая аутентификация: проблемы будущего

Максим Репин, Дмитрий Машков, Анастасия Саккулина

В наше время одним из самых перспективных направлений в системах контроля доступа становится использование биометрических данных человека. Такой способ аутентификации очень удобен. Однако биометрия находится в самом начале длинного пути, и существует ряд проблем, связанных с относительной новизной данной технологии.

АУТЕНТИФИКАЦИЯ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ

Технология сканирования отпечатков пальцев – одна из самых распространенных. Отпечатки индивидуальны для каждого человека и не меняются в течение всей жизни, поэтому их относят к статическим методам распознавания.

На данный момент существуют три типа сканеров отпечатков: оптические (FTIR, оптоволоконные, оптические протяжные и др.), полупроводниковые (термосканеры, протяжные термосканеры, емкостные и др.) и ультразвуковые. Все они работают по разным принципам, но в итоге получают схожие изображения, которые в соответствии с определенными математическими алгоритмами преобразуются в контрольную сумму. Возможными уязвимостями данной технологии могут быть:

1. Создание муляжа на основе латекса или желатина. Подобный муляж может сработать на простых сканерах.

Решение: установка многофакторного сканера, фиксирующего температуру и потливость.

2. Перехват сигнала в случае, если сканер связан с основной системой проводным интерфейсом.

Решение: использование методов криптографии при передаче сигналов.

3. Конденсация (направление струи теплого воздуха на сканер и, как результат, восстановление последнего отпечатка). Решение: проблема сохранилась только для дешевых оптических сканеров, на полупроводниковых данный метод не работает. Кроме того, существует проблема распознавания пальца с порезами, "сморщиванием" кожи и другими дефектами, которую можно обойти за счет снятия нескольких отпечатков. Однако важно избежать избыточности биометрической информации в системе, так как это является нарушением ФЗ "О персональных данных" и постановления "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".

Аутентификация по геометрии лица Системы по распознаванию геометрии лица работают на основе физических и структурных признаков (формы лица, симметрии/асимметрии лица, формы и размера губ, носа, глаз и др.). Получив изображение лица, система создает на его основе уникальный шаблон, который сравнивается с образцом, хранящимся в базе организации (математические алгоритмы, применяемые при этом, зависят от производителя). Данные системы уже применяются на улицах и в аэропортах многих городов мира. Минусы данной технологии:

1. Изменение освещенности, мимики, волосяного покрова, наличие или отсутствие макияжа и др. препятствуют распознаванию. Решение: на дорогих системах используется возможность наблюдения в инфракрасном диапазоне (термография лица). Таким образом качество прямо пропорционально зависит от цены.

2. Обман системы с помощью фотографии лица зарегистрированного пользователя или перебор фотографий с разными типами лиц срабатывает на биометрических системах, установленных на ноутбуках нескольких крупных производителей.

Решение: использование 3D-распознавания (что недешево).

3. Система не может отличить близнецов.

Решение: использование двойной схемы – геометрия лица + отпечаток пальца/почерк/голос/пароль.

Аутентификация человека по радужке Это одна из наиболее надежных систем, представленных на рынке. Преимущество данной технологии – высокая информативность структуры радужки глаза. Однако из-за своей молодости технология несовершенна. Основным способом обхода системы является использование различных муляжей. Рассмотрим несколько методов защиты от компрометации системы.

1. Регистрация непроизвольных движений зрачка и глаза. Метод эффективный, но существует проблема с физиологическими особенностями людей. У некоторых это происходит редко, поэтому есть вероятность ошибки отказа аутентификации.

2. Проверка спектра отражения глаза. Способ основан на различии спектра отражения живого глаза и муляжей за счет влажности роговицы. Такую систему довольно легко обмануть путем смачивания муляжа желатином или другой смазкой.

3. Пупилография. Метод заключается в фиксации реакции зрачка на световой импульс. Муляж будет выявлен, так как сокращаться может только живой зрачок. Недостатки – неприятные ощущения при подаче импульса и продолжительное время аутентификации.

Для большинства систем перечисленные методы довольно надежны, но есть одно "но". Известно, что люди в линзах успешно проходят аутентификацию. Учитывая это, можно изготовить линзы с рисунком сетчатки легального пользователя.

Аутентификация по голосу Ее внедрение вызвано постоянным ростом и распространением телефонных линий различного типа. Данный вид биометрии основан на анализе характеристик голоса: громкости, скорости, манере речи и др.

Основные проблемы данного вида аутентификации:

- изменение голоса (эмоции, состояние здоровья);

- помехи в микрофоне и линиях связи;

- перехват конфиденциальной информации нарушителем.

Решение: использование ларингофона может дать звуковой сигнал, индивидуальный для каждого человека и весьма трудно дискредитируемый. Значительное развитие данного способа аутентификации может дать использование вейвлет-преобразования, которое позволяет уменьшить количество ошибок первого рода при фиксированной ошибке второго рода.

Аутентификация по подписи В настоящее время данная технология распространена мало. По сравнению с остальными биометрическими данными, подпись легко изменяется, что является существенным преимуществом. Проблемы этого способа связаны с человеческим фактором, так как почерк может значительно видоизмениться в зависимости от окружающей обстановки и эмоционального состояния человека. В связи с этим разработчики вынуждены допускать возможность довольно большой погрешности, чем и могут воспользоваться злоумышленники. Использование динамических характеристик, таких как сила нажатия на перо или скорость письма, затрудняет подделку, но ведет к усложнению устройства аутентификации и существенному росту его цены. Решением многих проблем может стать применение вейвлет-преобразований.

Несмотря на существующие проблемы и недостатки, биометрические устройства являются очень перспективным направлением развития систем контроля доступа и аутентификации, так как существенно упрощают процесс и позволяют легко выполнять самые сложные задачи.

Максим Репин, специалист ОАО "Концерн "ВЕГА" Дмитрий Машков, студент МГТУ им. Н.Э. Баумана Анастасия Сакулина, специалист ОАО "Концерн "ВЕГА"

**Список литературы**

Информационная безопасность" № 6, октябрь–ноябрь 2009