Рис. 1. Изображение отпечатка пальца

С позиции анализа в каждом отпечатке пальца можно определить два типа признаков – глобальные и локальные.

1. **Глобальные признаки** – это те, которые можно увидеть невооружённым глазом: папиллярный узор; область образа, выделенный фрагмент отпечатка, в котором локализованы все признаки; ядро, пункт, локализованный в середине отпечатка или некоторой выделенной области; пункт «дельта», начальная точка. Место, в котором происходит разделение или соединение бороздок папиллярных линий, либо очень короткая бороздка (может доходить до точки); тип линии – две наибольшие линии, которые начинаются как параллельные, а затем расходятся и огибают всю область образа; счётчик линий, число линий на области образа, либо между ядром и пунктом «дельта».

2. **Локальные признаки** (их называют минуциями) – уникальные для каждого отпечатка признаки, определяющие пункты изменения структуры папиллярных линий (окончание, раздвоение, разрыв и т.д.), ориентацию папиллярных линий и координаты в этих пунктах. Каждый отпечаток содержит до 70 минуций. Согласно стандартам РФ [2] существует два основных типа минуций (контрольных точек): точка окончания основы гребня и точка бифуркации основы гребня (или точка разветвления). Помимо указанных типов в отпечатках пальцев реже встречаются и другие типы информативных точек, имеющих более сложные определения. На рис. 2 представлены некоторые варианты расположения и измерения контрольных точек.

Рис. 2. Расположение и ориентация контрольных точек

Данные об отпечатке пальца пользователя формируются в соответствующую структуру согласно [2], которая имеет различные поля: идентификатор формата; номер версии; длина записи; идентификационный номер биометрического сканера; уровень настроек получения изображений; число изображений пальцев/ладоней; единица измерения разрешения; разрешение сканирования (горизонтальное); разрешение сканирования (вертикальное); разрядность шкалы градаций серого; Алгоритм сжатия изображения.

Применение отпечатков пальце в идентификации личности позволяет упростить и ускорить (автоматизировать) многие выполняемые человеком операции, поскольку обычное удостоверение личности, которое можно утратить, забыть, заменяется собственным отпечатком. При этом гарантируется высокая точность и надежность идентификации личности. С использованием технологии идентификации по отпечаткам пальцев надежно решаются следующие задачи: банковские транзакции, аутентификации водительских прав, задачи пограничного контроля, допуск на рабочие места и др. В перспективе имеется множество задач, где еще может применятся данная технология.

Список литературы

1. Болл Р., Коннел Дж. Руководство по биометрии. – М.: Техносфера, 2007.
2. ГОСТ Р ИСО/МЭК 19794-2-2005 Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки.

ФАКТОРЫ УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ ТЕХНИЧЕСКОЙ СИСТЕМЫ

Жаринов А.А., Шмокин М.Н.

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: los@pgta.ru

Одной из проблем, возникающих при планировании системы информационной безопасности предприятия, является необходимость оценить актуальность угроз, создаваемых различными источниками. Оценка актуальности этих угроз и целесообразности применяемых мер противодействия должна основываться на вероятностях реализации этих угроз. Оценить вероятность реализации тех или иных угроз можно лишь, основываясь на публикациях экспертных организаций, которые проводят расследование инцидентов в области информационной безопасности, а также выполняют тесты на проникновение.

В общем случае можно выделить три основных возможности проникновения в информационные системы компаний:

– использование ошибок в настройках телекоммуникационного оборудования и серверов;

– уязвимости *Web*-приложений, когда злоумышленник использует ошибки, допускаемые разработчиками этих приложений;

– использование нарушителем уязвимостей рабочих мест пользователей в сочетании с методами социальной инженерии.

Анализ недостатков сетевой инфраструктуры показывает, что залогом успешной атаки является не отсутствие тех или иных средств защиты, а неправиль-

ное использование этих средств или неправильная реализация отдельных механизмов защиты.

Проблемы парольной защиты. Разработчики бизнес-приложений часто допускают одновременно две ошибки:

– не предусматривают ограничения на минимальную сложность задаваемого пользователем пароля;

– не предусматривают механизмов противодействия автоматическому перебору паролей – блокировку учетной записи после определенного числа неуспешных попыток аутентификации и т.п..

Как показывают результаты исследований, российские пользователи склонны выбирать пароли, являющиеся сочетанием расположенных рядом клавиш клавиатуры. При этом, наиболее распространенные пароли: «1234567» – 3,36 %; «12345678» – 1,65 %.

Кроме онлайновых методов подбора пароля, нарушителю доступны и другие методы, например восстановление пароля по его хэшу. Источниками парольных хэшей могут являться:

– конфигурационные файлы сетевого оборудования;

– файлы */etc/shadow* операционных систем *Unix*;

– резервные копии операционных систем;

– системные таблицы СУБД, в том числе – доступные с помощью уязвимостей *Web*-приложений и т.п.

При правильной организации локальной вычислительной сети рекомендуется разделять ее на сегменты разного функционального назначения и обеспечивать фильтрацию трафика на границах сегментов.

При развертывании сетевых сервисов при наличии защищенных вариантов протоколов прикладного уровня, для передачи конфиденциальной информации используются их аналоги без криптографии или со слабой криптографической защитой (*NTLM* вместо *Kerberos*, *POP3* вместо *IMAP*, а также *SMTP*, *FTP* и *HTTP* без поддержки *SSL*/*TLS*).

Использование сотрудниками ноутбуков создает для нарушителя дополнительный фактор проникновения. Соединяясь с посторонней точкой доступа, пользователь попадает в среду, созданную владельцем этой точки доступа.

Как правило, в отношении мобильных устройств применяются те же меры защиты, что и для стационарных рабочих мест.

Одним из самых больших недостатков является несвоевременная установка обновлений безопасности или отказ от установки этих обновлений.

Аналогичную картину можно наблюдать при анализе конфигурации программного обеспечения. Для безопасной настройки операционной системы *Windows XP* необходимо настроить свыше 200 параметров, при этом около 60% параметров настраиваются автоматически при инсталляции операционной системы, а остальные требуют дополнительной настройки. Как правило, анализ конфигурации показывает, что подобная настройка не выполняется, что приводит к наличию на рабочих станций типичных ошибок конфигурации:

– использование протокола *NTLM*;

– сохранение парольных хэшей *LanManager*;

– автозапуск с отчуждаемых носителей и т.п.

Подобные ошибки активно используются при проникновении в информационные системы.

АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО СПЕЦИАЛИСТА УЛЬТРАЗВУКОВОЙ ДИАГНОСТИКИ

Жданов Д.Н., Затяжнов Д.В., Шитов Д.С.

Алтайский государственный технический университет, Барнаул, e-mail: bigdymon@mail.ru

Информационные технологии и микропроцессорная техника уже давно стали неотъемлемой частью самых разных сфер жизни человека. Особенно активно стало расти внедрение этих технологий в область здравоохранения. Врачи on-line консультируют пациентов посредством цифровой техники и телекоммуникаций, диагностическая аппаратура оснащена мощными процессорами, конференции и консилиумы проводятся через интернет. Таким образом, сегодня медицинские информационные технологии приобретают все большую актуальность, а программное обеспечение для медицины становится все более востребованными.

Понимая все это, многие российские компании специализируются на создании автоматизированного рабочего места врача, разрабатывая совместно со своими партнерами самое разнообразное программное обеспечение для лечебно профилактических учреждений (ЛПУ) и программно-аппаратные комплексы. Внедрение медицинских информационных систем способно значительно усовершенствовать рабочие процессы на самых разных уровнях: начиная от отдельных рабочих мест врачей как в отдельном ЛПУ, так до комплексной автоматизации поликлиник и стационаров на региональном уровне.

С 2006 года в рамках национального проекта «Здоровье» во многие российские клиники стали устанавливаться ультразвуковые сканеры Уральского приборостроительного завода «Карис плюс», выпущенные по лицензии компании Esaote S.p.A.. Отличительной особенностью данных аппаратов является закрытое программное обеспечение, фирменный формат сохранения изображений и необходимость перекодировки в популярные растровые стандарты при передачи на ПК с помощью дорогостоящего фирменного программного пакета IMT.LAB software.

Для ликвидации возникающих проблем при эксплуатации оборудования и повышения эффективности работы врача было предложено создание автоматизированного рабочего места (АРМ) специалиста ультразвуковой диагностики (УЗД) на основе персонального компьютера и ультразвукового сканера «Карис плюс». Для этого необходимо было решить следующие основные задачи:

1. Создать соединение между ПК и ультразвуковым сканером, позволяющее захватывать и сохранять на ПК изображения с одним из распространенных растровых форматов типа jpg, bmp, tiff.

2. Разработать автоматизированное рабочее место специалиста УЗД на основе базы данных MS Access, с возможностью создания и сохранения протокола обследования и изображений, захваченных с ультразвукового сканера.

Алгоритм программного обеспечения реализует следующие основные этапы в рамках работы специалиста ультразвуковой диагностики с пациентом:

- создание новой (открытие существующей) карточки пациента для ведения истории обследования;
- выбор профиля исследования и загрузка соответствующего шаблона согласно предполагаемому заболеванию органа человека;
- получение исходных данных исследования;
- сохранение изображений исследуемого органа;
- вывод результатов на печать, сохранение карточки пациента;
- анализ полученных данных и рекомендации.

При этом можно отметить, что программное обеспечение АРМ специалиста УЗД соответствует следующим требованиям заказчика:

- создаёт персональные карточки пациентов, хранить карточки или ссылки на них в собственной или подключаемой базе данных;
- получает изображения с экранов УЗИ-аппаратов, работая в рамках протокола DICOM;
- работает с шаблонами профилей УЗ-исследований;
- создаёт архивные копии картотеки и ведёт их учет;