быстродейственным и простым в реализации методом аутентификации по отпечатку пальца является сравнение по особым точкам. Существуют проверенные временем алгоритмы, реализующие данную процедуру аутентификации, однако, необходимость в разработке и реализации новых алгоритмов с лучшими характеристиками не отпадает и на сегодняшний день.

Литература

1. Stan Z. Li Anil K. Jain, Encyclopedia of Biometrics. Second edition, Springer, 2009.
2. Maltoni D., Maio D., Jain A.K., Prabhakar S., Handbook of Fingerprint Recognition, Springer, 2003.

ИССЛЕДОВАНИЕ И ПРИМЕНЕНИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ИНТЕГРИРОВАННОЙ КИС

М.М. Гондаг Саз, В.А. Вишняков

Выбрана конструкция функция безопасности для MVC 5, которая основана на средствах Owin − промежуточного программного обеспечения аутентификации. В процессе исследований аутентификации использовалась система мобильных приложений для банка Последовательность для входа в систему приложений следующая: 1. Пользователь регистрировался в системе ibank24.ir. 2. После регистрации по электронной почте он получает экаунт активизации, в котором содержался ключ активизации мобильных приложений. 3. Пользователь загружает сайт Android app. 4. Для работы используется: имя, пароль и ключ активизации. 5. Ключ запрашивается системой для входа в облачную среду. 6. Меню и ключ вводится пользователем.

Представлена структура программной системы аутентификации в ИКИС для работы сотрудников с мобильными приложениями в реальной системе защиты информации банка. Проведены исследования модели и алгоритмов аутентификации пользователей мобильных приложений в облачной среде, результаты которых показали их эффективность при работе в системе защиты информации банка.

Разработанные модели и средства аутентификации пользователей мобильных приложений использованы в учебном процессе кафедры ИТ Минского инновационного университета для улучшения изучения дисциплины «Основы защиты информации» студентами специальности ПОИТ, а также при выполнении НИР «Модели и средства информационного управления и электронного маркетинга предприятия».

КОМПОНЕНТЫ СИСТЕМЫ АУТЕНТИФИКАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ИНТЕГРИРОВАННОЙ КИС

М.М. Гондаг Саз, В.А. Вишняков

Активное развитие мобильных технологий ставит перед организациями вопрос аутентификации в корпоративной сети с облачными вычислениями. Простой и достаточно надежный метод аутентификации – это технология одноразовых паролей (One Time password, OTP). Такие пароли могут генерироваться специальными программами, дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на страницу доступа к облачному сервису. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и язык программирования SAML (Security Assertion Markup Language).

Усиленная аутентификация, в том числе с использованием дополнительных факторов, должна происходить на компьютере и мобильном устройстве, иначе мобильность будет слабым звеном в контуре безопасности организации. При этом меры обеспечения ИБ не должны создавать неудобства для пользователей. Одной из современных тенденций в области аутентификации является использование SSO (Single Sign-On). Идея этой технологии

заключается в обеспечении единой аутентификации для всех информационных систем организации, которые с точки зрения доступа являются разнородными и никак не интегрированы между. Вместо ввода логина и пароля для каждого приложения достаточно один раз пройти аутентификацию, например, при входе в домен. В докладе раскрывается особенности к реализации SSO-технологии.

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ RFID

Р.А. Жерносеков, В.Т. Першин

Основная цель использования технологии радиочастотной идентификации (Radio Frequency Identification, RFID) заключается в обеспечении в режиме реального времени бесконтактного и точного сбора и обработки данных по учету расположения и перемещения товарных изделий в складских условиях, реализуемых в компьютерных и телекоммуникационных сетях. Сегодня RFID-технология пока не получила широкого распространения в Республике Беларусь. Основной причиной, тормозящей ее развитие, является стоимость программно-аппаратного оборудования. Цена необходимого для реализации RFID технологии сопоставима со стоимостью оборудования, применяемого в обычной системе управления складом (Warehouse Management System, WMS). Однако, стоимость расходных материалов, а именно RFID-меток, остается несравнимо выше. Например, стоимость этикеток штрих-кода для одной метки колеблется в пределах 0,5–10 долл. Исследованию подвергалась технология RFID с маркировкой всех товаров, а также ячеек стеллажей и зон склада. Сигналы меток считывались автоматически или в ручном режиме дистанционно. Физический контакт метки и считывающего устройства при этом не требовался. RFID – это технология автоматического ввода данных, состоящая из компактных радиометок, использующихся в качестве носителей информации и стационарных или мобильных считывателей. Метки прикрепляются к идентифицируемым объектам или встраиваются в них. Считыватели могут устанавливаться в местах, где производится ввод данных, или применяться в качестве мобильных устройств. Технология RFID используется для маркировки, идентификации и отслеживания товаров в процессе их движения от производителя по цепочке поставок в руки покупателя или потребителя. Технология радиочастотной идентификации в Республике Беларусь только формируется, но она имеет хороший потенциал, поскольку экономика нашей страны интегрируется с экономикой России, а в России уже работают, по крайней мере, два завода по производству RFID идентификаторов.

ИССЛЕДОВАНИЕ УСТРОЙСТВА СЧИТЫВАНИЯ ИНФОРМАЦИИ В RFID СТАНДАРТА EM-MARINE

Р.А. Жерносеков, В.Т. Першин

Сообщаются результаты теоретического и экспериментального исследования устройства считывания бесконтактным способом уникального кода, записанного в RFID карты, другие метки стандарта EM-Marine. Показано, что данный считыватель может применяться во всех программных приложениях, используемых в компьютерных и телекоммуникационных сетях, требующих ввода пароля для проверки полномочий или проверки права пользователя на доступ к конкретным ресурсам и выполнение определенных операций над ними. Это могут быть дисконтные системы в сфере продаж товаров и услуг, системы учета, контроля доступа, контроля рабочего времени, как в локальных, так и в более развитых компьютерных и телекоммуникационных сетях. Анализируемое устройство может использоваться при парольной защите всего компьютера, например, устанавливаемой в BIOS. Уникальный код, прочитанный из RFID-метки стандарта EM-Marine, представляет собой 40 бит двоичной информации. Для передачи в компьютер эта информация преобразуется в последовательность символов. Единого стандарта для такого преобразования не существует. Поэтому, в различных программах формат посылки кода, ожидаемый от считывателя, может отличаться. Эмулируя ввод на клавиатуре компьютера в виде цифровых символов, этот набор передается в компьютер в виде сигнала на рабочей частоте 125 кГц с использованием амплитудной манипуляции. Все настраиваемые параметры считывателя запоминаются в его энергонезависимой памяти, т.е. сохраняются при выключении питания и при подключении