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

считывателя к другому компьютеру. Это позволяет произвести настройку или конфигурирование считывателя на одном компьютере, а эксплуатировать – на другом компьютере. Используемое программно-аппаратное оборудование соответствовало основному действующему стандарту ISO/IEC 18000-2:2009. Дистанция регистрации обычно составляла 10 ~ 50 мм. Оборудование близкого чтения недорого, но сами метки являются относительно дорогими и без перспектив удешевления из-за конструктивных особенностей их изготовления.

ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНЫХ СТРУКТУР ПРИ РАБОТЕ С БОЛЬШИМИ ОБЪЕМАМИ ДАННЫХ

И.Е. Закревский

Операции над большими массивами данных являются неотъемлемой частью ежедневной работы. Растут базы данных, что сказывается на скорости работы средств защиты информации, таких как средства аутентификации, DLP системы, анализаторы трафика и т.д. Одним из путей решения проблем скорости доступа является использование вероятностных структур данных, в частности – фильтр Блума.

Фильтр Блума – это вероятностная структура данных, позволяющая хранить и проверять принадлежность элемента к множеству [1]. В фильтре Блума возможны ложноположительные срабатывания. Фильтр Блума представляет собой битовый массив из m бит, которые по умолчанию обнулены. Далее, пользователю необходимо определить k независимых хеш-функций, которые будут преобразовывать массив входных данных произвольной длины в битовую строку фиксированной длины m достаточно равномерным способом. Процент ложноположительных может быть уменьшен увеличением размера массива m и/или числа хеш-функций k [2].

В данной работе был реализован фильтр Блума ($k = 3$, $m = 109$) и использован для определения необходимости вызова удаленной БД. Использование фильтра Блума в качестве структуры данных для хранения информации о наличии элемента в БД позволило сократить на 77 % используемую память по сравнению с хеш-таблицами, также незначительно уменьшило время на добавление состояния новых элементов в множество (> 5 %).

Литература

1. Bloom, B.H. Space/time trade-offs in hash coding with allowable errors.
2. Dillinger, P.C. Fast and Accurate Bitstate Verification for SPIN.

РАЗРАБОТКА ПРИЛОЖЕНИЙ ДЛЯ БЕЗОПАСНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ГОМОМОРФНОЙ КРИПТОГРАФИИ И ОЦЕНКА ИХ ЭФФЕКТИВНОСТИ

М.А. Кадан

С внедрением повсеместного использования облачных технологий остро встает вопрос сохранности данных и их безопасной обработки в облачных хранилищах. Разумным решением проблемы обеспечения конфиденциальности данных может служить шифрование всех приватных данных перед передачей в облако и обеспечение выполнения операций над зашифрованными данными, без их предварительного дешифрования, известное как гомоморфное шифрование [1].

Предметом доклада является применение гомоморфного шифрования в реализации безопасных мобильных приложений для облачных вычислений. Рассматривается задача определения требований к безопасности использования облачных хранилищ данных и подходов к проведению безопасных вычислений над данными облачного хранилища с использованием методов гомоморфного шифрования [2].

На основе теоретических принципов гомоморфного шифрования обоснован, спроектирован и реализован модуль для обеспечения возможности безопасного хранения и обработки данных в облачных структурах, не имеющий аналогов для решения задач данного рода на платформе iOS. Исследована эффективность использования метода гомоморфного шифрования в зависимости от максимальной длины операндов и ключа шифрования, а также исследована производительность модуля с использованием приложения на языке Swift.