УДК: 519.25; 004.8

НЕДОСТАТКИ NFC МЕТОК ПРИ АУТЕНТИФИКАЦИИ

А.Ю. Исхаков

В работе проводится исследование применимости технологии беспроводной высокочастотной связи малого радиуса в качестве транспорта аутентификационной информации. Исследование проводится в рамках разработки системы двухфакторной аутентификации с использованием программного токена, хранящегося в мобильном средстве связи.

Ключевые слова: NFC; аутентификация; идентификация; метка; токен.

Введение

Аутентификация является динамично развивающейся областью обеспечения информационной безопасности. Это обусловлено тем, что, по мере появления новых прогрессивных способов для ее реализации, появляются также и новые средства для осуществления нелегального получения привилегий в системе безопасности.

В современных системах контроля и управления доступом (СКУД) [1] процедура аутентификации пользователей при входе в здание зачастую реализуется посредством электронных проходных. Они представляются в виде турникетов, триподов [1], калиток, в стойки которых встроены контроллер и считыватель бесконтактных карт доступа.

Такое решение позволяет организовать контроль доступа и пропускной режим на предприятии наиболее удобным образом, реализуя возможность проведения учета рабочего времени.

В качестве носителей пользовательских идентификаторов широко используются бесконтактные карты доступа. Они являются классическим примером аутентификации 2 типа (Autentification by Ownership) [2], наследуя недостатки любой системы однофакторной аутентификации. В связи с этим предлагается механизм реализации двухфакторной аутентификации с использованием мобильного устройства связи (смартфона или коммуникатора) в качестве носителя пользовательского идентификатора

Данная реализация учитывает особенности процедуры аутентификации в электронных проходных, а также обладает следующими преимуществами по сравнению с аппаратными специализированными устройствами аутентификации:

- не требуется оснащение пользователей дорогостоящими аппаратными токенами [2, 3] / смарт-картами;
- пользователю нет необходимости носить с собой дополнительный предмет (токен / смарт-карту). Мобильные устройства являются наиболее распространенным средством связи, которым пользуется подавляющее большинство людей;
- частое использование телефона повышает вероятность быстрого обнаружения кражи (или потери) токена.

В связи с этим возникает вопрос о выборе технологии коммуникации сервера аутентификации и мобильных устройств пользователей.

Технология NFC меток

Технология беспроводной высокочастотной связи малого радиуса действия NFC [3], несомненно, является одним из наиболее популярных современных трендов в области бесконтактного транспорта данных.

Эта технология является расширением стандарта бесконтактных карт (ISO 14443), которая объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами и считывателями стандарта ISO 14443, и с другими устройствами NFC, и, таким образом, совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC, прежде всего, ориентирована на использование в мобильных телефонах.

В рассматриваемом вопросе о применимости данной технологии в качестве транспорта аутентификационных данных выделяется довольно важное преимущество в удобстве использования. В отличие от систем штрих-кодов или передачи данных по каналам передачи данных общего пользования (Wi-Fi, Bluetooth) в случае применения NFC система аутентификации характеризуется очень коротким временем для установки соедине-ния. Вместо выполнения инструкций по согласованию для идентификации устройства, связь между двумя устройствами NFC устанавливается моментально (менее чем за одну десятую секунды). Кроме того, техноло-

гия беспроводной высокочастотной связи малого радиуса действия может также работать, когда одно из устройств не снабжено источником питания (например, выключенный телефон не создаст препятствий пользователю при прохождении через электронный турникет).

Недостатки технологии беспроводной высокочастотной связи малого радиуса действия в вопросе аутентификации

Несмотря на вышеперечисленные преимущества в удобстве пользования, технология накладывает ограничение в виде необходимости наличия NFC модуля в мобильном средстве связи. Данный вопрос значительно сокращает модельный ряд смартфонов, которые возможно было бы применять в качестве аутентификаторов пользователя.

Кроме того, взаимодействие через радиоинтерфейс NFC открывает возможность злоумышленникам для активного поиска уязвимостей:

Подслушивание. Радиочастотный сигнал беспроводной передачи данных может быть перехвачен антеннами. Расстояние, с которого атакующий в состоянии подслушать радиочастотный сигнал, зависит от многочисленных параметров, но в любом случае — это всего несколько метров. Пассивное устройство, которое не производит собственное радиочастотное поле, намного тяжелее подслушать, чем активное устройство.

Стандарт NFC сам по себе не предлагает защиты против подслушивания. Поэтому стек протоколов должен использовать криптоалгоритмы поверх NFC для защиты данных.

Модификация данных. Разрушение данных относительно легко осуществить средствами радиоэлектронной борьбы (РЭБ). Нет способа предотвратить такое нападение, однако единственным его результатом будет невозможность установить связь.

Несанкционированная модификация данных внутри сообщения атакующим устройством нереализуема на практике в связи с невозможностью предсказать амплитуду и сдвиг фазы наведенного сигнала на приемном устройстве. RFID приемник чувствителен к внезапной смене амплитуды и фазы несущего сигнала.

Атака с использованием ретрансляции (Relay attack) [5]. Поскольку NFC устройства обычно также обеспечивают функциональность ISO 14443, описанная атака также выполнима и для NFC. Для этого нападения злоумышленник должен отправить жертве запрос считывателя и её ответ в режиме реального времени передать дальше на считывающее устройство. Это делается для того, чтобы выполнить задачу, симулирующую владение смарт-картой жертвы.

Однако на практике такая атака довольно затруднительна в связи с жёсткими ограничениями по времени на ответ запрашиваемого устройства. В некоторых случаях речь может идти о микросекундных допусках (например, при выполнении обязательной процедуры антиколлизии).

Вывод

Таким образом, дальнейшее развитие АСТПП необходимо осуществлять в направлении создания полноценной системы управления ЖЦ изделия (PLM). При этом обязательным условием должно стать наличие

Несмотря на то, что радиус действия рассматриваемой технологии ограничен несколькими сантиметрами, сама NFC не гарантирует безопасности соединений. Однако использование современных крипто алгоритмов позволяет обеспечивать безопасную передачу данных.

Учитывая, что число мобильных телефонов с NFC-функциональностью постоянно растет (сейчас на российском рынке представлено более 50 моделей устройств), можно утверждать, что через несколько лет данная технология станет хорошей альтернативой банковской карты для оплаты различных услуг с помощью мобильного телефона.

Однако значительные ограничения на наличие NFC модуля в современном модельном ряде мобильных устройств не позволяет использовать эту технологию в качестве единственного транспорта для передачи аутентификационной информации. [6,7]

СПИСОК ЛИТЕРАТУРЫ

1. Электронные проходные [Электронный ресурс]: Электрон. дан. [Москва] – Режим доступа: http://sotops.ru/catalog/elektronnye-prohodnye-Perco, свободный. Загл. с экрана.
2. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам. Учебное пособие для вузов. Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. Гриф УМО. - М.: Горячая линия - Телеком, 2009.- 552 с.: ил. ISBN 978-5-9912-0110-0
3. Костюченко, Е.Ю. Идентификация по биометрическим параметрам при использовании аппарата нейронных сетей/ Е.Ю. Костюченко, Р.В. Мещеряков // Нейрокомпьютеры: разработка, применение. 2007. № 7. С. 39-50.
4. Технология NFC и перспективы ее использования на транспорте [Электронный ресурс]: Электрон. дан. [Москва] – Режим доступа:

http://www.novacard.ru/ru/actual/?id= 850, свободный. Загл. с экрана.
5. How secure is NFC tech? [Электронный ресурс]: Электрон. дан. – Режим доступа: http://www.howstuffworks.com/how-secure-is-nfc-tech.htm, свободный. Загл. с экрана.
6. Сабанов, А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. 2012. № 2-1. С. 61-67.
7. Ходашинский, И.А. Технология усиленной аутентификации пользователей информационных процессов/ И.А. Ходашинский, М.В. Савчук, И.В. Горбунов, Р.В. Мещеряков // Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. № 2-3. С. 236-248.

***Исхаков А.Ю.**, инженер каф. КИБЭВС ТУСУР*

УДК: 004.42

РАЗРАБОТКА ИНТЕРНЕТ-ПОРТАЛА ПОДДЕРЖКИ МАЛОГО И СРЕДНЕГО БИЗНЕСА Г. ЮРГА

С.В. Сахаров

В статье рассматривается задача повышения эффективности поддержки малого и среднего бизнеса, посредством разработки и внедрения комплексного решения в виде интернет-портала. Информационная система представленная в статье уже частично реализована и проходит апробацию.

Ключевые слова: информационная система, интернет-портал, малый и средний бизнес, государство, экономика

Введение

Малый и средний бизнес играет большую роль в экономике, его развитие влияет на экономический рост, на ускорение научно-технического прогресса, на насыщение рынка товарами необходимого качества, на создание новых дополнительных рабочих мест, то есть решает многие актуальные экономические, социальные и другие проблемы. Для повышения уровня развития малого и среднего бизнеса, а также открытия новых направлений деятельности необходима всесторонняя поддержка со стороны государства. И это означает не только выделение средств из бюджета на целевые программы, а ещё создание грамотной информационной среды для бизнесменов. Сейчас, остро стоит вопрос о том, как сформировать информационную поддержку так, чтобы она была доступна для всех. Прежде всего, в этом должны быть заинтересованы органы, которые непосредственно работают с бизнесменами. Ведь одной из основных обязанностей центра поддержки малого и среднего бизнеса как раз и является информирование бизнесменов, начиная с процедур открытия бизнеса и заканчивая появлением целевых программ и конкурсов.

Способы информационной поддержки

Существуют различные способы информационной поддержки, различающиеся как по целевой аудитории, так и по способу представления информации. Одним из самых распространенных способов на сегодняшний день остаются публикации в СМИ. Этот способ направлен как на привлечение населения к созданию собственного бизнеса, путем создания различных конкурсов и программ, так и для информирования инвесторов о новых инвестиционных площадках. Другой путь для донесения информации до целевой группы - публикация на специализированных сайтах для людей, уже имеющих свой бизнес, а также для потенциальных инвесторов. Нельзя исключать и такой ключевой элемент, как центр поддержки малого и среднего бизнеса, который непосредственно взаимодействует с бизнесменами и является самым важным источником информации.

Проведенное исследование показывает, что существующие средства информационной поддержки не реализуют в полной мере описанные выше способы и не предоставляют комплексного подхода для решения сложившейся ситуации.

Интернет-портал для поддержки МСБ

Благодаря широкому распространению Интернета каждый бизнесмен, инвестор или просто человек, который хочет открыть собственный бизнес, могут получить необходимую информацию из Интернет-сайтов. Прошло то время, когда веб-сайты создавались просто как домашняя страничка пользователя. Сейчас, интернет-сайт - это мощный инструмент, который можно использовать как систему для управления и автоматизации различных процессов. Одной из разновидностей таких сайтов являются порталы. Портал