УДК 004.056

Аржаков А.В., Морозова Т.В., Сильнов Д.С.

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ ДЛЯ УВЕЛИЧЕНИЯ ДАЛЬНОСТИ СЧИТЫВАНИЯ RFID-ТРАНСПОНДЕРОВ СТАНДАРТА ISO-14443

АННОТАЦИЯ

В статье рассмотрены и проанализированы основные аспекты технологии радиочастотной идентификации (RFID), приведены основные области применения идентификационных меток. Описана проблема, связанная с увеличением дальности считывания RFID-транспондеров стандарта ISO-14443. Показано, какими преимуществами и недостатками обладает технология радиочастотного считывания транспондеров, проведена классификация меток. На основе проведенных исследований сделано заключение о тех областях жизни человека, к которым злоумышленники могут получить доступ, проводя несанкционированное считывание радиочастотных меток. Приводится обзор на уже существующие технологии, способные увеличить радиус действия скиммеров. Описаны значимые характеристики и возможности аппаратного средства Proxmark 3, которое позволяет реализовать процесс удалённого сканирования. Обозначена территория, на которой будет проводиться эксперимент с использованием разработанной антенны для увеличения радиуса считывания. Приведены основные задачи, которые необходимо решить для получения новых экспериментальных данных, описаны возможные перспективы в исследованиях.

КЛЮЧЕВЫЕ СЛОВА

RFID-технологии; скиммер; усиление радиочастотного сигнала; Proxmark3; транспондеры; уязвимость RFID; сканирование RFID.

Arzhakov A.V., Morozova T.V., Silnov D.S.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Russia

ANALYSIS OF EXISTING SOLUTIONS TO INCREASE ISO-14443 RFID-TAGS READING RANGE

ABSTRACT

In this article there is given an analysis of radio frequency identification technology (RFID) and basic ways for applying it. The problem associated with the increase of reading range of ISO-14443 standard is revealed and proved. There is described what areas of life can be accessed by attackers, who use unauthorized readers. Main advantages and disadvantages are described and types of transponders are classified. There is also given a survey on Proxmark 3 hardware, which is needed for scanning, and existing technologies in increasing skimmers working radius. Territory, on which the experiment with the developed antenna will be held, is specified. There is described main problem, which is needed to be solved, to obtain new experimental data and possible research aspects are described.

KEYWORDS

RFID-technologies; skimmer; RF signal amplification; Proxmark3; transponders; RFID vulnerability; RFID skanning.

В настоящее время все большее распространение получают различные технологии, призванные упростить или оптимизировать повседневные дела и трудовые будни. Некоторые из них остаются малозаметными, но при этом их вклад сложно переоценить. К одной из таких технологий можно смело отнести радиочастотную идентификацию, известную во всем мире как Radio Frequency IDentification или RFID (Рисунок 1). Данная технология применяется для осуществления автоматической идентификации объектов. Принцип действия таких технологий довольно прост: с помощью радиосигналов считываются или перезаписываются данные, хранящиеся в транспондерах (RFID-метках). Любая RFID-система состоит из считывателя информации и транспондера (носителя информации). Одним из важнейших преимуществ рассматриваемой технологии является возможность быстрого считывания информации, не требующая прямого контакта с самой меткой, а также отсутствие каких-либо требований к позиционированию метки относительно считывателя, что существенно упрощает и, следовательно, ускоряет сам процесс идентификации (считывания).

Рисунок 1 – применение RFID в повседневной жизни

Технология RFID получила широкое применение в следующих сферах:

- система контроля оплаты проезда. Практически во всех современных мегаполисах и крупных городах е применяется автоматизированные система контроля оплаты проезда на наземном и подземном общественном транспорте. В данном случае считывающее устройство располагается непосредственно на транспортном средстве, или же на проходной (например, в рамках подземной транспортной системы), а транспондером является проездной билет, внутри которого и располагается сама RFID-метка, содержащая информацию о текущем балансе или сроке действия;
- пропускная система. Применяется в ряде организаций с большим количеством личного персонала для предотвращения проникновения на объект (или в отдельные помещения) посторонних лиц или лиц с недостаточным уровнем допуска. Принцип действия аналогичен предыдущему пункту, за исключением того, что транспондер содержит информацию, которая позволяет идентифицировать личность владельца и его уровень допуска;
- организация складских помещений. Размещение RFID-меток внутри упаковочной тары с информацией о содержимом позволяет осуществлять сортировку товаров с большей скоростью, не нарушая целостности упаковки, что косвенно позволяет предотвращать хищение или порчу товаров;
- интеллектуальные транспортные системы. Одним из самых ярких примеров в данной области может послужить установка RFID-меток в государственные регистрационные знаки. Данная технология позволит в значительной степени повысить точность сбора исходных данных как для систем директивного (автоматизированные системы управления дорожным движением) и систем косвенного управления транспортными потоками (интеллектуальные системы информирования водителей транспортных средств), так и создает благоприятные условия для развития ИТС более высокого уровня (кооперативные интеллектуальные транспортные системы). Рассматриваемый вариант установки RFID меток уже существует в виде прототипов и находится на этапе тестирования и стандартизации;
- средства защиты от угона транспортных средств. Некоторые противоугонные системы предусматривают скрытую установку считывателей, и перед тем, как открыть автомобиль необходимо провести идентификацию RFID-метки, которая должна быть у водителя. В противном случае использование транспортного средства будет расцениваться как несанкционированное;
- в ряде других сфер деятельности (логистика, торговля, медицина и др.).

Применение RFID-транспондеров в данных областях значительно упрощает жизнь населения и процесс производства. Автоматизация процессов идентификации значительно экономит время и уменьшает вероятность возникновения ошибок, связанных с человеческим фактором.

RFID-системы можно классифицировать по дальности действия:

- ближней идентификации (расстояние до 20 см);
- средней идентификации (от 20 см до 5 м);
- дальней идентификации (от 5 до 300 м).

Также классификация может быть проведена по типу используемой памяти:

- RO – Read Only. Данные в памяти записываются только один раз при изготовлении. Этот способ хранения данных используется исключительно для идентификации;

- WORM – Write Once Read Many. Объем памяти увеличен в связи с тем, что кроме уникального идентификатора в ней хранятся какие-то данные, которые нельзя перезаписать, но можно многократно считывать;
- RW – Read and Write. Помимо идентификатора присутствует также блок многократно перезаписываемой памяти.

RFID-системы ближней идентификации регламентируются стандартом ISO-14443. Рабочая частота системы – 13,56 МГц. Дальность считывания таких меток обычно составляет 5-10 см. Данные транспондеры являются пассивными: они не будут передавать информацию до тех пор, пока не попадут в область действия считывателя. Считыватель генерирует электромагнитный импульс, возбуждая антенну, встроенную в метку (Рисунок 2). В случае, если транспондер принадлежит к классам RO или WORM, он передает данные только на считывание. Если транспондер принадлежит к классу RW, данные, находящиеся внутри него, также изменяются. В качестве примера RO(WORM)-метки можно привести пропуск на режимный объект такой, как НИЯУ «МИФИ». В качестве примера RW-меток можно привести систему оплаты в наземном транспорте и метрополитене г. Москвы: после каждого успешного прохода уменьшается количество поездок или денег на счету проездного билета.

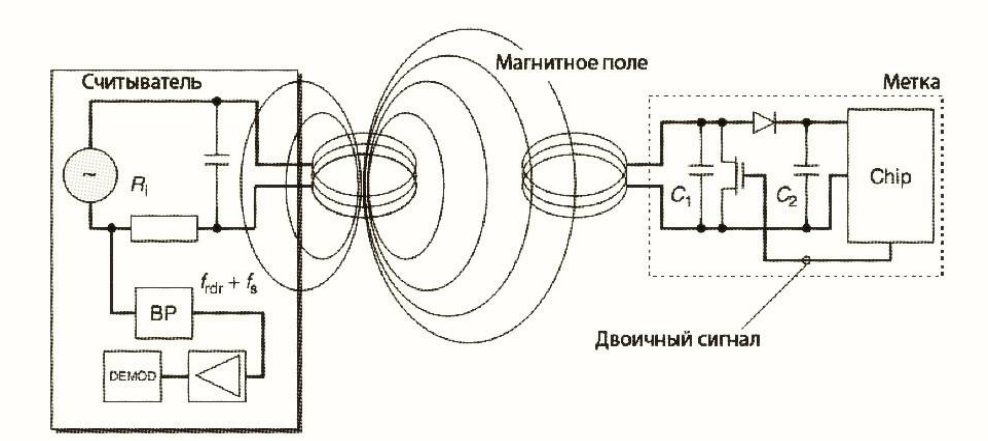

Рисунок 2 – принцип работы бесконтактных RFID-транспондеров

Метки RFID просты в использовании и изготовлении, имеют невысокую стоимость, в связи с этим их легко подделать. Так как данная технология является довольно свежей, в ней постоянно появляются какие-то новые аспекты, следовательно, технология является весьма уязвимой. Из-за распространенности меток стандарта ISO-14443 они постоянно подвергаются атакам злоумышленников с различными целями:

- подделка и перезапись проездных билетов. Атаке подверглись транспортные карты во нескольких мегаполисах. В России проводилось клонирование карт «Тройка» (г. Москва) и «Подорожник» (г. Санкт-Петербург). На билеты с исчерпанным количеством поездок записывались новые;
- кража персональных данных. Считав данные с бесконтактных кредитных карт можно легко использовать доступные на ней платежные средства без ведома владельца [1];
- угон автомобильных средств. Существуют виды автомобильных сигнализаций с RFID-метками. Чтобы получить доступ к транспортному средству, необходимо просканировать «ключом» каждую метку. Если есть возможность дублировать ключ, то можно беспрепятственно попасть в автомобиль;
- фальсификация товаров. В упаковках товаров, в частности, лекарств, производители помещают транспондеры, содержащие полную информацию о товаре. Просканировав метку, можно изменить любую информацию. Что еще хуже, метку также можно дублировать, а, следовательно, подделать товар;
- атаки через RFID-метки. Проведя редактирование информации, записанной на транспондере, можно получить доступ к компьютеру и внедрить вредоносный код через web-интерфейс или SQL-Injection.

Таким образом, проблема уязвимости технологии RFID встает очень остро. Для того, чтобы предупредить действия злоумышленников, необходимо знать, какими именно методами и способами скимминга они располагают. Это поможет лучше понять, насколько уязвимой является технология, и помочь в устранении этих уязвимостей.

Основным достоинством небольшого радиуса считывания являлось то, что злоумышленник мог получить данные с RFID-транспондера на крайне малом расстоянии (5-10 сантиметров), так как дальность считывания меток стандарта ISO-14443 уменьшается при наличии преград (например, пропуск находится в кармане или кошельке) [2]. Поэтому основной задачей недоброжелателей стала разработка

RFID-скиммера с увеличенным радиусом действия. В 2006 году в статье «How to Build a Low-Cost, Extended Range RFID Skimmer» (авторы – Ilan Kirschenbaum, Avishai Wool) был предложен вариант бюджетного RFID-скиммера с дальностью действия около 25 сантиметров, и это позволяет владельцу считывающего устройства производить захват данных, не находясь непосредственно рядом с жертвой, а, следовательно, не привлекать лишнего внимания [3]. Простые RFID-транспондеры «отвечают» на любой запрос независимо от того, можно ли доверять источнику запроса. Таким образом, попав в радиус действия магнитного поля считывателя, метка сразу становится уязвимой, и пока она находится в этом радиусе, можно изменить любые данные (если метка принадлежит к типу RW) или завладеть нужной информацией (для типов RO, WORM и RW).

Увеличение дальности считывания RFID-транспондеров стандарта ISO-14443 будет весьма полезно в интеллектуальных транспортных системах (сокращенно ИТС). На данный момент существуют прототипы государственных регистрационных знаков со встроенными RFID-метками. Такая конструкция помогает производить идентификацию транспортного средства с более высокой точностью. Это может быть использовано при оплате проезда по платным дорогам и как альтернатива дорожным камерам. При выполнении перестроения транспортное средство может не попасть в радиус действия. Поэтому увеличение диапазона захвата позволит производить более корректное считывание информации с транспондеров.

Таким образом, увеличение радиуса считывания RFID-меток стандарта ISO-14443 может послужить как минимум двум целям:

- улучшение системы считывания RFID-транспондеров в интеллектуальных транспортных системах;
- лучшее понимание методов несанкционированного доступа к личным данным.

Так как подробно рассмотреть первую из целей автору не представляется возможным, анализ проблемы будет проведен на примере второй из предложенных целей.

Существует два варианта увеличения дальности считывания:

- усиление электромагнитного поля со стороны приемника сигнала (самого транспондера);
- усиление электромагнитного поля со стороны источника сигнала (считывателя).

Единственным возможным методом усиления сигнала от транспондера является преобразование пассивной метки в активную. Активные RFID-транспондеры характеризуются собственным источником энергии, следовательно, они могут сами генерировать электромагнитное поле. Но этот способ потребует много денежных и производственных ресурсов. Следовательно, единственным выходом остается усиление поля источника поля. Самым простым вариантом решения этой задачи является конструирование антенны-усилителя.

В рамках означенного исследования стоит задача разработки антенны-усилителя для RFID-скиммера «Proxmark3» (Рисунок 3). Это устройство было разработано для обнаружения, считывания и клонирования RFID-транспондеров низкой (125 кГц) и средней (13.56 МГц) частот.

Рисунок 3 – устройство Proxmark3

Proxmark3 – многофункциональное устройство. Оно может быть использовано в качестве:

- считывателя (возбудителя сигнала для активации пассивной RFID-метки);
- подслушивающего устройства (принцип работы похож на криптографическую атаку «человек посередине»);
- меткой (то есть может принимать данные от источника).

В рамках исследовательской работы необходим только режим работы считывателя. Устройство Proxmark3 позволяет считать данные с RFID-транспондера и вывести полную информацию, хранящуюся в памяти транспондера, на монитор, используя пользовательский интерфейс (Рисунок 4). Если злоумышленники обладают этой информацией, они получают возможность перепрограммировать или дублировать метку с целью хищения информации, денежных средств и получения доступа к защищенным данным и закрытым помещениям.

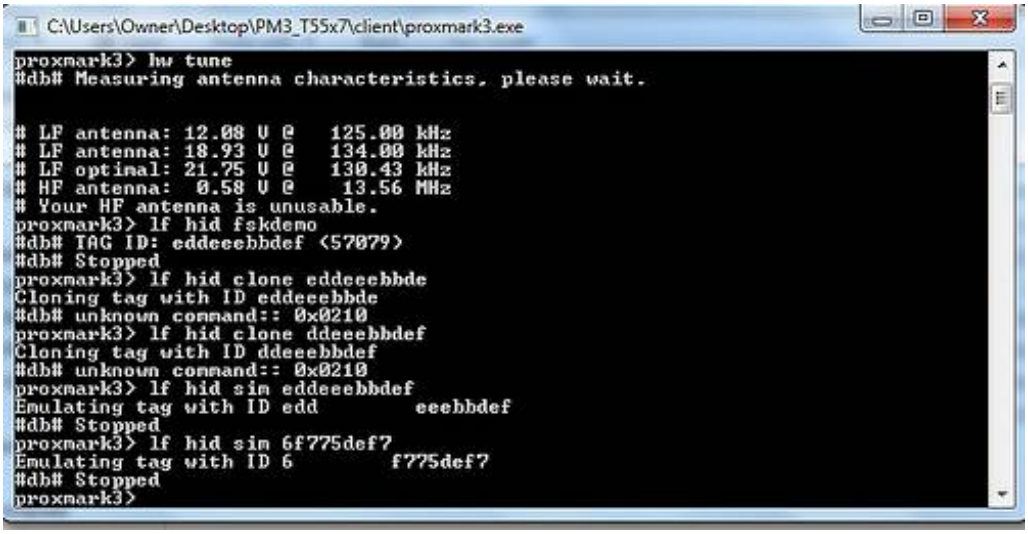

Рисунок 4 – консольное окно приложения Proxmark3

Проведение испытаний скиммера с увеличенной дальностью работы на основе Proxmark3 будет осуществляться на проходной НИЯУ «МИФИ» с целью выявления уязвимости пропускной системы университета. Это поможет указать на ее недостатки и уязвимые места, и, как следствие, повысить уровень безопасности. Решение поставленной задачи может быть предложено как часть разработки качественно новой полезной модели с последующим патентованием.

Литература

1. Wim Aerts, Elke De Mulder, Bart Preneel, Guy A. E. Vandenbosch, Senior Member, IEEE, and Ingrid Verbauwhede, Senior Member, IEEE Dependence of RFID Reader Antenna Design on Read Out Distance // IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION. - 2008. -VOL. 56, NO. 12.
2. Chris Paget Extreme-range RFID tracking // Blackhat USA. - Las Vegas: Blackhat USA, 2010.
3. Ilan Kirschenbaum, Avishai Wool How to Build a Low-Cost, Extended-Range RFID Skimmer // - Vancouver, Canada: Usenix Security, 2006.

References

1. Wim Aerts, Elke De Mulder, Bart Preneel, Guy A. E. Vandenbosch, Senior Member, IEEE, and Ingrid Verbauwhede, Senior Member, IEEE Dependence of RFID Reader Antenna Design on Read Out Distance // IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION. - 2008. -VOL. 56, NO. 12.
2. Chris Paget Extreme-range RFID tracking // Blackhat USA. - Las Vegas: Blackhat USA, 2010.
3. Ilan Kirschenbaum, Avishai Wool How to Build a Low-Cost, Extended-Range RFID Skimmer // - Vancouver, Canada: Usenix Security, 2006.

Поступила: 15.09.2016

Об авторах:

Аржаков Антон Валерьевич, магистрант кафедры компьютерных систем и технологий Национального Исследовательского Ядерного Университета «МИФИ», zdj22@yandex.ru;

Морозова Татьяна Васильевна, студент кафедры компьютерных систем и технологий Национального Исследовательского Ядерного Университета «МИФИ», tatyana.enot@gmail.com;

Сильнов Дмитрий Сергеевич, кандидат технических наук, доцент кафедры компьютерных систем и технологий, Национального Исследовательского Ядерного университета «МИФИ», ds@silnov.pro.