УДК 004.056.2 Вестник УрФО № 4(50) / 2023, с. 53–59

Неклюдов Д.Н., Лебедь А.С., Кузьмина У.В.

DOI: 10.14529/secur230405

ИССЛЕДОВАНИЕ АТАК НА БЕСКОНТАКТНЫЕ СМАРТ-КАРТЫ И RFID-МЕТКИ

В данной статье рассматриваются особенности безопасности бесконтактных смарт-карт и RFID-меток, широко используемых в настоящее время. Приведены результаты практического исследования уязвимостей и потенциальных атак на эти устройства, также представлены результаты экспериментов по созданию и использованию скиммера для считывания данных с карт. Описаны атаки, основанные на восстановлении секретных ключей, которые могут быть использованы злоумышленниками. Рассматриваются такие атаки, как Lock Attack, Darkside Attack, Nested Attack и Communication Interception Attack, и описываются методы и инструменты для их реализации. Предлагаются рекомендации по улучшению защиты и безопасности бесконтактных смарт-карт и RFID-меток.

Ключевые слова: *информационная безопасность, угроза безопасности информации, системы контроля и управления доступом, RFID-метка, бесконтактная карта, скимминг, смарт-карта.*

Neklyudov D.N., Lebed A.S., Kuzmina U.V.

RESEARCH ON ATTACKS AGAINST CONTACTLESS SMART CARDS AND RFID TAGS

This article examines the security features of contactless smart cards and RFID tags, which are widely used today. The results of a practical study of vulnerabilities and potential attacks on these devices are presented, and the results of experiments on the creation and use of a skimmer for reading data from cards are also presented. Attacks based on the recovery of secret keys that could be exploited by malicious actors are described. Attacks such as the Lock Attack, Darkside Attack, Nested Attack, and Communication Interception Attack are discussed, along with methods and tools for their implementation. Recommendations for improving the protection and security of contactless smart cards and RFID tags are also provided.

Keywords: *information security, information security threat, access control and management system, RFID-tag, contactless card, skimming, smart card.*

В связи с растущей потребностью в обеспечении безопасности транспорта и контрольно-пропускных пунктов бесконтактные карты и брелоки становятся все более популярными способами идентификации ввиду простоты устройства, низкой стоимости и практичности. Обеспечение охраны путем разграничения доступа данной технологией используется на большинстве современных объектов. Несмотря на обширность примене-

ния, системы имеют критические незакрытые уязвимости, из-за которых обеспечение безопасности таких систем является большой проблемой, о которой некоторые пользователи даже не подозревают.

Информация на самых популярных метках MIFARE Classic 1K состоит из 16 секторов памяти, каждый из которых включает 4 блока. Другие же метки могут отличаться количеством блоков и памятью, однако, это несущественно. Нулевой блок нулевого сектора содержит уникальный идентификатор и информацию о производителе, за которым идет контрольный байт (BCC), вычисленный при помощи операции XOR. Блок программируется при производстве чипа и имеет защиту от перезаписи. Каждый четвертый блок сектора называется трейлер, он содержит 2 ключа доступа к каждому блоку и условия доступа [2]. Трейлер хранит ключ A, обязательный для чтения и опциональный ключ B, а также условия доступа к 6 – 9 блоку. Условия доступа определяют, какие операции доступны для этого сектора. Считыватель должен пройти аутентификацию для сектора, прежде чем будут разрешены какие-либо операции с памятью. Схема памяти карты mifare Classic 4k представлена на рисунке 1.

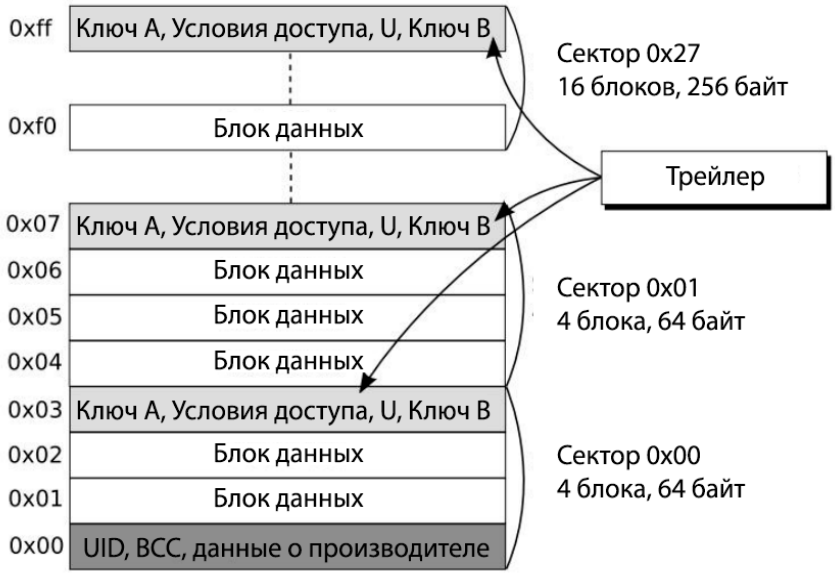

Рис. 1. Устройство памяти карты MIFARE Classic 4k

Трейлер имеет особые условия доступа. Ключ A никогда не читается, а ключ B может быть настроен как читаемый или нет. В этом случае память используется только для хранения данных, а ключ B не может использоваться в качестве ключа аутентификации. Помимо AC – условий доступа, и ключей, остается один байт данных – U, неопределенный байт, который может использоваться для хранения данных.

Блок данных используется для хранения произвольных данных или может быть настроен как блок значений. При использовании в качестве блока значений 4-байтовое значение со знаком сохраняется последовательно: дважды неинвертированным и один раз инвертированным. Эти четыре байта хранятся от младшего значащего байта слева до старшего значащего байта справа. Оставшиеся 4 байта используются для хранения блок адреса, который может быть задействован в качестве указателя. Схема трейлера представлена на рисунке 2.

Большинство команд связаны с блоком данных (набор команд MIFARE Classic) требуют, чтобы считыватель был аутентифицирован для сектора. Условия доступа проверяются каждый раз при выполнении команды, чтобы определить, разрешено это или нет. Блок данных может быть настроен только для чтения.

Существует несколько способов осуществления атак на восстановление секретных ключей карт, с помощью которых злоумышленник может скомпрометировать информацию с карты жертвы:

• card-only attacks (злоумышленник имеет считыватель, ему достаточно только карта для осуществления атаки);

• перехват логов во время обмена данными карты и считывателя.

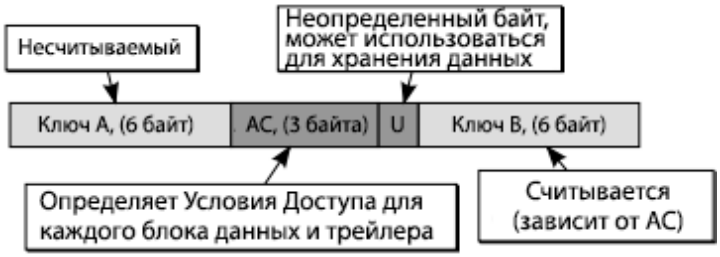

Рис. 2. Содержание трейлера

В обоих случаях злоумышленнику необходимо определенное устройство, выполняющее функции считывателя. Таким устройством может выступать как смартфон с NFC-чипом и установленной утилитой (например, NXP TagInfo), так и специализированное оборудование, такое как Proxmark3 [8]. В первом случае смартфон не может прочитать все стандарты карт, а Proxmark3, несмотря на то, что это уже готовое решение, не подвержено модификации, в случае необходимости, не говоря о том, что стоимость данного продукта в несколько раз выше, чем стоимость реализации такого устройства своими руками. Несмотря на то, что за создание и дистрибьюцию такого устройства предусмотрена уголовная ответственность по статье 138.1 УК РФ «Незаконный оборот специальных средств, предназначенных для негласного получения информации» в виде лишения свободы на срок до четырех лет, устройство, как и его комплектующие, свободно распространяются в сети Интернет.

В рамках исследования был собран скиммер. Для этого нам понадобилось: программируемый микроконтроллер; модуль, считывающий смарт карты; источник питания; перезаписываемые карты; программное обеспечение.

В качестве микроконтроллера подойдут любые контроллеры, например, семейства Arduino (для компактности можно использовать Arduino Mini). Устройство для считывания смарт карт и RFID-меток высокой частоты– Mifare RC522 или, в случае, если понадобится считать карты, работающие на низкой частоте – RDM6300 UART. Перезаписываемые карты – Mifare Zero. Источником питания может быть все, начиная от батарейки до портативного аккумулятора или смартфона.

Собранное устройство (рис. 3), может считывать, как низкочастотные карты, так и высокочастотные, из-за двух считывающих модулей.

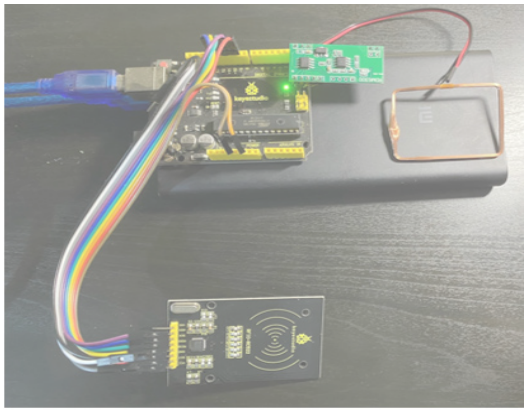

Рис. 3. Разработанный скиммер

За счет его программируемости, оно может осуществлять следующие атаки:

- Lock Attack;
- Nested Attack;
- Darkside Attack;
- Communication interception Attack;

Lock Attack - атака, использующая возможность изменения лок-битов карты, преимущественно применима для транспортных карт.

Например, в lock секторе карты MIFARE ULTRALIGHT мы можем заблокировать статус сектора OTP, что делает невозможным изменение его битов на 1.

Путем установки 4-ого бита первого байта в значение 1, мы заблокировали сектор OTP (рис. 4).

HEX	F2 03
BIN	1111**0**010 00000011
HEX	FA 03
BIN	1111**1**010 00000011

Рис. 4. Изменение lock бита

Изменяя лок-биты, можно добиться невозможности перезаписи контрольной суммы (т.е. количество поездок) валидатором, с

сохранением доступа в транспортную систему. Как итог – «вечный» проездной [1].

Darkside Attack – атака, которая заключается в том, что во время аутентификации, тег проверяет биты четности. Если один из восьми битов четности неверен, тег не отвечает. Однако, если все восемь битов четности верны, но ответ неверен, тэг ответит 4-битным код ошибки 0x5 (NACK), указывающий на ошибку передачи [9]. Более того, этот 4-битный код ошибки отправляется в зашифрованном виде. Если злоумышленник объединит (XOR) значение кода ошибки 0x5 (известный открытый текст) с его зашифрованной версией, он может восстановить четыре бита ключевого потока.

Атака может осуществляться с помощью утилиты MFCUK (MiFare Classic Universal toolKit) [10]. Утилита помогает, при помощи перебора словарей, получить первичный ключ сектора (рис. 5, 6).

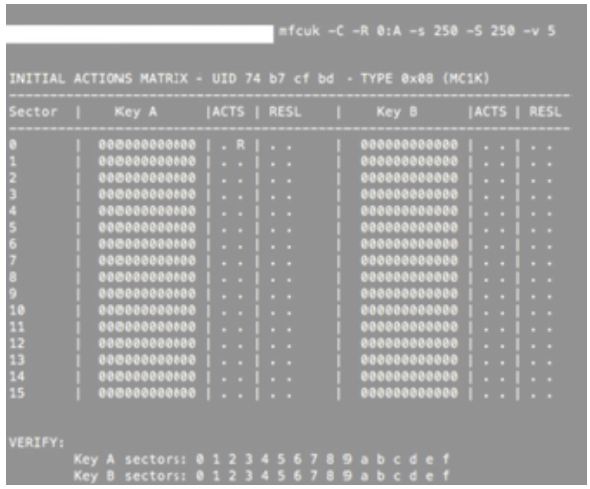

Рис. 5. MFCUK

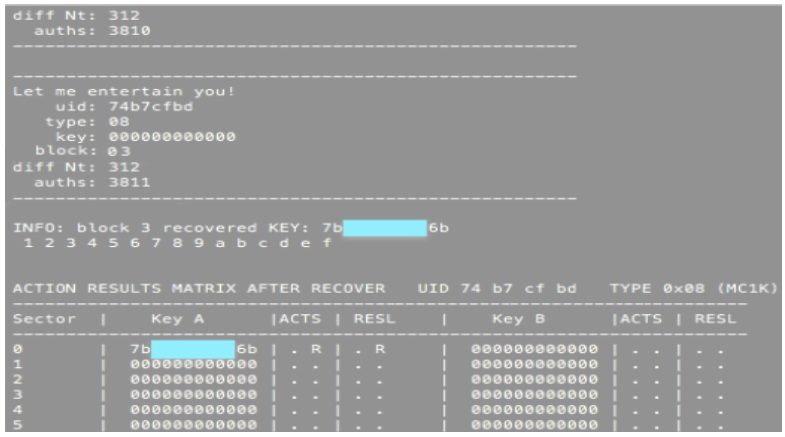

Рис. 6. Получение ключа используя Darkside attack

Полученный ключ можно использовать при реализации следующих атак.

Nested Attack – смысл атаки заключается в подборе паролей исходя из известного ключа к одному блоку данных. Атака является результатом уязвимости генератора псевдослучайных чисел (ГПСЧ), которая заключается в утечке битов кода ошибки и битов четности. Чтобы атака считалась успешной необходимо знать хотя бы один секретный ключ любого блока, из-за чего можно восстановить ключи к оставшимся блокам [3]. Атака работает для любых карт с CRYPTO1.

Реализованный нами скиммер может осуществлять данную атаку за счет записи дампа смарт-карты. Благодаря открытой утилите MFOC (Mifare Classic Offline Cracker) (рисунок 7), зная один из секретных ключей, можно восстановить второй секретный ключ сектора или всех секторов сразу (рис. 9). Данный алгоритм, как и MFCUK, при большем объемом памяти микроконтроллера, можно вшить в само устройство, тем самым реализовать атаку без использования второстепенных устройств.

Communication Interception Attack – ата-

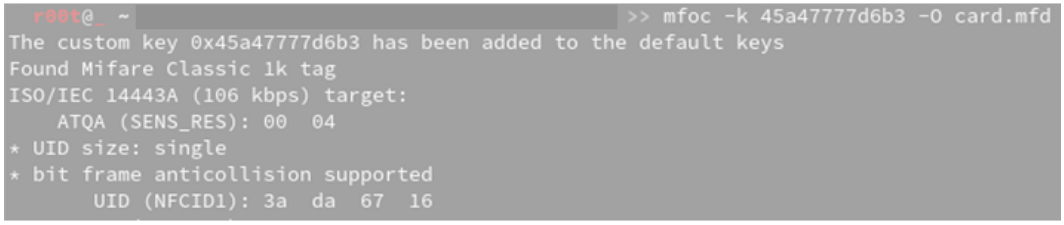

Рис. 7. Запуск MFOC

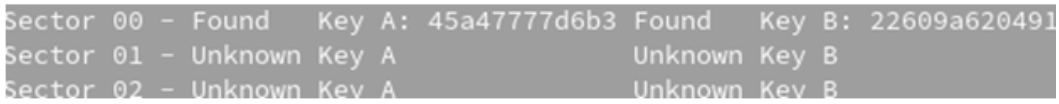

Рис. 8. Восстановление ключа B

ка, позволяющая провести откат состояния регистра LFSR (от англ. Linear Feedback Shift Register – линейный регистр с обратной связью) до первоначального. Заключается в восстановлении ключа для шифрования перехваченной фазы аутентификации между интеррогатором и транспондером. Важным условием, стоит отметить то, что оба устройства должны знать секретный ключ. Атака использует два ключевых недостатка в потоковом шифре CRYPTO1, а именно возможность восстановления состояния LFSR вследствие того, что в генераторе фильтров используются только нечетные биты, что в свою очередь позволяет откатить состояние регистра до первоначального из-за того, что первые девять битов LFSR не используются генератором фильтров [4]. Данная атака основана на механизме двух вышеупомянутых атак.

В качестве рекомендаций по защите бесконтактных смарт карт и RFID-меток может быть предложено их хранение в картхолдерах, футлярах или кошельках из радио непроницаемых материалов (например, они могут быть изготовлены из алюминия, карбона или других менее дорогих материалов, таких как фольга). Осуществить переход на более современные стандарты карт с более совершенными алгоритмами шифрования данных. В прошивке интеррогатора установить дополнительную проверку на блокировку сектора OTP.

Литература

1. Медведев Н.М., Лукьянов Г.И., Баранкова И.И. Оценка надежности использования RFID-технологии / Сбродова Е.А., М.А. Загребин // Безопасность информационного пространства. 2018. Т.1. С. 169-173.

2. Цапов А.Е., Литвинова А.В., Лукьянов Г.И. Оценка безопасности СКУД на базе RFID-системы / Баранкова И.И., Михайлова У.В., Лукьянов Г.И. // Актуальные проблемы современной науки, техники и образования. 2021. Т.1. С. 404.

3. Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur Wirelessly Pickpocketing a Mifare Classic Card / Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur [Электронный ресурс] // Researchgate:[сайт].—URL: https://www.researchgate.net/publication/220713937_Wirelessly_Pickpocketing_a_Mifare_Classic_Card.

4. Шинкевич Н.Н. ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ БЕСКОНТАКТНЫХ СМАРТ-КАРТ НА ПРИМЕРЕ MIFARE CLASSIC / Шинкевич Н.Н. [Электронный ресурс] // Cyberleninka : [сайт]. — URL: https://cyberleninka.ru/article/n/issledovanie-bezopasnosti-beskontaktnyh-smart-kart-na-primere-mifare-classic/viewer.

5. Sarrias M. B., Jordi H. J. Security in RFID devices / Marti Berini Sarrias, Jordi Herrera Joancomartí [Электронный ресурс] // Universitat Autònoma de Barcelona. Escola d'Enginyeria.: [сайт]. — URL: https://ddd.uab.cat/pub/trerecpro/2013/hdl_2072_232718/PFC_MartiBeriniSarrias.pdf.

6. Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijrers et al Dismantling MIFARE Classic / Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijrers et al [Электронный ресурс] // 13th European Symposium on Research in Computer Security: [сайт]. — URL: https://www.cs.bham.ac.uk/~garciaf/publications/Dismantling.Mifare.pdf.

7. Lupták P. Mifare Classic analysis / Pavol Lupták [Электронный ресурс] // nethemba: [сайт]. — URL: https://nethemba.com/resources/mifare-classic-slides.pdf.

8. Larson K. Mifare Smart Card Security / Larson Kevin [Электронный ресурс] // Incyber: [сайт]. — URL: https://incyber.org/en/mifare-smart-card-security-by-kevin-larson.

9. Courtois N.T. THE DARK SIDE OF SECURITY BY OBSCURITY and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime / Nicolas T. Courtois [Электронный ресурс] // eprint: [сайт]. — URL: https://eprint.iacr.org/2009/137.pdf .

10. Márcio Almeida Hacking Mifare Classic Cards / Márcio Almeida [Электронный ресурс] // www.blackhat.com: [сайт]. — URL: https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

References

1. Medvedev N.M., Luk'janov G.I., Barankova I.I. Ocenka nadezhnosti ispol'zovanija RFID-tehnologii / Sbrodova E.A., M.A. Zagrebin // Bezopasnost' informacionnogo prostranstva. 2018. T.1. S. 169-173.

2. Capov A.E., Litvinova A.V., Luk'janov G.I. Ocenka bezopasnosti SKUD na baze RFID-sistemy / Barankova I.I., Mihajlova U.V., Luk'janov G.I. // Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija. 2021. T.1. S. 404.

3. Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur Wirelessly Pickpocketing a Mifare Classic Card / Garcia Flavio D., Peter van Rossum, Roel Verdult, Ronny Wichers Schreur [Electronic resource] // Researchgate:[website].—URL: https://www.researchgate.net/publication/220713937_Wirelessly_Pickpocketing_a_Mifare_Classic_Card.

4. Shinkevich N.N. SECURITY RESEARCH OF CONTACTLESS SMART CARDS ON THE EXAMPLE OF MIFARE CLASSIC / Shinkevich N.N. [Electronic resource] // Cyberleninka: [website]. — URL: https://cyberleninka.ru/article/n/issledovanie-bezopasnosti-beskontaktnyh-smart-kart-na-primere-mifare-classic/viewer.

5. Sarrias M. B., Jordi H. J. Security in RFID devices / Marti Berini Sarrias, Jordi Herrera Joancomartí [Electronic resource] // Universitat Autònoma de Barcelona. Esc ola d'enginyeria.: [website]. — URL: https://ddd.uab.cat/pub/trerecpro/2013/hdl_2072_232718/PFC_MartiBeriniSarrias.pdf.

6. Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijrers et al Dismantling MIFARE Classic / Garcia Flavio D., Gerhard de Koning Gans, Ruben Muijrers et al [Electronic resource] // 13th European Symposium on Research in Computer Security: [website]. — URL: https://www.cs.bham.ac.uk/~garciaf/publications/Dismantling.Mifare.pdf.

7. Lupták P. Mifare Classic analysis / Pavol Lupták [Электронный ресурс] // nethemba: [сайт]. — URL: https://nethemba.com/resources/mifare-classic-slides.pdf.

8. Larson K. Mifare Smart Card Security / Larson Kevin [Электронный ресурс] // Incyber: [сайт]. — URL: https://incyber.org/en/mifare-smart-card-security-by-kevin-larson

9. Courtois N. T. THE DARK SIDE OF SECURITY WITH THE HELP OF OBSCURITY and cloning of classic MiFare railway and construction passes anywhere and anytime / Nicholas T. Courtois [Electronic resource] // eprint: [website]. — URL: https://eprint.iacr.org/2009/137.pdf.

10. Márcio Almeida Hacking Mifare Classic Cards / Márcio Almeida [Electronic resource] // www.blackhat.com: [website]. — URL: https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf.

НЕКЛЮДОВ Данил Николаевич, студент 4 курса по специальности «Информационная безопасность автоматизированных систем» кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: dejeksdan@gmail.com

NEKLYUDOV Danil Nikolaevich, 4th year student majoring in "Information Security of Automated Systems" department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: dejeksdan@gmail.com

ЛЕБЕДЬ Александр Сергеевич, студент 4 курса по специальности «Информационная безопасность автоматизированных систем» кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: mail23032019@mail.ru

LEBED Alexander Sergeevich, 4th year student majoring in "Information Security of Automated Systems" department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: mail23032019@mail.ru

КУЗЬМИНА Ульяна Владимировна, кандидат технических наук, доцент кафедры информатики и информационной безопасности, ФГБОУ ВО «Магнитогорский государственный технический университет им Г.И. Носова». 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: Ylianapost@gmail.com

KUZMINA Ulyana Vladimirovna, candidate of Technical Sciences, associate professor of the department of Computer Science and Information security, Nosov Magnitogorsk State Technical University, 455000, Magnitogorsk, Lenin Ave., 38. E-mail: Ylianapost@gmail.com