УДК 004.056.53

Атаки на смарт-карты. Методы защиты смарт-карт

Лыонг Ха Ча Ми [1], А. Р. Тахаутдинов [2], А. А. Привалова [3]

[1] lhtrmi0212@gmail.com, [2] aidartahasutdinov@gmail.com, [3] bruder.ocn@gmail.com

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Аннотация. В статье рассмотрены атаки на интеллектуальные карты, а также их классификация по уровню осуществления атаки и по фазе жизненного цикла самой смарт-карты. Затронута проблема обеспечения безопасности смарт-карт и меры их защиты.

Ключевые слова: смарт-карты; информационная безопасность; атака; методы защиты; smart-cards; information security; attack; protect.

ВВЕДЕНИЕ

В связи со стремительным развитием информационных технологии и массовым внедрением в них использование смарт-карт, возникает вопрос об уровне обеспечения информационной безопасности интеллектуальных карт и методах их защиты от несанкционированного доступа.

Целью данной работы является рассмотрение различных видов атак на смарт-карты и выработка методов и средств ее защиты.

Смарт-карта (англ. smart card – интеллектуальная карта) представляет собой устройство в виде пластиковой карты, которая в основном содержит микропроцессор и операционную систему, контролирующую доступ к объектам в памяти [1]. Главным ее компонентом является кремниевый чип, который представляет собой встроенную часть аппаратного обеспечения. Смарт карта позволяет проводить криптооперации в доверенной среде, хранить важную ключевую информацию, а также осуществлять аутентификацию и идентификацию пользователя. Смарт-карты находят свое широкое применение в таких областях и сферах деятельности как банковские кредитные карты, различные системы лояльности, например карты для накопления баллов, проездная карта, студенческий билет, применение электронной цифровой подписи и электронные паспорта. Веб-браузеры также могут использовать технологию смарт-карт в дополнение к протоколу Secure Sockets Layer (SSL) для повышения безопасности интернет-транзакций [2].

С учетом вышесказанного можно выделить ряд преимуществ «умной» карты:

– Высокая надежность. Копирование данных, кроме как их производителями, практически невозможно благодаря уникальному внутреннему коду , записанному на каждой карте;

– Долговечность использования. Микросхема карты изнашивается медленно, а микропроцессор в целом выдерживает значительнее ударные и температурные нагрузки;

– Многофункциональность. Смарт-карты могут осуществлять многие математические и логические операции, что дает возможность использовать их в различных информационных сферах;

– Высокие эксплуатационные характеристики. Например:

а) время хранения информации – 10 лет;

б) минимальное число перезаписей – 10 000 раз;

в) время записи одного байта информации – не более 10 мс;

г) температура хранения – от – 20 до +55° С [3].

АТАКИ НА СМАРТ-КАРТЫ

На сегодняшний день многие утверждают, что смарт-карты являются наиболее безопасными технологиями для хранения данных и аутентификации из-за невозможности их вскрытия. Но так ли это на самом деле?

К сожалению, с развитием информационных технологий растет и количество атак, направленных на нарушение целостности, доступности и конфиденциальности информации, находящейся на смарт-картах.

Существуют различные подходы к систематизированной классификации атак на смарт-карты. Рассмотрим виды атак по уровню их проведения:

1. Атака на смарт-карты на социальном уровне.

Объектом атаки на социальном уровне являются люди, которые работают со смарт-картами. Ими могут быть, например, держатели смарт-карт, разработчики чипов, разработчики программного обеспечения. Но данная атака маловероятна при должной организации мер безопасности. Например, можно легко предотвратить перехват PIN-кода при подсматривании процесса его набора на клавиатуре, если установить непрозрачные экраны по обе стороны клавиатуры. Атаки на социальном уровне против программистов смарт-карты становятся бесполезными при разработке ими процедур, которые будут использоваться открыто, а также при привлечении третьей стороны для оценки программных кодов, разработанных этими программистами. [4]

2. Атака на смарт-карты на физическом уровне.

Для реализации данной атаки обычно требуется сложное техническое оборудование, поскольку злоумышленнику нужно получить физический доступ к аппаратным средствам микроконтроллера смарт-карты.

Выделяют три основных вида физических атак:

а) Активные атаки с проникновением

Данный вид атаки подразумевает проникновение в саму микросхему. Примерами таких атак являются атаки на основе проб (probe attacks), часто комбинированные с различными методами снятия корпуса микросхемы и послойного доступа к топологии кристалла (machining methods) и другие. [5]

б) Активные атаки без проникновения

Это атаки, основанные на генерации «случайных» аппаратных ошибок во время исполнения криптоалгоритма. Например, злоумышленник пытается нарушить правильную работу карты для вскрытия ключей шифрования, путем изменения параметров внешней среды (напряжения питания, температуры, тактовой частоты). Атакующий может увидеть при этом как корректный результат работы функции шифрования, так и ошибочный, а анализ разницы между ними позволяет провести «обратный инжиниринг» процесса шифрования и попытаться вскрыть ключ шифрования. Методами атак без проникновения являются DFA (дифференциальный анализ неисправностей), воздействие лазером или пучком электронов, а также другие методы.

в) Пассивные атаки

При пассивной атаке злоумышленник может выполнить измерения на полупроводниковом устройстве либо анализировать шифр-текст или криптографический протокол, не изменяя его. [6]. Атаки по энергопотреблению (SPA и DPA), атаки по времени, атаки по электромагнитному излучению – примеры пассивных атак на смарт-карты.

3. Атака на смарт-карты на логическом уровне.

Данная категория атак включает классический криптоанализ, а также атаки, использующие известные неисправности в операционной системе смарт-карты и «троянских коней» в исполняемом коде приложений смарт-карты. [6]. Логические атаки обычно применяются вместе с другими видами атак. Атака на физическом уровне может подготовить путь для последующей атаки на логическом уровне, в качестве которой может быть применен, например, дифференциальный анализ после намеренно введенной неисправности.

Выделяют также атаки по времени их проведения , то есть фазе жизненного цикла смарт-карты. В основные фазы жизненного цикла интеллектуальной карты входят:

1. разработка смарт-карт;
2. производство смарт-карт;
3. применении смарт-карт в приложениях.

В связи с этим рассмотрим атаки по данной классификации:

– Атака в фазе разработки смарт-карт происходит в момент разработки чипа, разработки операционной системы и генерации приложений. Зачастую, атака на рассматриваемой фазе осуществляется путем манипулирования аппаратным и программным обеспечением.

– Атака в фазе производства смарт-карт связана со всеми процессами производства смарт-карты от производства полупроводниковых пластин до персонализации карт и их отправки конечным пользователям.

– Атака в фазе применения смарт-карт в приложениях. Последняя фаза характеризуется атаками на прикладные системы и приложения, которые непосредственно используют смарт-карты. На этом этапе вероятность получения доступа к данным смарт-карты становится относительно высокой по сравнению с атаками на фазе производства, так как получение доступа к элементам смарт-карты после ее выпуска становится легче.

Важно отметить, что уже на начальной стадии жизненного цикла смарт-карты необходимо принять меры по обеспечению ее безопасности.

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ СМАРТ-КАРТ

Смарт-карты чаще всего используются, в приложениях и деятельности которых требуется высокая надежность и достаточный уровень безопасности. Задача применяемых мер по защите смарт-карт состоит в том, чтобы максимально затруднить работу нарушителя и в конце концов довести его затраты сил и средств до того уровня, когда они перестанут окупаться, так как полностью обезопасить смарт-карту от взлома пока не представляется возможным.

Современный микропроцессор смарт-карты имеет несколько уровней защиты от несанкционированного доступа к информации, которая хранится в нем: программный, аппаратный и технологический.

1. Программный уровень защиты. В нем используются такие средства и методы обеспечения защиты, как защита PIN-кодом с противодействием его подбору, взаимная аутентификация между картой и терминалом, шифрование данных, использование сеансовых ключей для всех криптографических преобразований и другие.

2. Аппаратный уровень защиты. Для данного уровня защиты в микросхеме реализуются специальные датчики, устройства и элементы: детектор пониженной и повышенной тактовой частоты, стирание области ОЗУ при сбросе или срабатывании датчиков, защита от высокочастотных помех, уникальный идентификационный номер чипа, уникальные характеристики шифрования, защита от подключений зондами.

3. Технологический уровень защиты характеризуется приемами, которые затрудняют несанкционированное извлечение информации на смарт-карте. Таким образом создаются многослойные структуры кристаллов (до 22 слоев), ответственные части схемы (ПЗУ и ЭСПП ЗУ) помещаются внутрь, вводятся дополнительные слои металлизации.

Рассмотрим методы защиты смарт-карт. Меры защиты смарт-карт можно разделить на три основные группы:

– Физические меры. Основным методом физической защиты противодействия от атак является использование датчиков состояние среды, датчиков состояния предметов.

– Программные меры. К ним относятся:

а) Контроль целостности данных;

б) Контроль потока управления;

в) Рандомизация вычислений;

г) Защита программного кода от анализа;

д) Применение методов верификации кода для защиты от ошибок реализации.

– Математические меры. К математическим мерам защиты можно отнести балансирование криптографических операции и их маскировку.

ЗАКЛЮЧЕНИЕ

В данной статье были изучены различные виды атак на смарт-карты, а также рассмотрены методы обеспечения безопасности и меры защиты смарт-карт.

Таким образом, смарт-карты имеют много различных возможностей, что привлекает и подталкивает злоумышленников осуществлять разного рода атаки.

Как бы досадно ни звучало, не существует универсального и единого метода противодействия от вышеописанных атак. Но надежная защита может быть обеспечена при использовании комплекса методов, средств и мер защиты на всех фазах жизненного цикла смарт-карты.

СПИСОК ЛИТЕРАТУРЫ

1. Смарт-карта // Википедия. [2020] URL: https://ru.wikipedia.org/?curid=146248&oldid=106510802

2. Copy "What is a smart card?" HowStuffWorks.com. URL: https://computer.howstuffworks.com/question332.htm

3 Коровяковский Д.Г. Сравнительная характеристика расчетов смарт-картами и картами с магнитной полосой. Перспективы развития пластиковых (банковских) карт в россии // Финансы и кредит. 2007. №34 (274). URL: https://cyberleninka.ru/article/n/sravnitelnaya-harakteristika-raschetov-smart-kartami-i-kartami-s-magnitnoy-polosoy-perspektivy-razvitiya-plastikovyh-bankovskih-kart-v

4. Даценко П. Е. Атаки на смарт-карты и способы противодействия таковым // Современные информационные технологии. Информационная безопасность. - 2009. - №4. URL: http://www.rusnauka.com/10_NPE_2009/Informatica/44170.doc.htm

5. Steve H. Weingart. Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. CHES 2000, Springer-Verlag, 2000. URL: http://www.atsec.cn/downloads/pdf/phy_sec_dev.pdf

6. Классификация атак на смарт-карты // GPS/GSM/RFID системы**.**Защита информации/ URL: http://asupro.com/gps-gsm/data-protection/classification-attacks-on-smart-cards.html

ОБ АВТОРАХ

ЛЫОНГ ХА Ча Ми, студент 3-го курса ФИРТ.

ТАХАУТДИНОВ Айдар Радикович, студент 3-го курса ФИРТ.

ПРИВАЛОВА Анна Александровна, магистрант 1-го курса ФИРТ.

METADATA

Title: Smart card attacks. Methods for protecting smart cards.

Authors: Cha Mi Lyong Ha[1], A. R. Tahautdinov[2], A. A. Privalova[3]

Affiliation: Ufa State Aviation Technical University (UGATU), Russia.

Email: [1] lhtrmi0212@gmail.com, [2] aidartahasutdinov@gmail.com, [3] bruder.ocn@gmail.com

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), no. 1 (24), pp. 25-28, 2021. ISSN 2225-9309 (Print).

Abstract: The article discusses attacks on smart cards, as well as their classification by the level of attack and by the phase of the life cycle of the smart card itself. The problem of ensuring the security of smart cards and measures for their protection is touched upon.

Key words: smart cards; information security; attack; protect

About authors:

LYONG HA, Cha Mi, 3rd year student.

TAHAUTDINOV, Aydar Radikovich, 3rd year student.

PRIVALOVA, Anna Aleksandrovna, 1st year master student.