Московский физико-технический институт
(национальный исследовательский университет)
Кафедра защиты информации

Разработка стенда для анализа взаимодействия с аппаратными CCID-токенами

Отчет об обследовании

Автор: Иванов Василий Павлович
Научный руководитель: Алтухов Андрей Андреевич

Москва, 2020 г.

СОДЕРЖАНИЕ

Словарь терминов и сокращений

CCID - Chip Card Interface Device

APDU - Application Protocol Data Unit

ИС - информационная система

API - Application Programming Interface

PC/SC - Personal Computer/Smart Card

1 ПОСТАНОВКА ЗАДАЧИ

В наши дни ключевые носители, такие как смарт-карты и токены, распространены повсеместно и считаются безопасными, защищенными от взлома и заслуживающими доверия устройствами. Они используются для выполнения конфиденциальных операций, таких как идентификация и аутентификация пользователей, а также для хранения и обработки конфиденциальных данных. Такие операции подразумевают взаимодействие между ключевым носителем и сторонними недоверенными системами.

Согласно [1, с. 159] защищенный ключевой носитель должен обладать несколькими свойствами, одно из которых заключается в обеспечении возможности защищенного хранения криптографических ключей с применением интерфейсов работы со смарт-картой (CCID или PKCS#11).

CCID, как стандарт интерфейса USB, является одним из наиболее распространенных на сегодняшний день [2]. Вендоры смарт-карт и токенов предоставляют разработчикам возможность взаимодействовать со своими устройствами посредсвом проприетарных команд. Тем не менее, часто документация находится в закрытом доступе, либо ее вообще может не быть, потому что разработчик не позаботился об этом. В таких случаях, работа с аппаратными CCID-токенам может осуществляться лишь методом научного тыка. Либо можно подойти к задаче более систематически и попробовать разобраться, что происходит в устройстве и какие более низкоуровневые команды вызываются при определенных действиях разработчика. К тому же, такой анализ позволит понять, насколько надежно спроектирована и реализована система с точки зрения безопасности.

Обследование проводится в рамках предпроектных работ по теме «Разработка стенда для анализа взаимодействия с аппаратными CCID-токенами».

Заказчиком работ является кафедра защиты информации.

Исполнителем работ является студент кафедры защиты информации 519 группы ФРТК МФТИ Иванов Василий Павлович.

Объектом обследования является процесс взаимодействия с аппаратными CCID-токенов.

Целью обследования является формирование требований для реализации стенда, позволяющего провести анализ взаимодействия с аппаратными CCID-токенами.

Результаты проведенной работы отражены в настоящем отчете, который имеет следующую структуру:

- описание предметной области – Раздел 2;
- выбор и обоснование критериев качества – Раздел 3;
- анализ аналогов и прототипов – Раздел 4;
- перечень задач, решаемых в процессе разработки – Раздел 5;
- проект технического задания – Приложение 1.

2 ОПИСАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

Для анализа взаимодействия CCID-токенов необходимо разработать ИС, которая позволит этот анализ провести. Следует построить логическую модель предметной области, которая бы иллюстрировала все сущности, а также взаимоотношения между ними.

2.1 APDU

Коммуникация между терминалом и смарт-картой (токеном) происходит в формате APDU команд, которые описаны в ГОСТ Р ИСО/МЭК 7816 (аналоге зарубежного ISC/IEC 7816) [3]. Прикладной протокол, описанный в этом стандарте, оперирует блоками данных которые состоят из двух подряд идущих сообщений: APDU команды (C-APDU) и APDU ответа (R-APDU) [4]. Структура любой APDU команды описана в таблице 2.1.

Поле	Число байтов	Описание
CLA	1	Байт класса CLA
INS	1	Командный байт INS
P1-P2	2	Байты параметры P1-P2
L_c	0, 1 или 3	Длина передаваемых данных
Command Data	N_c	Набор байтов представляющий собой передаваемые данные
L_e	0, 1, 2 или 3	Максимальное количество данных, ожидаемых в поле данных ответа

Таблица 2.1 – Структура APDU команды

APDU команды начинается с байта CLA, который задает класс команды, отвечающий за параметры коммуникации. Если старший бит установлен в 1, то это проприетарная команда, не описанная в стандарте ГОСТ Р ИСО/МЭК 7816. Следующий байт INS (командный байт) опеределяет функцию. Полный список стандартных значений функций подробно описаны в разделе 5.1.2 вышеуказанного ГОСТ. Байты P1 и P2 задают параметры команды, и их

семантика зависит от первых двух байтов. Первые 4 байта образуют заголовок APDU команды и являются обязательными.

Формат команды ответа должен состоять как минимум из 2 байт, в которых содержится статус выполнения команды. Допустимые значения для статусов ответа также определены в ГОСТ Р ИСО/МЭК 7816. Помимо двух зарезервированных байтов под статус ответа, R-APDU также может содержать полезную нагрузку - данные, которые вернулись в ответ на вызов APDU команды.

2.2 PKCS

PKCS#11 - один из наиболее широко применяемых в мире стандартов криптографии, описывающий платформонезависимый интерфейс прикладного программирования (API) для криптографических токенов, которые хранят и обрабатывают аутентификацирующую информацию пользователя, включая персональные данные, криптографические ключи, сертификаты, цифровые подписи и биометрические данные [5]. API оперирует с наиболее часто используемыми в криптографии объектами: RSA ключи, сертификаты X.509 и другие, - а также описывает функции, необходимые для работы с этими объектами.

Некоторые вендоры токенов позволяют разработчикам взаимодействовать со своими устройствами, предоставляя собственные библиотеки, использующие стандарт PKCS#11 [6–8]. Схема взаимодействия показана на рис. 1: сначала вызывается функция из библиотеки, которую предоставил вендор устройства, затем делается запрос к PKCS#11 API, и в итоге пакеты в формате APDU команд передаются на смарт-карту, либо токен.

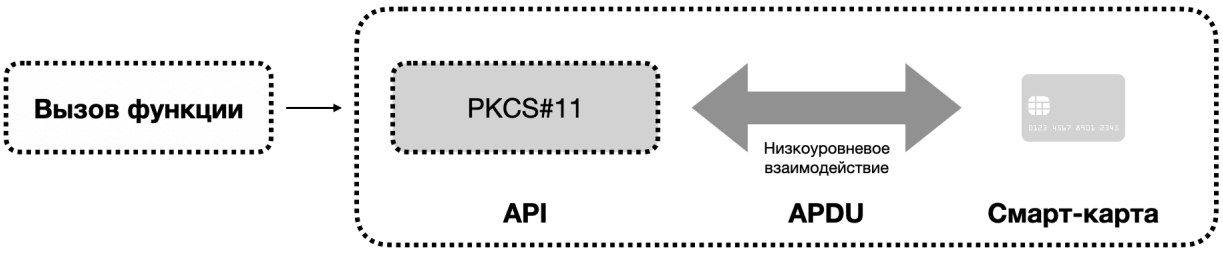

Рис. 1 – Взаимодействие со смарт-картой

Стандарт обладает рядом преимуществ [9]:

– кросплатформенность
– высокий уровень абстракции
– простой интерфейс для языка C

Тем не менее, стандрат также имеет и недостатки, которые стоит учесть при разработке стенда. Значимым недостатком является отсутствие полноценной поддержки стандарта операционными системами семейства Windows и, как следствие, прикладным программным обеспечением под Windows.

Для работы с PKCS#11 API приложение инициирует сеанс с токеном, предоставляя PIN-код. Стоит учитывать, что если на хост-машине запущен вредоносный код, то PIN-код пользователя может быть легко перехвачен, например с помощью кейлогера или поддельного CCID-драйвера устройства, позволяя злоумышленнику инициировать свои собственные сеансы с устройством. Тем не менее, стандарт был разработан для защиты конфиденциальных данных даже в тех случаях, если устройство подключено к скомпрометированному считывателю. Для этих целей вводятся дополнительные меры безопасности в виде аттрибутов, которыми помечаются ключи, хранящиеся на устройстве, и которые не позволяют читать их содержимое открытым текстом [11]. После инициирования сессии приложение может получить доступ к объектам, хранящимся на токене, например, ключам и сертификатам.

Несмотря на меры безопасности, предполагающие работу с компрометированным хостом, существует описание атак, которые могут

приводить к краже конфиденциальных данных, поэтому анализ защищенности токенов является актуальной задачей и по сей день [10].

2.3 Анализаторы траффика CCID-токенов

Поскольку основной задачей предпроектного исследования является анализ взаимодействия с аппаратными CCID-токенами, то следует рассмотреть инструментарий, с помощью которого анализ будет проведен. А именно, существующие анализаторы USB траффика. На сегодняшний день на рынке распространены анализаторы двух видов: программные и аппаратные.

Программные анализаторы заменяют собой программный стек протокола USB на хост-машине, чтобы контролировать и отслеживать данные, идущие с периферийного устройства. Как следствие, такие анализаторы полностью зависят от аппаратного обеспечения хостовой ЭВМ, а именно хост-контроллера USB. Хост-контроллер отвечает за коммуникацию с периферийными устройствами, а также за управление действиями, такими как повторная передача данных при ошибках. Контроль выполнения таких действий осуществляется внутри хост-контроллера USB, и поэтому они не входят в компетенцию каких-либо анализаторов трафика. [12]

Преимущества аппаратного анализатора траффика заключаются в:

- Независимости от хост-машины, на которой производится анализ, поскольку мониторинг не нуждается во взаимодействии с шиной USB
- Возможности отслеживать низкоуровненые состояния шины USB и ошибки
- Возможности добавления точек останова при анализе трафика
- Высокой временной точности мониторинга событий

Однако, большинство решений на рынке являются довольно дорогостоящими. К тому же, ни один из производителей не заявляет поддержку стандарта CCID, лишь HID (Human Interface Device) и Mass Storage [13–15].

Программные анализаторы USB трафика в большинстве своем являются бесплатными проектами, поддерживающими как ОС семейства Windows, так

и ОС Linux. Эти программы устанавливает свой собственный драйвер между драйвером хост-контроллера USB и драйвером устройства, а затем отслеживает все блоки запросов USB (USB Request Blocks), отображая их пользователю в легко читаемом формате [16]. Программные анализаторы позволяют:

– контролировать траффик, проходящий через шину USB
– декодировать и отображать данные
– проводить обратную разработку USB протоколов, устройств, драйверов и приложений

Наиболее подходящие программные аналазиторами для решения поставленной задачи перечислены в таблице 2.2.

Название	Описание	Поддержка windows	Поддежка Linux
Wireshark	Известный всем	+	+
Free USB Analyzer	asd	+	-
APDUPlay	some description	+	+
pcsc-tools	debian tools	-	+

Таблица 2.2 – Программные анализаторы

2.4 Компоненты системы

Для разработки стенда необходимым аппаратным обеспечением являются ЭВМ, на которой будет проводиться анализ, а также CCID-токен. Как уже отмечалось выше, ОС семейства Windows не имеют полноценной поддержки протола PKCS#11. К тому же, в ОС семейства Linux, а именно Debian, имеется встроенный набор утилит для взаимодействия с аппаратными CCID-токенами, поэтому хостовой ОС на ЭВМ будет Linux Debian 10.5, имеющая последнюю мажорную версию ядра Linux и поддерживаемая разработчиками.

Наглядно-графическая модель системы представлена на рис. 2.

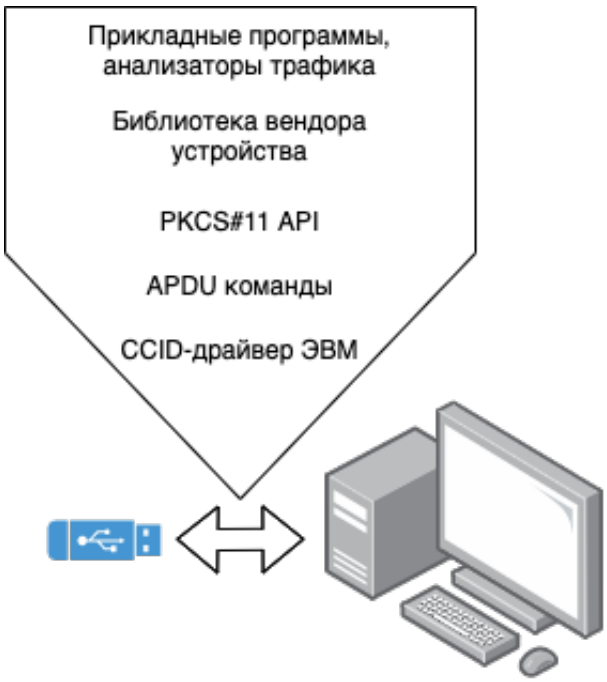

Рис. 2 – Схематическое представление предметной области

2.5 Анализ уязвимостей при взаимодействии с CCID-токенами

При работе с токенами, либо смарт-картами происходит обмен конфиденциальной информацией между токеном и сторонними системами. Такой обмен подвержден атакам типа ”человек посередине”, что делает токены уязвимыми. Анализ трафика CCID-токенов привлек много внимания и впоследствии было предложено множество инструментов. Например, некоторые из работ показали, что знание семантики взаимодействия с токеном может позволить злоумышленнику [18, 19]:

- получить PIN-код или другие аутентифицирующие данные в открытом виде
- получить доступ к конфиденциальным ключам
- выполнять несанкционированные операции
- клонировать токен или карту

3 ВЫБОР И ОБОСНОВАНИЕ КРИТЕРИЕВ КАЧЕСТВА

4 АНАЛИЗ АНАЛОГОВ И ПРОТОТИПОВ

5 ПЕРЕЧЕНЬ ЗАДАЧ, РЕШАЕМЫХ В ПРОЦЕССЕ РАЗРАБОТКИ

ПРИЛОЖЕНИЕ 1. ТЕХНИЧЕСКОЕ ЗАДАНИЕ

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Конявский В.А., Конявская С.В. Доверенные информационные технологии: от архитектуры к системам и средствам. Москва: URSS, 2019. – 159 с.

2. Преимущества использования протокола CCID в аппаратных СЗИ [Электронный ресурс] URL: https://www.okbsapr.ru/library/publications/yelkin_tezisy2013/ (дата обращения 05.08.2020)

3. Смарт-карты. Часть 2. APDU [Электронный ресурс] URL: https://habr.com/ru/post/367241/ (дата обращения 06.08.2020)

4. ГОСТ Р ИСО/МЭК 7816-4-2013 Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена [Электронный ресурс] URL: http://docs.cntd.ru/document/1200110393 (дата обращения 06.08.2020)

5. OASIS Enhances Popular Public-Key Cryptography Standard, PKCS #11, for Mobile and Cloud [Электронный ресурс] URL: https://www.oasis-open.org/news/pr/oasis-enhances-popular-public-key-cryptography-standard-pkcs-11-for-mobile-and-cloud (дата обращения 06.08.2020)

6. ESMART Список функций PKCS11 [Электронный ресурс] URL: https://esmart.ru/upload/iblock/733/ESMART.pdf (дата обращения 06.08.2020)

7. Высокоуровневые программные интерфейсы [Электронный ресурс] URL: https://dev.rutoken.ru/pages/viewpage.action?pageId=2228245 (дата обращения 06.08.2020)

8. JaCarta PKI [Электронный ресурс] URL: https://www.aladdin-rd.ru/catalog/jacarta_pki/ (дата обращения 06.08.2020)

9. Рекомендации по выбору высокоуровневого интерфейса. Стандарт PKCS#11 [Электронный ресурс] URL:

https://dev.rutoken.ru/pages/viewpage.action?pageId=2228227 (дата обращения 06.08.2020)

10. Attacking and fixing PKCS#11 security tokens [Электронный ресурс] URL: https://www.researchgate.net/publication/221609910_Attacking_and_fixing_PKC (дата обращения 06.08.2020)

11. PKCS #11 v2.20: Cryptographic Token Interface Standard [Электронный ресурс] URL: https://www.cryptsoft.com/pkcs11doc/STANDARD/pkcs-11v2-20.pdf (дата обращения 07.08.2020)

12. Benefits of Using a Hardware USB Protocol Analyzer over a Software-Only Solution [Электронный ресурс] URL: https://www.totalphase.com/solutions/apps/usb-analyzer-benefits/ (дата обращения 15.08.2020)

13. Overview of the Beagle USB Protocol Analyzers [Электронный ресурс] URL: https://www.totalphase.com/solutions/apps/usb-analyzer-guide/ (дата обращения 15.08.2020)

14. USB Explorer 200 - Comparison chart [Электронный ресурс] URL: https://www.ellisys.com/products/usbex200/chart.php (дата обращения 15.08.2020)

15. Voyager M310P [Электронный ресурс] URL: http://lecroy-rus.ru/catalog/serialdata/usb_3_0/voyager_m3x../voyager_m310p/ (дата обращения 15.08.2020)

16. Free USB Analyzer Overview [Электронный ресурс] URL: https://freeusbanalyzer.com/ (дата обращения 15.08.2020)

17. CaptureSetup/USB - Wireshark Wiki [Электронный ресурс] URL: https://wiki.wireshark.org/CaptureSetup/USB (дата обращения 15.08.2020)

18. The SmartLogic Tool: Analysing and Testing Smart Card Protocols [Электронный ресурс] URL: https://ieeexplore.ieee.org/document/6200201 (дата обращения 15.08.2020)

19. The Smart Card Detective: a hand-held EMV interceptor [Электронный ресурс] URL: https://www.cl.cam.ac.uk/ osc22/docs/mphil_acs_osc22.pdf (дата обращения 15.08.2020)