УДК 004.056.5 + 004.5 : 004.6

Моисеев А. М., Мамыкин А. В., Москвин В. В.

АТАКА ЧЕРЕЗ USB

USB – очень распространённый последовательный интерфейс передачи данных. За последние десятилетия этот стандарт успешно завоевал мир благодаря своей универсальности – различные устройства, работающие с USB, могут подключаться к одному и тому же разъему. В этом году за месяц до ежегодной хакерской конференции Black Hat USA был анонсирован доклад Карстена Ноля под названием «BadUSB – об аксессуарах, обратившихся во зло». В нем была описана уязвимость, которая не подлежит обнаружению стандартными средствами защиты. В данной статье мы хотели бы показать, что вовсе необязательно модифицировать уже существующие, а можно разработать свои устройства для проведения атаки через USB-интерфейс.

Ключевые слова: *информация, безопасность, уязвимости, информационная безопасность, инженерно-техническая защита информации.*

Moiseev A. M., Mamykin A. V., Moskvin V. V.

USB DRIVEN ATTACK

USB is a very common serial data interface. Over the past decades the aforementioned standard has successfully conquered the world due to its versatility: different devices operating with USB can connect to the same port. This year, a month before the annual hacker conference Black Hat USA Karsten Noll report entitled 'BadUSB. On accessories enquired with evil' was announced. It has described vulnerability that is not subject to detection by standard means of protection. In this article the authors would like to show that it is not necessary to modify the existing devices, one can develop personal device for an attack through the USB interface.

Keywords: *information, security, vulnerability, information security, engineer and technical information security.*

Интерфейс USB применяется в огромном количестве самых различных устройств, начиная с персональных компьютеров и заканчивая телевизорами. Этот стандарт имеет несколько версий. Причем устройства новых версий совместимы с интерфейсами старых версий, и наоборот (прямая и обратная совместимость).

Различных типов USB-устройств выделяется достаточно много: flash-накопители, USB-cdrom'ы, мыши, клавиатуры, игровые контроллеры, сетевые карты и множество других. Каждое такое устройство относится к определенному классу, согласно спецификации, определяющей функциональность этого устройства.

Примерами таких классов являются: звуковые карты, сетевые карты, устройства HID, веб-камеры, принтеры и прочие. Более подробно с классами устройств можно ознакомиться на сайте http://www.usb.org/developers/defined_class.

Классов устройств существует достаточно много. Наиболее известными и распро-

страненными среди этих классов являются HID, или «устройства человеческого интерфейса» – клавиатуры, мыши, джойстики, контроллеры беспроводной связи (Bluetooth/Wi-Fi), внешние устройства памяти и т. д. USB-HID не требуют установки специальных драйверов и могут работать сразу после подключения к ПК (Plug&Play). Реализовано это за счёт наличия драйверов в составе самой ОС.

Функциональность каждого устройства обеспечивает программно-управляемый USB-контроллер причем для различных классов может применяться один и тот же контроллер, с различной прошивкой. Именно USB-контроллер «сообщает» ПК о том, какое устройство к нему подключено.

Уязвимость «BadUSB», описанная в докладе Карстена Нолла, основывается на том, что при наличии соответствующей прошивки любое устройство может «маскироваться» под устройство другого класса и выполнять его функции.

С первого взгляда может показаться, что публикация этой уязвимости приведет к очередной эпидемии, ведь каждый желающий сможет реализовать её без каких-либо проблем. На самом деле проблем достаточно, и самая главная и очевидная проблема – в выборе оборудования. Для USB-устройств производители используют специальное ПО с закрытым исходным кодом. Чтобы преодолеть эту проблему, нужно прибегнуть к back-инжинирингу, чем и занялись специалисты Адам Коудил и Брэндон Уилсон, которые рассказали в совместном докладе на ежегодной конференции Derby Con об успешной прошивке контроллера Phison 2303 (2251-03). В итоге им удалось создать альтернативную прошивку, имитирующую клавиатуру.

В данной статье мы хотели бы показать, что проведение back-инжиниринга готового устройства – это не единственный способ реализации атаки через USB. Вместо того чтобы модифицировать заводское, можно достаточно просто разработать своё специализированное устройство для проведения данного вида атаки. Для этого необходимо воспользоваться практически любым микроконтроллером с аппаратной поддержкой USB. Мы остановились на наиболее широко распространенном микроконтроллере STM32F103C8 европейской фирмы STMicroelectronics. Принципиальная схема разработанного нами устройства, изображена на рис. 1.

Данный микроконтроллер имеет 32-битную архитектуру ARM Cortex M-3 с тактовой

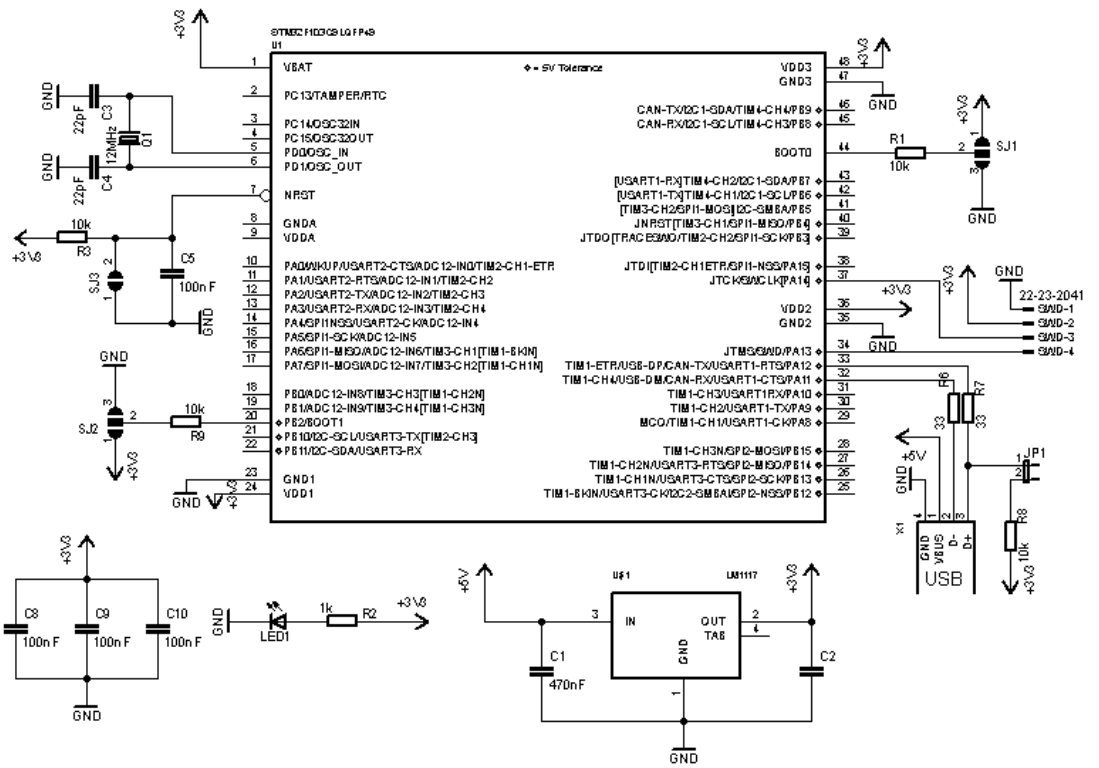

Рис. 1. Схема устройства

частотой до 72 МГц, 64 кБ программной памяти и 20 кБ оперативной памяти. Также он поддерживает следующие интерфейсы: CAN, I2C, SPI, USART и, конечно, USB.

Прошить его можно несколькими способами: через специализированные отладочные порты JTAG/SWD и программатор-отладчик (нами использовался ST-Link/v2), либо воспользовавшись простым USB-UART (COM-UART) адаптером, поскольку данный микроконтроллер содержит в памяти встроенный загрузчик.

Прежде всего необходимо определиться с HID-классом устройства. Для целенаправленной атаки на ПК лучше всего подойдет эмулирование клавиатуры, поскольку с помощью неё доступно выполнение большинства функций операционной системы. Вся информация, необходимая для поддержки функционирования HID-устройств, заложена в дескрипторах. Кроме того, можно привести небольшой список аналогичных векторов атак, основывающихся на других HID-устройствах:

• эмулирование сетевой карты и подмен/анализ пакетов данных. Предоставляет широчайшие возможности для атак типа «Man in the middle»;

• эмулирование флэш-накопителя совместно с клавиатурой с целью заражения ОС и подключенных уязвимых микроконтроллеров или модификации bios.

Дескриптор – это описание свойств устройства, а также функций, выполнение которых оно поддерживает. Он определяет способы обмена информацией, режимы работы и подходящий для устройства драйвер. Управлением шины занимается хост, поэтому HID-устройство не может инициировать передачу данных самостоятельно, оно лишь опрашивается хостом. Поэтому в описании дескриптора должна быть указана частота опроса. Считывание дескриптора производит требование GET_DESCRIPTOR. Ниже приведена таблица стандартных дескрипторов.

Так как Device дескриптор определяет само устройство, то он всегда один, а дескрипторов Configuration, Interface и Endpoint может быть несколько. Это связано с тем, что устройство может быть составным и иметь различные параметры электропитания. Дескрипторы, перечисленные в данном абзаце, являются обязательными, все остальные – необязательные (могут быть не заданы).

Отдельно выделяют Report дескриптор. ПК и USB-устройство обмениваются данными с помощью пакетов заранее определенного формата (report пакет). Различных типов пакетов может быть много, каждый – для выполнения своей задачи. Так как у данного дескриптора достаточно строгий формат, а ошибки в нем недопустимы, можно автоматизировать процесс его настройки с помощью утилиты «Usb Hid Demonstrator» от STMicroelectronics.

Для того чтобы наше устройство не вызывало подозрений у пользователя, такие параметры как VendorID, ProductId, а также серийный номер и производитель, могут быть скопированы с реального устройства.

В нашем случае использовался лишь микроконтроллер, но с добавлением к нему новых устройств его функционал можно значительно расширить – к примеру, flash-накопитель, который может нести в одном из разделов вирус, загружаемый в систему.

На данный момент каких-либо способов защиты от атак данного типа, кроме использования доверенных устройств, не существу-

Таблица 1

Код	Тип описания
0	DEVICE (устройство)
1	CONFIGURATION (конфигурация)
2	STRING (строка)
3	INTERFACE (интерфейс)
4	Зарезервировано
5	ENDPOINT (точка)
6	DEVICE_QUALIFIER (устройство для другой скорости)
7	OTHER_SPEED_CONFIGURATION (конфигурация для другой скорости)
8	INTERFACE_POWER

ет, но производители могут следовать определенным рекомендациям, чтобы значительно уменьшить вероятность их реализации в будущем:

1) Разделить USB-порты в ПК в зависимости от класса устройства. Таким образом, к примеру, выполнение функций клавиатуры USB-накопителем станет невозможным;

2) Контролирование классов устройств на программном уровне. Своеобразный USB-фаервол, проверяющий соответствие класса устройства и выполняемых им функций;

3) Подпись прошивок производителем устройства и проверка цифровой подписи ОС при подключении. ОС просто заблокирует устройство с модифицированной прошивкой.

Примечания

1. Чекунов, Д. Программисту USB-устройств. Часть 1. Знакомство с USB / Д. Чекунов // Современная электроника. – 2004. - № 1. – С. 68–71.

2. Чекунов, Д. Программисту USB-устройств. Часть 2. Стандартные требования USB / Д. Чекунов // Современная электроника. – 2004. - № 2. – С. 70–75.

3. Чекунов, Д. Программисту USB-устройств. Часть 3. Стандартные дескрипторы USB / Д. Чекунов // Современная электроника. – 2005. - № 1. – С. 72–77.

4. Defined 1.0 Class Codes [Электронный ресурс]. - Usb.org. Режим доступа: www.usb.org/developers/defined_class, свободный. – Загл. с экрана.

Моисеев Алексей Михайлович, студент КГУ. E-mail: mamykin.av@bk.ru

Мамыкин Андрей Владимирович, студент КГУ. E-mail: mamykin.av@bk.ru

Москвин Владимир Викторович, ст. преподаватель КГУ.

Aleksey Michailovich Moiseev, student of Kurgan State University. E-mail: mamykin.av@bk.ru

Andrey Vladimirovich Mamykin, student of Kurgan State University. E-mail: mamykin.av@bk.ru

Vladimir Viktorovich Moskvin, senior teacher of Kurgan State University.