УДК 004.056

ИССЛЕДОВАНИЕ АЛГОРИТМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ ПРЕДПРИЯТИЙ НА БАЗЕ ИНТЕРФЕЙСА USB

Варавка А.В., Демеш Н.С., Приходько Т.А.
Донецкий национальный технический университет, г. Донецк
Кафедра компьютерной инженерии
E-mail: antosha90@yandex.ru

Аннотация:
Варавка А.В., Демеш Н.С, Приходько Т.А, Исследование алгоритма информационной безопасности в компьютерных системах предприятий на базе интерфейса USB. *Проведен анализ принципа работы интерфейса USB. Исследована архитектура и взаимодействие компонентов USB. Приведен принцип работы программы-разведчика USB-носителей.*

Интерфейс USB

Шина USB (Universal Serial Bus - универсальная последовательная шина) является промышленным стандартом расширения архитектуры персонального компьютера, ориентированным на интеграцию с телефонией и устройствами бытовой электроники. Шина появилась по компьютерным меркам довольно давно - версия первого утвержденного варианта стандарта появилась 15 января 1996 года (USB 1.0). Спецификация периферийной шины USB была разработана лидерами компьютерной и телекоммуникационной промышленности — Compaq, DEC, IBM, Intel, Microsoft, NEC и Northern Telecom — для подключения компьютерной периферии вне корпуса машины по стандарту plug'n'play, в результате чего отпадала необходимость в установке дополнительных плат в слоты расширения и переконфигурировании системы. Шина USB позволяет одновременно подключать последовательно до 127 устройств, таких, как мониторы или клавиатуры, выполняющие роль дополнительно подключенных компонентов, или хабов (т.е. устройств, через которые подключается еще несколько) [1].

Для исследований выбран стандарт USB 2.0, во-первых, потому что интерфейс USB 3.0 пока не получил столь широкого распространения, а во-вторых, USB 3.0 совместим с USB 2.0, а значит разработка сохраняет свою актуальность. Пропускной способности в 480 Мбит/с достаточно для удовлетворения потребностей всех применений в полной мере. Спецификация USB 2.0 позволяет производить обмен информацией с периферийными устройствами на трех скоростях:

- Низкая скорость (Low Speed - LS) - 1,5 Мбит/с (интерактивных устройств);
- Полная скорость (Full Speed - FS) - 12 Мбит/с (аудио-, видеоустройства);
- Высокая скорость (High Speed - HS) - 480 Мбит/с (видеоустройства, память).

Архитектура и взаимодействие компонентов USB

USB обеспечивает обмен данными между хост-компьютером и множеством одновременно доступных периферийных устройств. Распределение пропускной способности шины между подключенными устройствами планируется хостом и реализуется им с помощью посылки маркеров. Шина позволяет подключать, конфигурировать, использовать и отключать устройства во время работы хоста и самих

устройств - динамическое ("горячее") подключение и отключение. Устройства (Device) USB могут являться хабами, "функциями" или их комбинацией. Хаб (Hub) обеспечивает дополнительные точки подключения устройств к шине. "Функции" (Function) USB предоставляют системе дополнительные возможности - например, подключение к ISDN, цифровой джойстик, акустические колонки с цифровым интерфейсом и т.д.

Работой всей системы USB управляет хост-контроллер. являющийся программно-аппаратной подсистемой хост-компьютера. [2]

"Функции" представляют собой устройства USB, способные принимать или передавать данные или управляющую информацию по шине. Физически в одном корпусе может быть несколько "функций" со встроенным хабом обеспечивающим их подключение к одному порту. Каждая "функция" предоставляет конфигурационную информацию, описывающую его возможности и требования к ресурсам. Перед использованием функция должна быть сконфигурирована хостом - ей должна быть выделена полоса в канале, выбраны специфические опции конфигурации.

Хаб - ключевой элемент системы Plug-and-Play в архитектуре USB. Хаб является кабельным концентратором, точки подключения называются портами хаба. Каждый хаб преобразует одну точку подключения в их множество. Архитектура подразумевает возможность соединения нескольких хабов.

Система USB разделяется на три уровня с определенными правилами взаимодействия. Устройство USB делится на интерфейсную часть, часть устройства и функциональную часть. Хост тоже делится на три части - интерфейсную, системную и ПО устройства. Каждая часть отвечает только за определенный круг задач, взаимодействие между ними показано на рисунке 1 [4].

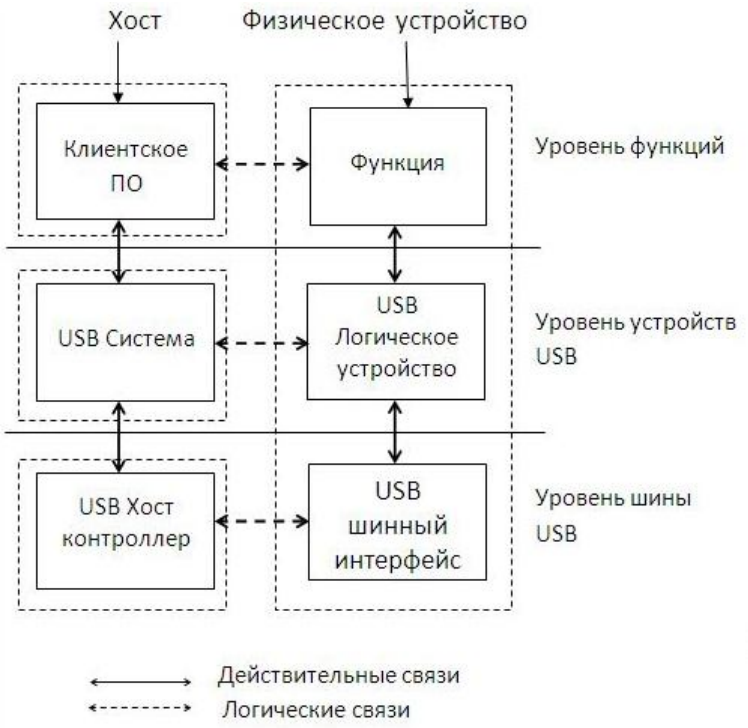

Рисунок 1 - Взаимодействие компонентов USB

1. Физическое устройство USB - устройство на шине, выполняющее функции, интересующие пользователя.
2. Client SW - программное обеспечение, соответствующее конкретному устройству, исполняемое на хост-компьютере. Может являться составной частью ОС или специальным продуктом.
3. USB System SW - системная поддержка USB операционной системой, независимая от конкретных устройств и клиентского ПО.
4. USB Host Controller - аппаратные и программные средства, обеспечивающие подключение устройств USB к хост-компьютеру.

Программа-разведчик в системах информационной безопасности предприятий

Каждый пользователь современного персонального компьютера имеет возможность хранить и передавать информацию с помощью USB-накопителей (флэш-память). Стоимость таких устройств на компьютерном рынке составляет около 10 долларов. В связи с довольно низкой стоимостью, а также достаточно гибким и удобным использованием флеш-памяти большинство пользователей и работников предприятий выбирают именно данный способ хранения информации. Основной задачей для автора данной статьи является описание алгоритма наблюдения за действиями работников какой-либо организации или предприятия, а именно какая информация записывается на служебные компьютеры либо переписывается с жестких дисков компьютеров на USB-носители. Данный алгоритм наблюдения можно реализовать с помощью написания программы-разведчика, которая будет отслеживать работу всех накопителей, подключенных к компьютеру через универсальную последовательную шину USB. Программа начинает выполняться автоматически при запуске операционной системы Windows на служебном компьютере без уведомления пользователя. Программа запущена, однако работа происходит в «скрытом режиме» (о том, что существует процесс можно посмотреть только в диспетчере задач Windows, который может отключить системный администратор).

Основные функции программы:

1. Определение типа подключаемого устройства, а также следующие параметры: производитель, модель, серийный номер устройства.
2. Перехват запросов на чтение/запись информации.
3. Определение MAC-адреса текущего служебного ПК.
4. Создание файлов для хранения истории процессов работы USB-накопителя.
5. Передача по локальной сети файлов с результатами работы программы-шпиона на компьютер администратора предприятия.

Принцип взаимодействия программы-разведчика с контроллером шины USB и компьютером администратора приведен на рисунке 2.

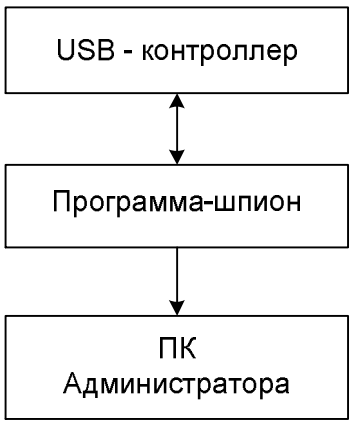

Рисунок 2 – Принцип взаимодействия программы-разведчика с контроллером шины USB и компьютером администратора

Выводы.

В результате анализа архитектуры и взаимодействия компонентов USB, было проведено исследование алгоритма информационной безопасности на базе интерфейса USB, а также изложен принцип работы программы-разведчика. Можно сделать вывод, что для систем информационной безопасности, которые используются в общественных, частных или государственных организациях можно реализовать алгоритм, с помощью которого можно улучшить безопасность конфиденциальной информации.

Литература.

1. Агуров П. В. Интерфейс USB. Практика использования и программирования.- СПб:БХВ-Петербург,2004.-576 с.-ISBN 5-94157-202-6

2. Скотт Мюллер. Модернизация и ремонт ПК (глава 15 — Последовательный, параллельный и другие интерфейсы ввода/вывода — USB) = Upgrading and Repairing PCs. — 17 изд. — М.: «Вильямс», 2007. — С. 1016—1026. — ISBN 0-7897-3404-4

3. Материалы сайта http://hi-tech.mail.ru/articles/item/1896/

4.Don Anderson. Universal Serial Bus System Architecture/- Mindshare INC http://interface.centraltreasure.com/files/pdf/Hardware_USB_System_Architecture_pdf.pdf

Заявка участника

Название доклада	Исследование метода информационной безопасности в компьютерных системах предприятий на базе интерфейса USB
Секция выступления	6
ВУЗ	ДонНТУ
Автор	Варавка Антон Витальевич
Адрес автора	г. Макеевка, ул. Лазо, д. 77, кв. 80.
E-mail автора	antosha90@yandex.ru
Телефон автора	(099)953-64-73
Руководитель 1	Демеш Наталья Сергеевна
Ученое звание	Нет
Научная степень	Нет
Должность	Ассистент кафедры компьютерной инженерии
Адрес руководителя	83000, Артема 58, корп. 4, каб. 35
E-mail руководителя	dns666@bk.ru
Телефон руководителя	301-07-53
Руководитель 2	Приходько Татьяна Александровна
Ученое звание	Нет
Научная степень	к.т.н
Должность	Ассистент кафедры компьютерной инженерии
Адрес руководителя	83000, Артема 58, корп. 4, каб. 38
E-mail руководителя	pr.tatyana@gmail.com
Телефон руководителя	301-07-53