МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики
Кафедра технологии программирования

Разработка драйвера для контроля подключений USB –устройств

Минск 2012

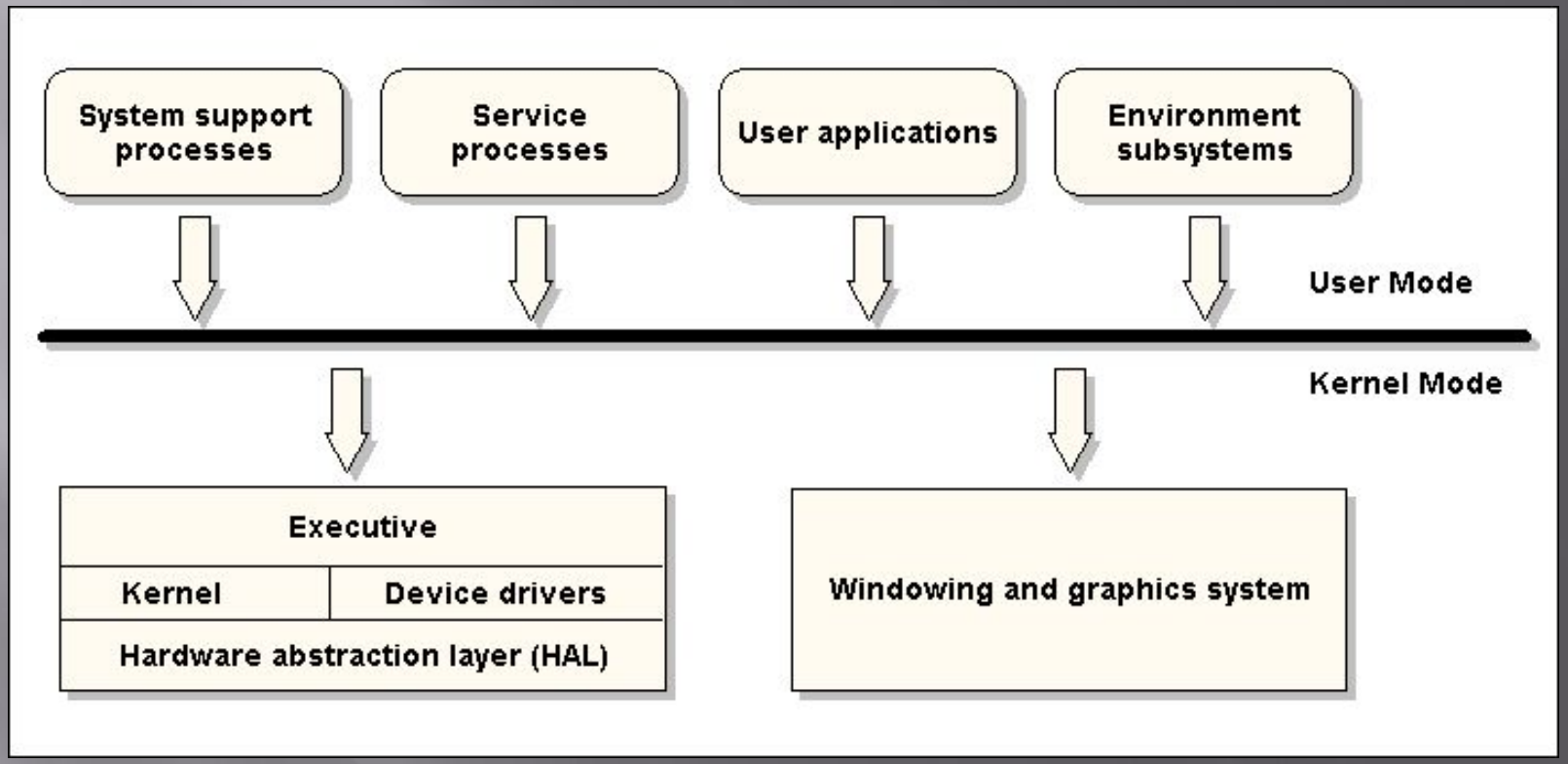
Толмачев М. А.

Введение

Перемещение информации через границы охраняемого периметра локальной сети компании доставляет, пожалуй, наибольшее количество хлопот службе информационной безопасности.

За последнее время резко увеличилось число всевозможных USB-устройств, которые могут использоваться в качестве накопителей. Поэтому разработка методов контроля подключений USB-утсройств является необходимым условием обеспечения информационной безопасности пользователей.

Обзор архитектуры Windows



Драйверы ОС Windows

Драйвер устройства – это программа предназначенная для управления каким-то устройством, причем устройство это не обязательно должно быть физическим. Оно может быть логическим или виртуальным.

Драйверы пользовательского режима (User-Mode Drivers)

- Драйверы виртуальных устройств (Virtual Device Drivers, VDD) - используются для поддержки программ MS-DOS;
- Драйверы принтеров (Printer Drivers).

Драйверы режима ядра (Kernel-Mode Drivers)

- Драйверы файловой системы (File System Drivers) - реализуют ввод-вывод на локальные и сетевые диски;
- Унаследованные драйверы (Legacy Drivers) - написаны для предыдущих версий Windows NT;
- Драйверы видеоадаптеров (Video Drivers) - реализуют графические операции;
- Драйверы потоковых устройств (Streaming Drivers) - реализуют ввод-вывод видео и звука;
- WDM-драйверы (Windows Driver Model, WDM) - поддерживают технологию Plag and Play и управление электропитанием

Разделение драйверов по способу обработки запросов ввода-вывода

- Одноуровневые драйверы
- Многоуровневые драйверы

Уровни запросов прерывания

Прерывание – неотъемлемая часть любой операционной системы. Прерывание требует обработки, поэтому выполнение текущего кода прекращается и управление передается обработчику прерывания.

Существуют как аппаратные, так и программные прерывания.

Общая классификация драйверов WDM

- Драйверы шин (Bus Drivers). Управляют логическими или физическими шинами. Отвечают за распознавание устройств, подключение их к управляемой ими шине и оповещение о них диспетчера PnP.
- Функциональные драйверы (Function Drivers). Управляют конкретным типом устройств. Экспортируют рабочий интерфейс устройства операционной системе.
- Драйверы фильтров (Filter Drivers). Занимая более высокий логический уровень, чем функциональные драйверы, добавляют функциональность или изменяют поведение устройства либо другого драйвера. Этот тип драйверов не обязателен для нормальной работы устройства.

Драйверы фильтров

- Драйверы фильтров шин (Bus Filter Drivers).
- Низкоуровневые драйверы фильтров (Lower-Level Filter Drivers).
- Высокоуровневые драйверы фильтров (Upper-Level Filter Drivers).

Типы объектов «устройство»

- Объект "физическое устройство" (Physical Device Object, PDO) - Создается драйвером шины по заданию диспетчера PnP, когда драйвер шины, перечисляя устройства на своей шине, сообщает о наличии какого-либо устройства. PDO представляет физический интерфейс устройства.
- Объект "функциональное устройство" (Functional Device Object, FDO) - Создается функциональным драйвером, который загружается диспетчером PnP для управления обнаруженным устройством. FDO представляет логический интерфейс устройства.
- Необязательная группа объектов "устройство-фильтр" (Filter Device Object, FiDO). Одна группа таких объектов размещается между PDO и FDO (эти объекты создаются драйверами фильтров шин), вторая - между первой группой FiDO и FDO (эти объекты создаются низкоуровневыми драйверами фильтров), а третья - над FDO (эти объекты создаются высокоуровневыми драйверами фильтров).

Этапы разработки драйвера

- Выбор типа драйвера;
- Составление спецификации оборудования, достаточной для начала работы над драйвером;
- Тестирование установочного файла во всех операционных системах;
- Создание панелей управления и прочих вспомогательных программ;
- Реализация и тестирование функциональности WMI и журнала событий;

Модель взаимодействия

Возможности драйвера

- Заблокировать устройство.
- Разрешить подключение и дальнейшую работу устройства.

Спасибо за внимание