УДК004.89

**НЕКОТОРЫЕ ВОПРОСЫ СЕТЕВОЙ БЕЗОПАСНОСТИ WINDOWS**

**А.Б. Оспанова, А. Сахов**

*Евразийский национальный университет им. Л. Н. Гумилева, Астана*

*o.ademi111@gmail.com*

*Исследуется вопрос сетевой безопасности для сетей, работающих на платформах MS Windows. С этой целью проведен обзор модели драйверов Windows. На основе примера из набора для разработки драйверов Windows Driver Kit (WDK), предоставляемого фирмой Microsoft, – драйвера Pussthru – разработана утилита, осуществляющая мониторинг сетевого трафика. А также описаны потенциальные возможности, допускаемые при использовании WDK, помогающие в решении вопросов сетевой безопасности.*

***Ключевые слова:****Сетевая безопасность, протокол Интернета, сетевые драйверы, драйверы протокола, сетевой трафик.*

**Введение**

Компьютерные сети используются повсеместно как на корпоративном уровне, так и в частных компьютерных системах.Под компьютерной сетью будем понимать в том числе и распределенную систему[1]. Для создания составных компьютерных сетей в основном применяется стек протоколов TCP/IP,позволяющий организовать коммуникации в неоднородной сетевой среде. Ранее в работе [2] проведен обзор реализаций Интернет-стека TCP/IP, его достоинств, а также обзор и сравнительный анализ четвертой и шестой версий протокола сетевого уровня IP – Ipv4 и IPv6, процесса развертывания версии IPv6. Эти результаты, а также рост количества и разнообразия сетевых угроз, показывают, что различные задачи, связанные с безопасностью компьютерных сетей, вне зависимости от используемой версии IP, все еще долго будут оставаться актуальными. Кроме того, в виду различных обстоятельств [1] неотъемлемо развиваются сетевые технологии, что снова влечет проблемы безопасности сетей, требуя постоянного совершенствования существующих методов защиты. Среди способов обеспечения безопасности – мер законодательного уровня, административно-организационного и программно-технического – для поддержания высокого уровня информационной безопасности особенно важны меры программно-технического уровня.

В данной работе рассматриваются некоторые аспекты сетевой безопасности. Изучены возможности, предоставляемые свободно распространяемыми инструментальными средствами Microsoftдля разработки драйверов – пакетомWDK – на предмет повышения эффективности защиты компьютерной информации в сети.Разработана утилита, осуществляющая контроль сетевого трафика по некоторым параметрам. Приводимая разработка является одним из примеров, иллюстрирующих использование средств WDK.

**IP-сети и безопасность**

Несмотря на то, что существует и другие стеки протоколов, применяемые в компьютерных сетях, TCP/IP является наиболее популярным и быстроразвивающимся, существенным преимуществом которого является его независимость от системных архитектур и аппаратных платформ.Относительно безопасности протоколов TCP/IP, то есть безопасности передачи данных в Интернете в целом, отметим, что все данные этими протоколами передаются в открытом виде[3]. В спецификациях ранних версий IP отсутствовали требования безопасности. В середине 90-х годов консорциумом IETF(Inernet Engineering Task Force) – рабочей группой технического обслуживания Интернета был разработан набор протоколов IPSec для шифрования данных, передаваемых по сетям с архитектурой, совместимой с IPv4 – протоколом IP версии 4 [3-6]. Начиная с систем MS Windows Server 2008 и Windows Vista все версии Windows содержат полностью переработанный набор протоколов TCP/IP. Он включает поддержку как протокола IP версии 4, так и протокола IP версии 6, что соответствует современным требованиям к возможности подключения и производительности сетевых сред. В протокол IPv6 по умолчанию включена технология IPSec.Несмотря на улучшенную безопасность сетей в версии IPv6 из прогнозов и статистических данных, приводимых ранее в работе [2], следует, что достаточно большая часть Интернет-сообщества будет пользоваться Интернет-услугами и сетевыми технологиями через протокол IP версии 4 еще достаточное количество лет. Доля сетевого трафика на IPv6в настоящий момент относительно небольшая. Частично это связано с тем, что для перехода на новый протокол необходимо, чтобы его использовали все провайдеры, хостеры и пользователи;к тому же протоколы IPv4 и IPv6 не совместимы. Более подробно этот вопрос освещен в [2]. Ввиду сказанного нужно не только не отбрасывать вопросы безопасности протокола IPv4, но и со всей серьезностью относиться к ним.К тому же, в использовании IPSec имеются свои трудности, связанные со сложностью в применении.

IP-сети, в том числе корпоративные и беспроводные сети, уязвимы для многих способов несанкционированного вторжения в процесс обмена данными.Рост популярности Интернет-технологий сопровождается ростом серьезных угроз разглашения персональных данных, критически важных корпоративных ресурсов, государственных тайн и т. п. Такие факторы, как повсеместное проникновение Интернета и всеобщее распространение простых в использовании операционных систем и средств разработки, способствуют увеличению числа опасных, но несложных в исполнении сетевых атак.Можно выделить такие виды современных сетевых атак: подслушивание (sniffing), изменение данных, анализ сетевого трафика, подмена доверенного субъекта, посредничество, посредничество в обмене незашифрованными ключами (man-in-the-middle), перехват сеанса (sessionhijacking), отказ в обслуживании (DenialofService, DoS), парольные атаки, угадывание ключа, атаки на уровне приложений, сетевая разведка, злоупотребление доверием, компьютерные вирусы. В беспроводных сетях существуют также такие угрозы и опасности, как вещание радиомаяка, обнаружение WLAN, ложные точки доступа в сеть, анонимный доступ в Интернет [3]. Здесь в техническом плане должны развиваться и реализовываться такие механизмы безопасности, как идентификация и проверка пользователей, управление доступом, протоколирование и аудит, криптография, экранирование. Одно из наиболее эффективных программных средств защиты компьютерных сетей – это брандмауэры (firewalls), реализующие экранирование. Например, персональный брандмауэр Outpost Firewall или бесплатный брандмауэр COMODO Firewall Pro [7, 8]. Обозначим далее некоторые недостатки программных средств защиты информации:

• Многие из них эффективны, но доступны только крупным компаниям из-за высокой стоимости илислишком сложны вприменении (для обычных пользователей).

• Другие, свободно распространяемые программные средства аналогичного действия, как правило, с закрытым кодом. А это не дает уверенности в характере деятельности таких приложений, что влечет за собой скрытую опасность.

• Многие разработки в области защиты передаваемых данных обладают общим недостатком, выражающимся в их «привязанности» к определенному типу приложений. Самый радикальный способ преодоления указанного ограничения применительно к IP-сетям состоит том, что системы защиты должны действовать на сетевом уровне.

Из современных операционных систем наиболее уязвимой ввиду своей популярности у обычных пользователей остается система MS Windows.В настоящей работе предлагается практическая разработка, способная помочь избежать некоторых сетевых угроз в системах Windows.

**Сетевые компоненты Windows**

Далее описываются компоненты сетевых стеков MicrosoftWindows, среди которых особое внимание уделено NDIS-драйверам мини-порта. Здесь подробно рассматривается драйвер Passthru.

Microsoft Windows широко поддерживает работу в сети, как и система ввода-вывода и API-функции Windows. При создании сетевых стеков верхний уровеньнакладывается на нижний; эти уровни реализуются такими программными составляющими сетевых стеков, как службы, API-функции, протоколы и драйверы для сетевых адаптеров. Для каждого такого уровня у Windows имеются интерфейсы, что помогает сторонним разработчикам расширить сетевые возможности своей операционной системы путем разработки своих собственных компонентов.

*Опишем сетевые компоненты Windows.*

• Сетевые API-интерфейсы. Они позволяют приложениям обмениваться данными по сети. В некоторых случаях они служат оболочкой для других сетевых API-интерфейсов, реализующих определенную модель программирования или предоставляющих дополнительные виды обслуживания.

• Клиенты интерфейса транспортного драйвера –TransportDriverInterface (TDI). Это унаследованные драйверы устройств режима ядра, реализующие работающую в режиме ядра часть сетевого API-интерфейса. Интерфейс TDI по некоторым причинам не рекомендован к использованию [9].

• TDI-транспорты и драйверы протокола NetworkDriverInterfaceSpecification (NDIS) (или просто драйверы протокола). Это драйверы сетевого протокола режима ядра. Они принимают IRP-пакеты(I/o RequestPacket– пакет запроса на ввод/вывод – структура данных ядра[Windows](http://ru.wikipedia.org/wiki/Windows), обеспечивающая обмен данными между приложениями и[драйвером](http://ru.wikipedia.org/wiki/Драйвер), а также между драйвером и драйвером) от TDI-клиентов и обрабатывают запросы, представленные этими IRP-пакетами. Эта обработка может потребовать обмен данными по сети с равным по уровню узлом, побуждая TDI-транспорт добавлять специфичные для протокола заголовки (например, TCP, UDP и (или) IP) к данным, передаваемым в IRP, и обмениваться данными с драйверами адаптера с помощью NDIS-функций (описание этих функций дается в WindowsDriverKit). TDI-транспорты, как правило, облегчают связь сетевых приложений путем прозрачного проведения операций по отправке сообщений, например о сегментации и повторной сборке, установлении последовательности, подтверждении и о повторной передаче.

• Интерфейс предоставления транспортного сетевого уровня –TransportLayerNetworkProviderInterface (TLNPI). Это интерфейс между драйвером протокола TCP/IP и Winsock (Windows Sockets API – техническая спецификация доступа сетевого программного обеспечения Windows к сетевым сервисам, определяющая стандартный интерфейс между клиентским приложением и внешним стеком сетевых протоколов(TCP/IP)). Microsoft переработала ту часть сетевого стека, которая относится к сетевому протоколу, сделав ее строго ориентированной на TCP/IP.

• ЯдроWinsock–WinsockKernel (WSK). Независимый от транспортов сетевой API-интерфейс режима ядра, заменил устаревший TDI. WSK предоставляет сетевой обмен данными путем использования семантики программирования, похожей на сокеты, аналогичную Winsock пользовательского режима, а также другие свойства. WSK также изначально поддерживает функциональность IP версии 6 (IPv6) в сетевом стеке нового поколения (NextGeneration TCP/IP) в Windows.

• Платформа фильтрации Windows – Windows Filtering Platform (WFP).Это набор API-функций и системных служб, предоставляющих возможность создания сетевых фильтрующих приложений.

• Вызывающие драйверы WFP – WFP calloutdrivers. Драйверы режима ядра, реализующие вызовы, которые расширяют возможности WFP путем обработки сетевых данных.

• Библиотека NDIS (Ndis.sys). Средства, способствующие инкапсуляции драйверов сетевого адаптера (NetworkInterfaceCard, NIC). NDIS-библиотека экспортирует функции для использования транспорта TCP/IP и устаревшего транспорта TDI. Библиотека NDIS (C:\Windows\System32\Drivers\Ndis.sys) проводит границу, существующую между сетевыми транспортами, например, драйвером TCP/IP, и драйверами адаптеров. Библиотека NDIS является вспомогательной библиотекой, которую клиенты NDIS-драйвера используют для форматирования команд, отправляемых ими NDIS-драйверам. NDIS-драйверы работают с библиотекой, чтобы получать запросы и отправлять ответы.

• Драйверы мини-порта NDIS. Это драйверы режима ядра, отвечающие за согласование сетевого стека с конкретным NIC. Драйверы мини-порта NDIS заключены в оболочку NDIS-библиотеки Windows. Для работы протокольных драйверов в сети необходим сетевой адаптер. Как правило, поставщики сетевых адаптеров предоставляют их вместе с драйверами устройств. В 1989 году компании Microsoft и 3Com совместно разработали спецификацию интерфейса сетевых драйверов –Network Driver Interface Specification (NDIS), позволяющую протокольным драйверам связываться с драйверами сетевых адаптеров без учета особенностей тех или иных устройств. С Windows Server 2008 R2, Windows 7 и Windows 8 поставляются соответственно версии NDIS 6.1, 6.20, 6.30.

Отметим, что OSI-уровни не согласуются с фактическим программным обеспечением. Например, поставщики транспорта WSK часто переходят сразу несколько уровней. На рисунке 1 представлено взаимодействие сетевых компонентов относительно NDIS.

Рисунок 1. Взаимоотношения между различными компонентами, связанными с NDIS

*Драйверы мини-порта NDIS.*

Рассмотрим подробнее NDIS-драйверы, они необходимы для дальнейших исследований. Вместо простого предоставления вспомогательных процедур NDIS-границы, библиотека NDIS предоставляет NDIS-драйверы со всей средой выполнения. NDIS-драйверы не следуют стандарту модели драйверов устройств ввода-вывода Windows, и они не могут работать без инкапсуляции, предоставляемой им библиотекой NDIS. Этот изоляционный уровень помещает NDIS-драйверы в оболочку так, что NDIS-драйверы не могут принимать и обрабатывать IRP-пакеты. Точнее говоря, протокольные драйверы, например TCP/IP, вызывают функцию в NDIS-библиотеке, NdisAllocateNetBufferList, и передают пакеты мини-порту NDIS, вызывая функцию в NDIS-библиотеке (NdisSendNetBufferLists). Кроме того, для упрощения разработки все компоненты TCP/IP-стека Windowsпоследнихверсий используют структуру NET\_BUFFER\_LIST, включая TCP/IP и WSK, что упрощает связь с помощью NDIS. А именно, новые принципы передачи пакетов, заложенные в архитектуре NET\_BUFFER, уменьшили количество функций приема и отправки пакетов, которые должен реализовывать промежуточный драйвер.

NDIS обладают следующими свойствами:

• Драйверы NDIS могут сообщить, активна или нет их сетевая среда, что позволяет Windows показывать в панели задач значок подключенной или отключенной сети. Это свойство также позволяет протоколам и другим приложениям знать об этом состоянии и выдавать соответствующую реакцию. Например, TCP/IP-транспорт использует эту информацию для определения необходимости перевычисления адресной информации, полученной от DHCP.

• Работа драйверов NDIS может быть остановлена и продолжена, что позволяет перенастроить их на работающем компьютере, например, добавив или удалив драйвер легкого фильтра NDIS (NDIS Lightweight Filter). Легкий фильтр заменяет большинство экземпляров промежуточных драйверов NDIS, которые использовались до выхода NDIS версии 6. (Промежуточные драйверы по-прежнему поддерживаются в NDIS 6, но из-за своей сложности они подходят только для решения небольшого класса задач).

*Фильтр-драйверы*

Отметим один вид NDIS-драйверов мини-порта, реализуемый в модели NDIS. Это гибридные NDIS-драйверы сетевого транспорта – промежуточные NDIS-драйверы. Они находятся между транспортными драйверами и NDIS-драйверами мини-порта. Причем с позиции NDIS-драйверов мини-порта промежуточный NDIS-драйвер похож на транспортный драйвер, а с позиции транспортного драйвера промежуточный NDIS-драйвер похож на NDIS-драйвер мини-порта. Промежуточные NDIS-драйверы могут видеть весь сетевой трафик, происходящий в системе, потому что эти драйверы находятся между драйверами протокола и сетевыми драйверами. На промежуточных NDIS-драйверах основано программное обеспечение, которое предоставляет сетевым адаптерам отказоустойчивость и сбалансированность нагрузки, например разработанный Microsoft выравниватель сетевой нагрузки – Network Load Balancing Provider. И наконец, в NDIS-модели также реализованы драйверы легких фильтров (light weight filter drivers – LWF), похожие на промежуточные драйверы, но разработанные специально для фильтрации сетевого трафика. LWF-драйверы поддерживают динамические вставки и удаления при работе протокольного стека. Фильтрующие драйверы могут фильтровать все входящие и исходящие коммуникации использующегося адаптера мини-порта. Они также могут выбирать определенные типы фильтрации пакетов данных или управляющих сообщений. Модель драйверов Windows (WDM) выделяет драйверы трех типов – драйверы шины, функциональные драйверы и драйверы фильтра [9].

*Фильтр-драйвер Passthru.*

Рассмотрим теперь фильтр-драйвер семейства NDIS Passthru, пропускающий трафик через себя. Он будет использован нами при разработке программы, осуществляющей мониторинг сетевого трафика и состоящей из его модификации и вспомогательной программы пользовательского режима для управления драйвером.

Пример Ndislwf из Windows Driver Kit (WDK) 8.1 представляет собой образец соответствующего спецификации NDIS 6 фильтр-драйвера, который фактически ничего не делает: он просто пропускает весь сетевой трафик через себя, ничего не меняя, лишь демонстрируя базовые принципы работы фильтр-драйвера версии NDIS 6.

Хотя этот драйвер устанавливается в систему как модифицирующий фильтр-драйвер, он не изменяет сетевые пакеты, а лишь переупаковывает их и отсылает дальше. Можно модифицировать этот фильтр-драйвер таким образом, чтобы модифицировать пакеты перед дальнейшей их отсылкой. Например, можно фильтровать входящие/исходящие пакеты, можно шифровать/сжимать исходящие и дешифровать/распаковать входящие данные.

**Windows Driver Kit (WDK)**

В разработках на основе описанных сетевых компонент должен использоваться набор инструментальных средств для работы с драйверамиWindows Driver Kit (WDK), который доступен по программе подписки MSDN (Microsoft Developer Network – подразделение компании[Майкрософт](http://ru.wikipedia.org/wiki/Майкрософт), ответственное за взаимодействие фирмы с разработчиками) и его можно свободно скачать с сайта [10].

Microsoft WDK (Windows Development Kit (ранее назывался DDK) представляет собой набор из средств разработки, заголовочных файлов, библиотек, утилит, программного кода примеров и документации, который позволяет программистам создавать драйверы для устройств по определённой технологии или для определённой платформы (программной или программно-аппаратной).WDK содержит средства, упрощающие разработку драйвера (готовые примеры и шаблоны кода), обеспечивающие совместимость драйвера с операционной системой (символические определения констант, определения интерфейсных функций ОС, определения, зависящие от типа и версии ОС), а также установку и тестирование драйвера.

Документация по Windows Driver Kit включена в библиотеку MSDN. Хотя набор WDK предназначен для разработчиков драйверов устройств, он является обширным источником информации о внутреннем устройстве Windows. А в документации по WDK [11] содержится полное описание всех Windows-функций поддержки ядра и механизмов, используемых драйверами устройств как в виде учебного пособия, так и в виде справочника. В WDK, помимо документации, содержатся заголовочные файлы (в частности, ntddk.h, ntifs.h и wdm.h), определяющие ключевую внутреннюю структуру данных и константы, а также интерфейсы ко многим внутренним системным подпрограммам. Эти файлы полезны при исследовании внутренних структур данных Windows, используемых при отладке ядра.

На сегодняшний день на сайте Microsoft доступно обновление пакета WDK 8.1, содержащее инструменты для сборки, тестирования, отладки и развернутого использования драйверов для системWindows7, Windows 8 и выше.

В следующей части работы приводится небольшой пример использования сетевых компонентовWindows и средствWDK для усиления безопасности сетей: на основе Passthru с использованием WDK разработана утилита, осуществляющая мониторинг сетевого трафика. Этот пример предназначен для демонстрации возможностей, предоставляемых MicrosoftWindows частным разработчикам.

**Мониторинг сетевого трафика**

Предлагается утилита для мониторинга информационного потока через соединения поIP протоколу версии 4(темпы процесса развертывания протокола IPv6 в мире и в Казахстане в настоящее время не высоки ([2])), на персональных компьютерах с операционными системами MicrosoftWindows. Реализована возможность регулирования вывода информации о параметрах трафика – назначении, портах, протоколах, скорости и т. п. Имеется возможность фильтрации TCP/IP соединений. Функциональная часть программы выполнена путем модификации описанного сетевого драйвера из пакета WDK [12]. Помимо консольного варианта, что имеет свои преимущества, реализован также пользовательский интерфейс.

Для реализации блокировки и управления доступом блокируемыми IP-адресами необходимо создать текстовый файл со списком адресов и идентификатором соответствующего сетевого устройства на компьютере пользователя. Указанные идентификаторы и другую информацию о всех имеющихся сетевых интерфейсах можно получить командой /enum в консоли либо нажав кнопку «желілік интерфейстер»; соответствующая информация выводится в консоли либо в окне приложения.На рисунке 2 приведено содержание файла (в строках, начинающихся со знака #, содержится информация о сетевых интерфейсах). Другие возможности с их описанием можно просмотреть, исполнив команду /stats в консоли либо нажав, соответственно, кнопку «Статистика» в форме приложения.

Рисунок 2. Файл блокируемых IP-адресов.

Далее приведен результат работы программы. Указанный IP (можно вводить и доменное имя) заблокирован и трафик не проходит в обоих направлениях. Здесь реализована стандартная команда /ping.

Создавать альтернативы другим, возможно и популярным, программам аналогичного назначения необходимо ввиду того, что такиепрограммызачастую сложны и труднодоступны. К тому же, в операционных системахWindows отсутствуют подобные сервисы,а степень уязвимости информации в компьютерах пользователей возрастает. В этой связи требуется предоставить обычному пользователю возможность контролировать и регулировать свой сетевой трафик путем использования простых программ с понятным интерфейсом и с открытым кодом, исключающих скрытые нежелательные возможности их использования.

Работа предлагаемой утилиты успешно протестирована в системах Windows XP, Windows 7 и Windows 8.

**Заключение**

Пакет WDK в применении к описанным компонентам сетевых стеков Microsoft Windows представляет собой мощное средство для достижения желаемого уровня безопасности сетевых соединений, для изменения стандартного поведения системных функций в тех или иных целях, других задач.

Приводимая практическая разработка демонстрирует возможности укрепления сетевой безопасности Windows средствами, предоставляемыми самой системойчастным разработчикам.

Разработки с использованием рассмотренного инструментария можно обозначить как одно из направленийработы по обеспечению конфиденциальности и безопасности сетей на платформе Windows, взаимодействие в которых реализовано стеком TCP/IP.

**Использованная литература**

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.
2. Оспанова А. Б. Современные вопросы Интернет-протокола IP // Вестник ЕНУ им.  Л. Н. Гумилева. – 2014. – №3. – сдана в печать.
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: [Форум:](http://ru.wikipedia.org/w/index.php?title=Вильямс_(издательство)&action=edit&redlink=1) Инфра-М, 2008. – 416 с.
4. Информационный документ Интернета RFC791 – [www.ietf.org/rfc/](http://www.ietf.org/rfc/rfc791.txt)rfc791.txt.
5. Информационный документ Интернета RFC4301 – <http://tools.ietf.org/html/rfc4301>**.**
6. Информационный документ Интернета RFC6071 – <http://tools.ietf.org/html/rfc6071>.
7. Яремчук С. А. Защита вашего компьютера. – СПб.: Питер, 2008. – 288 с.
8. Платонов В. В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования. – М.: Академия, 2013. – 336 с.
9. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows, 6-е издание (Часть 1). Пер. с англ. – СПб.: Питер, 2013. – 800 с.
10. Инструментарий WDK – <http://msdn.microsoft.com/ru-ru/windows/hardware/hh852365>.
11. Документация WDK – [http://msdn.microsoft.com/library/windows/hardware/ff557573%28v=vs.85%29.aspx](http://msdn.microsoft.com/library/windows/hardware/ff557573(v=vs.85).aspx).
12. Примеры драйверов WDK – [http](http://code.msdn.microsoft.com/windowshardware)://code.msdn.microsoft.com/windowshardware.
13. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.
14. Они У. Использование Microsoft Windows Driver Model. 2-е изд. – СПб.: Питер, 2007. – 768 с.
15. Орвик П., Смит Г. Windows Driver Foundation. Разработка драйверов. – СПб.: БХВ-Петербург, 2008. – 880 с.

The MS Windows platforms network security subject is investigated. For this purpose the survey of Windows drivers model is carried out. The network traffic monitoring utility based on Pussthru sample driver from Windows Driver Kit (WDK) driver development kit provided by Microsoft is developed. Also the potential opportunities allowed at use of WDK and helping with solving of network security problems are described.

Исследуется вопрос сетевой безопасности для сетей, работающих на платформах MS Windows. С этой целью проведен обзор модели драйверов Windows. На основе примера из набора для разработки драйверов Windows Driver Kit (WDK), предоставляемого фирмой Microsoft, – драйвера Pussthru – разработана утилита, осуществляющая мониторинг сетевого трафика. А также описаны потенциальные возможности, допускаемые при использовании WDK, помогающие в решении вопросов сетевой безопасности.

MS Windows платформаларында жұмыс істейтін желілер үшін желілік кауіпсіздік мәселесі зерттелген. Осы мақсатта Windows драйвер моделіне шолу жасалған. Microsoft фирмасы ұсынатын Windows Driver Kit (WDK) драйверлер құру жиынтығының бір мысалы – Pussthru драйверінде негізделген желілік трафикті бақылауды іске асыратын утилита-бағдарламасы құрылған. Және де WDK-ны қолдану барысында пайдалануға болатын, желілік қауіпсіздік мәселелерін шешуге көмектесе алатын мүмкіндіктер сипатталған.