УДК 004.056.5
А.А. Брюховецкий, доцент, канд. техн. наук,
Г.Г. Сергеев, доцент, канд. техн. наук,
А.В. Скатков, проф., д-р техн. наук,
А.А. Абрамян
Севастопольский национальный технический университет
Студгородок, г.Севастополь, Украина, 99053
Pu88@mail.ru

ПРОГРАММНАЯ СИСТЕМА ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА ДЛЯ ОС WINDOWS

Рассматривается программный сетевой экран для защиты от несанкционированного доступа к информации для операционной системы Windows. Приводятся структуры и алгоритмы обработки данных, а также результаты тестирования программы в ОС Windows 95, Windows 95 OSR2, Windows 98, Windows 98SE на компьютерах с различной конфигурацией.

Главная причина проблемы безопасности при работе любого пользователя в Интернете связана с тем, что, получая доступ к ресурсам многих компьютеров сети, он одновременно предоставляет доступ, в той или иной степени, к ресурсам своего компьютера. Поэтому при работе в сети возможны ситуации, которые будут происходить независимо от действий пользователя. Практически любому пользователю, работающему в интернете, приходилось сталкиваться с так называемыми программами – spyware. Эти программы могут попасть в компьютер различными путями: от установки вместе с другими программами, до «прилипания» к компьютеру во время просмотра веб-страниц, содержащих ActiveX компоненты или Java – апплеты, которые в принципе могут выполнять любые действия, например, передавать файлы с частной информацией на другие компьютеры в сети. Кроме того, на компьютере может размещаться нежелательная информация (cookie или reference), по которой другие компьютеры сети смогут определить, к какой информации обращался пользователь и кто, в свою очередь, обращался к его компьютеру. При этом злоумышленники зачастую получают доступ к компьютеру пользователя не с тех узлов, которые он посещает, а с других, методом «сканирования» адресов протокола TCP/IP.

Наиболее широко за последние годы получила распространение операционная среда (ОС) Windows 98 и ее доработанная версия Windows 98SE. Она нетребовательна к ресурсам компьютера по сравнению с ОС семейства Windows NT. В этих операционных средах (Windows 9x) подсистема доступа к сетевым протоколам и их контроля реализована на основе одних и тех же библиотек, а значит и для разработки программ требуется идентичный код, использующий эти библиотеки. Таким образом, доступ в интернет в этих ОС реализован одинаково, но в них нет встроенной возможности контроля исходящего и входящего трафика.

В связи с тем, что в настоящее время на рынке специализированного программного обеспечения сложилась ситуация, когда значительная часть пользователей работает в ОС Windows 9x и спрос на высокотехнологичные реализации программных сетевых экранов – брандмауэров достаточно большой, их разработка является актуальной задачей [1,2]. В отличие от брандмауэров, реализованных на специализированных аппаратных платформах, персональные представляют собой относительно дешевое ПО, которое инсталлируется непосредственно на каждый защищаемый ПК. Такие брандмауэры осуществляют контроль над сетевыми устройствами и выполняют те же основные функции, что и корпоративные брандмауэры: обнаружение попыток вторжения, контроль доступа, выполнение правил безопасности, регистрацию событий. Персональный брандмауэр фильтрует весь сетевой трафик, разрешая только санкционированные соединения.

Программная система содержит следующие реализации: 1 – драйвера виртуального устройства, который предназначен для перехвата функций системного драйвера ndis.vxd, и 2 – собственно пользовательской части, из которой передаются параметры для разрешения или блокировки трафика. Драйвер виртуального устройства был разработан с использованием специального инструмента для разработки драйверов – DriverStudio [3]. Это – набор инструментальных средств, который позволяет быстро и профессионально разработать надежные, в том числе, сетевые драйверы NDIS (Network Device Interface Specification) и TDI (Transport Data Interface) для 32–битных приложений Windows. Для реализации программы на основе фильтрации трафика необходимо, чтобы разрабатываемый виртуальный драйвер грузился системой после загрузки системного драйвера ndis.vxd, но до регистрации сетевых протоколов. В созданном модуле виртуального драйвера реализованы следующие основные функции:

- вывод в лог-файл состояние пакета (строка с IP портами пакета, флаг приемки / отправки пакета, флаг состояния пакета, флаг результата);
- определение принадлежности IP-адреса;
- определение принадлежности порта;
- прием или блокировка пакета;
- вывод сообщений пользователю;
- очистка лог-файла при перезагрузке системы.

Пользовательский интерфейс программы был разработан в среде визуального программирования Borland Delphi. Использовались только стандартные компоненты среды программирования. Для

реализации дополнительных возможностей использовались функции ОС Windows – API [4]. Базовые структуры модуля интерфейса следующие: структура, описывающая один протокол; структура, описывающая один адаптер; структура, описывающая все протоколы и адаптеры. Основные функции и процедуры, используемые в модуле, перечислены ниже:

- функция вызывается драйвером при неизвестной комбинации состояния пакета;
- функция инициализирует доступ к драйверу; возвращает true, если удалось получить доступ к драйверу;
- процедура обновления списка протоколов и их адаптеров; также обновляется панель, на которой отображается выбранный протокол;
- процедура завершения работы защитного экрана; выполняет все необходимые действия для правильного завершения работы программы;
- процедура контроля состояния сетевого трафика; для различных режимов работы программы в системном трее отображаются разные значки;
- процедура чтения сохраненных настроек программы из файлов разрешенных и запрещенных комбинаций;
- процедура сохранения настроек программы в файлы разрешенных и запрещенных комбинаций.

Защитный сетевой экран с пакетным фильтром анализирует проходящий трафик, просматривая IP – адреса и номера TCP портов в заголовке текущего пакета, и принимает решение о том, пропускать пакет или блокировать. Пакетная фильтрация в данном случае состоит в сравнении адресов и портов в пакете с адресами и портами, прописанными в правилах. Правила доступа используют в качестве параметров следующие: адрес источника (отправителя); порт источника; адрес назначения (получателя); порт назначения. Причем один из адресов обязательно должен быть локальным адресом компьютера.

Правила прохождения пакетов хранятся в файлах настроек, которые находятся в соответствующем каталоге программы. Реализована следующая система правил защитного экрана:

- разрешение/блокировка исходящего трафика на определенные узлы;
- разрешение/блокировка входящего трафика с определенных узлов;
- разрешение/блокировка всего исходящего трафика;
- разрешение/блокировка всего входящего трафика.

Разработана сервисная утилита, облегчающая ввод, удаление, просмотр и редактирование набора правил администратором в графическом интерфейсе системы. Для каждого пакета программа просматривает весь набор правил в следующем порядке:

1) при прохождении пакета программа выделяет из его заголовка адрес отправителя, порт отправителя, адрес получателя и порт получателя;

2) анализируется список запрещенных комбинаций на наличие точного совпадения с проходящим пакетом; точным совпадением считается совпадение полученных параметров пакета с параметрами правила, не содержащего символ «*»; при этом в правиле допускается наличие диапазонов.

Программа была исследована на сериях тестов в ОС Windows 95, Windows 95 OSR2, Windows 98, Windows 98SE на компьютерах с типовой конфигурацией устройств, включающей процессоры Intel Celeron, Pentium, AMD Athlon и т.п. Так, например, в одной из серий тестов программа не была предварительно настроена. Поэтому при каждом обращении к узлу пользователю задавались запросы на разрешение или запрещение трафика. В частности, после запуска системы был осуществлен доступ на узел www.microsoft.com. Пользователю был задан запрос на действия для исходящего трафика с узла 195.5.36.117 порт 1027 на 207.46.249.222 порт 80. В появившемся окне была нажата кнопка **Разрешить.** В другой серии тестов программа предварительно настраивалась. Так, в одном из запусков системы в настройках были указаны параметры, разрешающие весь исходящий трафик с локального адреса на узел 81.19.66.109 (www.rambler.ru). В данном случае программа не выдавала запросов о действиях с исходящим трафиком, но были выданы запросы на действия с входящим трафиком. Наконец в третьей серии тестов на компьютере была установлена ОС Windows 2000. При запуске программа выдала сообщение об ошибке «Не могу загрузить драйвер ndis.vxd». Такое поведение программы является предусмотренным, поскольку виртуальный драйвер перехвата трафика разрабатывался для ОС Windows 9x. В ОС семейства Windows NT анализ трафика осуществляется через другие библиотеки и механизм перехвата трафика существенно отличается от Windows 9x.

Таким образом, в процессе испытаний программы проверена правильность обработки задаваемых правил на разрешение/блокировку трафика на компьютерах с различными ОС и конфигурациями. Это обстоятельство даёт основания для её использования для защиты информации от несанкционированного доступа на персональном компьютере при работе в Интернете.

Дальнейшие исследования предполагают разработку модуля «антиспам», осуществляющего защиту компьютера от несанкционированной рассылки почтовых сообщений.

Библиографический список

1. Чемпен Д. Брандмауэры Cisco Secure PIX / Д. Чемпен, Э.Фокс. — М.: Изд–во «Вильямс», 2003. — 384 с.

2. Польман Н. Архитектура брандмауэров для сетей предприятия / Н.Польман, Т.Кразерс. — М.: Изд–во «Вильямс», 2003. — 430 с.

3. Газах К. Разработка виртуальных драйверов для устройств Microsoft® Windows. / К.Газах // Soft & Script. — 2001. — № 31. — С. 51 – 53.

4. Ганеев Р.М. Проектирование интерфейса пользователя средствами Win32 API / Р.М.Ганеев. — М.: Изд–во «Радио и связь», 2001. —346с .

Поступила в редакцию 30.06.2004 г.