Практическая работа №15

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ И ДОСТУПА

Цель работы. Изучить способы защиты программного обеспечения от несанкционированного копирования и доступа.

Краткие сведения из теории

Рассматривая компьютер в составе глобальной или локальной сети как множество компонентов, являющихся объектами нападения, можно выделить три типа несанкционированного доступа (НСД):

– локальный НСД;

– удаленный НСД по сети без доступа непосредственно к компьютеру;

– НСД к информации на отчуждаемых компонентах, т. е. съемных носителях и в канале связи с другими компьютерами.

Локальный НСД – попытки получения информации при непосредственном доступе к компьютеру).

Рассмотрим несколько примеров. Возьмем известную утилиту Descreet из комплекта Norton Utilities. В основе ее работы по преобразованию информации лежит не менее широко известный алгоритм DES. Пусть пароль шифрования имеет достаточную длину, не позволяющую восстановить его полным перебором. Стойкость DES до недавнего времени подвергалась сомнениям (которые впоследствии оказались небезосновательными). Очевидно, что без применения специальных алгоритмов, используя только образ шифрованного диска, получить его содержимое и пароль за приемлемое время весьма затруднительно.

Для несанкционированного получения информации представляются разумными следующие варианты атак:

1. Атака целевым вирусом (закладкой):

– создать программу-вирус, заражающую только программу-драйвер DESCREET и при вводе пароля сохраняющую пароль в свободных областях на жестком диске (например, в зарезервированных секторах на нулевой дорожке, вместо серийного номера ОС вторичного загрузчика) или в незанятых "хвостах" (кластеров);

– внедрить программу-вирус в атакуемый компьютер;

– получить пароли.

– 2. Атака общим вирусом:

– создать программу, которая сохраняет первые несколько десятков байтов ввода после старта программ в скрытом файле;

– внедрить программу-вирус в атакуемый компьютер;

– снять полученную информацию;

– после изучения этой информации выделить пароль в открытом виде.

Против подобных атак можно применить различные проверки целостности программного обеспечения, которые, в свою очередь, могут быть нейтрализованы стелс-механизмами вирусов, и т. д. В конце концов можно предложить универсальную закладку, работающую в защищенном режиме микропроцессора, блокирующую всякого рода попытки программ пользователя переключиться в защищенный режим и эмулирующую все известные способы обращения к расширенной памяти. При таком подходе любые способы контроля целостности ПО не дадут корректного результата. Конечно, это будет закладка-монстр, но применяемые механизмы защищенного режима микропроцессора позволят скрыть значительные объемы информации.

Из вышесказанного следует, гарантированно корректно работает та программа (закладка или средство защиты от нее), которая первой получает управление.

Удаленный НСД по сети без доступа непосредственно к компьютеру

Во многих областях приходится пользоваться импортным программным обеспечением и аппаратными средствами передачи информации по сети с коммутацией пакетов. Ряд фирм (например, HP) ставят связные сервера вместе с программным обеспечением «под ключ», при этом еще и блокируя интерфейс администратора. В этом случае для гарантированной защиты обрабатываемой информации важно, с одной стороны, чтобы управление средствами шифрования не зависело от импортного программного обеспечения, а с другой – чтобы средства защиты были по возможности "прозрачными" по отношению к средствам обработки информации.

Использование многих программных продуктов создает дополнительные каналы утечки информации. Одними из наиболее популярных являются средства работы в Internet, предоставляемые фирмой Microsoft. Если внимательно (не штатными средствами MS Windows) рассмотреть файл WinWord, то в нем, помимо нескольких версий нужного документа, можно увидеть следы других документов. При отправке такого файла по сети могут "уйти" какие-нибудь «секретные слова». Противник может связать эти слова с почтовым адресом и фамилией конкретного человека, а потом продолжить работу с ним другими методами.

Учитывая полное отсутствие на сегодняшний день доверенных отечественных операционных систем и сетевых операционных систем в частности, говорить о передаче по каналам Internet конфиденциальной информации в общем случае не приходится. Кроме того, свойства семейства протоколов TCP/IP версии 4.0 не позволяют производить гарантированную идентификацию и аутентификацию пользователей.

В сложившейся ситуации можно говорить только о передаче конфиденциальной информации по виртуальным сетям. В данном случае под вир-

туальной сетью понимается сеть, образованная множеством криптомаршрутизаторов, использующих Internet как транспортную среду передачи данных. Каждый криптомаршрутизатор защищает свою подсеть посредством шифрования исходящих и расшифровки входящих пакетов. Криптомаршрутизаторы обмениваются информацией, зашифрованной на ключах парной связи между ними. Обмен ключами по сети отсутствует. Для закрытия информации эксплуатируется принцип инкапсуляции со скрытием внутренних адресов. Это означает, что выходящий пакет шифруется полностью вместе с заголовком на ключе парной связи текущего криптомаршрутизатора и криптомаршрутизатора, закрывающего подсеть, содержащую абонента. К этой криптограмме добавляется IP заголовок, с адресом отправителя – внешний адрес текущего криптомаршрутизатора и с адресом получателя – адрес криптомаршрутизатора, закрывающего сеть корреспондента. Для прохождения полученного пакета через устройства маскировки топологии надсетей (NAT) необходимо к IP заголовку добавить подзаголовок произвольного протокола, например UDP с некоторыми неиспользуемыми портами. Отсюда следует, что извне обмен информацией между защищаемыми подсетями выглядит как обмен UDP пакетами между парой компьютеров. Пользователи защищаемых сетей никакого влияния (за исключением некоторого замедления за счет шифрования) не замечают.

Все попытки зондирования нарушителем внутренних подсетей будут неудачными, поскольку пришедший пакет не будет правильно расшифрован. Отсутствие необходимости поддерживать транспортный уровень стека протоколов TCP/IP приводит к недейственности атак на транспортный уровень, что повышает надежность работы криптомаршрутизаторов.

Очевидно, что при таком подходе получить доступ к открытой сети Internet невозможно, но защита такого рода будет надежной с точностью до стойкости алгоритма шифрования.

НСД к информации на отчуждаемых компонентах, т. е. съемных носителях и в канале связи с другими компьютерами.

Для топологии сети «точка-точка» при возможном внедрении нарушителем произвольных закладок в программное обеспечение компьютеров и работе по коммутируемому или выделенному каналу по протоколу RS-232 возможно применение наложенных средств шифрования канала. Если обеспечить включение алгоритмов шифрования в состав каналообразующей аппаратуры только при непосредственной передаче информации в линию и выключение при отсутствии передачи информации при конфигурировании модема, то вне зависимости от количества и агрессивности закладок, нарушитель:

не сможет оказывать асинхронное воздействие извне на программно-аппаратные комплексы;

не получит открытую информацию, передаваемую по каналу при непосредственном съеме информации с линии;

не получит открытую информацию при перенаправлении ее по коммутируемому каналу.

Единственно, что может сделать закладка нарушителя, внедренная в ПО, – так это передавать ему «морзянкой», используя канал «окончания/начала» или «ошибка/не ошибка приема/передачи» сообщений. Однако, если учитывать скорость работы по коммутируемому каналу и инерцию каналообразующего оборудования, доля передаваемой таким способом информации представляется незначительной.

Порядок выполнения работы

1 Изучить краткие сведения из теории.

2 Произвести анализ угроз программному обеспечению по заданию преподавателя от локального НСД.

3 Произвести анализ угроз программному обеспечению по заданию преподавателя от удаленного НСД.

4 Произвести анализ угроз программному обеспечению по заданию преподавателя на отчуждаемом компоненте.

Содержание отчета

1 Цель работы.

2 Перечень мероприятий и их краткая характеристика при защите программного обеспечения от копирования.

3 Перечень мероприятий и их краткая характеристика при защите программного обеспечения от НСД.

4 Вывод по работе.

Контрольные вопросы

1 Угрозы информационной безопасности программного обеспечения.

2 Методы защиты программного обеспечения от копирования.

3 Методы защиты программного обеспечения от локального НСД.

4 Методы защиты программного обеспечения от удаленного НСД.

5 Методы защиты программного обеспечения от НСД к информации на отчуждаемых компонентах.