УДК 621.38

М.ДЖ.ОРОЗАЛИЕВ, Д.Ш.ОСМОНАЛИЕВ,
Ж..Р.ОСМОНОВА, К.Б.ТУРГАНОВ
E-mail: ksucta@elcat.kg.

ВОЗМОЖНОСТИ ПОДСИСТЕМЫ ЗАЩИТЫ WINDOWS И ЕЕ ТЕСТИРОВАНИЕ

Иштелип чыккан маалыматтын конфиденциалдуулугун, бүтүндүгүн жана жеткиликтүүлүгүн сактоо көбүнчө колдонулган операциялык тармактардын мүнөздөмөсүнөн көз каранды. Аяккы убактарда Microsoft Windows 2000/XP операциялык системасы кеңири тарады. Актуалдуу маселелердин бири болуп, көптөгөн жетиштүү укутарды жана шарттрады аныктоо, анын жардамы менен кирүүгө мүмкүнчүлүк кеңейет. Windows тун аныкдал келбестигин жана декларацияланган мүмкүнчүлүктөрдүн проблемаларын чечүү, операциялык системанын коопсуздугунун механизимине жана иштелип чыккан жыйынтыгын фиксирлөөгө тестик таасир этүүгө негизделген укуктардын жана шарттардын жетиштүү комбинацияларынын методун иштеп чыгуу жолу менен чечүүгө болот.

Поддержание конфиденциальности, целостности и доступности обрабатываемой информации во многом зависит от характеристик используемых операционных систем (ОС). В последнее время широкое распространение получила ОС Microsoft Windows 2000/XP.

Актуальной задачей является определение множества достаточных прав и привилегий (ДПП), при которых разрешается доступ. Решение проблемы несоответствия реальных и декларируемых возможностей (РДВ) Windows возможно путем разработки метода определения достаточных комбинаций прав и привилегий, основанного на оказании тестового воздействия на механизмы безопасности ОС и фиксировании результатов срабатывания.

Maintenance of confidentiality, integrity and availability of the processed information in many respects depends on characteristics of used operational systems (OS). Recently a wide circulation has received OS Microsoft Windows 2000/XP.

Actual problem is definition of set of the sufficient rights and privileges (ДПП) at which access is authorised. The decision of a problem of discrepancy of real and declared possibilities (РДВ) Windows is possible by working out of a method of definition of sufficient combinations of the rights and the privileges, the test influence based on rendering on mechanisms of safety of OS and fixation of results of operation.

Поддержание конфиденциальности, целостности и доступности обрабатываемой информации во многом зависит от характеристик используемых операционных систем (ОС). В последнее время широкое распространение получила ОС Microsoft Windows 2000/XP (далее —

Windows). Разработчики средств защиты и администраторы безопасности данной ОС имеют в своем распоряжении огромное количество разнообразной документации. Несмотря на это, открытые источники не содержат исчерпывающих сведений, раскрывающих все детали алгоритмов работы подсистемы защиты. Но даже использование доступных сведений не гарантирует адекватности разработки программных продуктов и корректности конфигурирования Windows. Множество нарушений безопасности возможно из-за неточности применяемой документации, что служит причиной ошибок в использовании функций подсистемы защиты.

Примером неточного описания прав и привилегий является указание на то, что право KEY_CREATE_LINK для ключа реестра зарезервировано только под системное использование, однако известно, что данное право необходимо при создании ссылки на ключ реестра с помощью функции Win32 API RegCreateKeyEx /1/. Примером неполного предоставления информации в MSDN также служит осуществление операции "чтение файла". Для выполнения данной операции пользователь должен иметь право FILE_READ_DATA на объект. Однако данное требование является лишь необходимым условием для доступа к файлу по чтению, но не достаточным. Иными словами, если пользователь обладает только необходимым правом, то доступ будет запрещен. Актуальной задачей является определение множества достаточных прав и привилегий (ДПП), при которых разрешается доступ. Решение проблемы несоответствия реальных и декларируемых возможностей (РДВ) Windows возможно путем разработки метода определения достаточных комбинаций прав и привилегий, основанного на оказании тестового воздействия на механизмы безопасности ОС и фиксировании результатов срабатывания.

В Windows контроль доступа осуществляется монитором обращений – специальным компонентом исполнительной системы, отвечающим за проверку прав доступа к ресурсам ОС, проверку привилегий и генерацию сообщений аудита /2, 3/. Как и в аналитическом представлении информационной системы в виде совокупности субъектов, объектов и прав доступа /4/, в Windows можно выделить указанные множества:

– множество субъектов ассоциируется с пользователями. Любой поток в ОС обладает маркером доступа пользователя, от имени которого он запускается. При проверке полномочий на выполнение действий монитор обращений использует составляющие маркера: идентификатор защиты пользователя, его группы и привилегии;

– множество объектов в Windows включает все защищаемые именованные ресурсы, предназначенные для хранения или обработки информации. Примерами таких объектов являются файлы, каталоги, ключи реестра, сервисы, принтеры, процессы, разделяемые ресурсы, объекты ядра;

– с каждым объектом сопоставлено множество прав доступа, выполненных в виде списков контроля доступа DACL. Список прав содержит множество записей, каждая из которых представляет собой пару "субъект-маска доступа". Маска доступа – 32-разрядное число, в котором каждый бит определяет некое право доступа субъекта к данному объекту.

Для тестирования монитора обращений на предмет выявления РДВ используется модель потока данных как один из подходов тестирования "черного ящика" /5/. В данной модели выделены два основных узла: входной и управляющий. Входной поток данных представлен множеством настроек безопасности, т.е. прав доступа и привилегий пользователей, влияющих на доступ к объекту. В роли управляющего узла выступает алгоритм принятия решения о предоставлении доступа, реализованного в мониторе обращений. В качестве результата, генерируемого управляющим узлом, выступает вердикт "доступ разрешен" или "доступ запрещен". Программная реализация метода представлена в виде средства, структурная схема которого представлена на рис. 1.

Параметрами исследования являются данные авторизации некоторого тестового пользователя, тип и имя объекта тестирования (например, файла) и действие (например, чтение данных), попытка осуществления которого будет производиться относительно объекта. Изменение комбинаций масок доступа и пользовательских привилегий во время тестирования осуществляет модуль изменения настроек безопасности. Модуль инициализации выполняет начальные установки. В тестирующей программе соответствующие подмодули производят попытки выполнения заданного действия над тестовым объектом. Таким образом, на выходе тестирующей программы генерируется множество ДПП по отношению к заданному типу объекта, полученное в результате работы подмодулей. Управление всем процессом осуществляет модуль тестирования настроек безопасности.

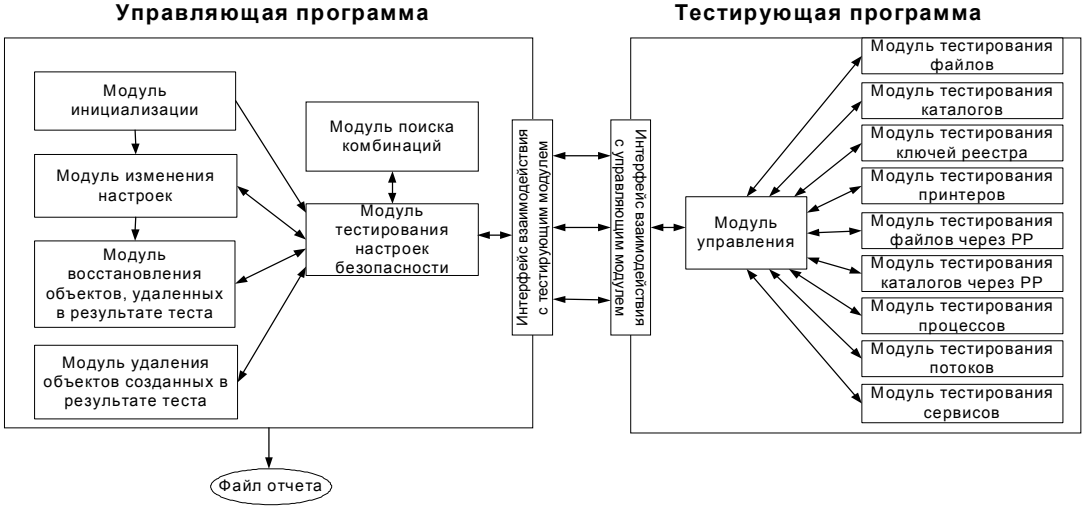

Рис. 1. Схема программного средства тестирования

Выполнение полного перебора всех комбинаций прав и привилегий для действий над всеми типами тестируемых объектов занимает огромный промежуток времени (например, для элементов файловой системы NTFS перебор требует более 20 часов). Поэтому был разработан алгоритм поиска ДПП, основанный на логической обработке накопленных экспериментальных данных /6/. Данный алгоритм реализован в модуле поиска комбинаций.

В качестве примера результирующих данных рассмотрим часть файла отчета, которая содержит список ДПП для действия "чтение данных" файла:

****
* ПРОГРАММА ПОИСКА ДПП *
****

Тестовое действие: “чтение данных”

Тип объекта: “файл”

Пользователь должен иметь права/привилегии:

[

прив.: SeChangeNotifyPrivilege (проход по структуре каталогов)

права: на файл:

FILE_READ_DATA (чтение данных - бит 0)

FILE_READ_ATTRIBUTES (чтение атрибутов - бит 7)

SYNCHRONIZE (синхронизация - бит 20)

]

ИЛИ

[

прив.: SeBackupPrivilege (архивирование файлов и каталогов)

SeChangeNotifyPrivilege (проход по структуре каталогов)

]

ИЛИ

[

прив.: SeChangeNotifyPrivilege (проход по структуре каталогов)

права: на контейнер:

FILE_LIST_DIRECTORY (просмотр каталога - бит 0)

права: на файл:

FILE_READ_DATA (чтение данных - бит 0)

SYNCHRONIZE (синхронизация - бит 20)

]

ИЛИ

[

прив.: SeChangeNotifyPrivilege (проход по структуре каталогов)

SeRestorePrivilege (восстановление файлов и каталогов)

права: на контейнер:

FILE_LIST_DIRECTORY (просмотр каталога - бит 0)

права: на файл:

FILE_READ_DATA (чтение данных - бит 0)

]

В соответствии с MSDN, пользователь для осуществления действия "чтение данных" над файлом должен обладать разрешениями:
правом GENERIC_ALL (общий полный доступ - бит 28)
ИЛИ
правом GENERIC_READ (общее чтение - бит 31)
ИЛИ
правом FILE_READ_DATA (чтение данных - бит 0).

При сопоставлении документации MSDN и полученных в ходе тестирования результатов позволяет выделить, например, следующие несоответствия:

– в MSDN указано, что для доступа необходимо, чтобы пользователь обладал правом GENERIC_ALL (общий полный доступ – бит 28) или правом GENERIC_READ (общее чтение – бит 31). Однако в действительности пользователь не может программно выставить биты 28 или 31. Причина этого кроется в автоматическом проецировании системой общих битов на другие биты маски;

– в MSDN указано, что для доступа по чтению пользователю необходимо обладать правом FILE_READ_DATA (чтение данных – бит 0). Однако помимо данного права пользователь должен иметь привилегию SeChangeNotifyPrivilege (проход по структуре каталогов), правами FILE_READ_ATTRIBUTES (чтение атрибутов – бит 7), SYNCHRONIZE (синхронизация – бит 20) или привилегией SeChangeNotifyPrivilege (проход по структуре каталогов), правом FILE_LIST_DIRECTORY (просмотр каталога – бит 0) на контейнер, правом SYNCHONIZE (синхронизация – бит 20).

Проведенное тестирование позволило выявить реальные возможности монитора обращений в части алгоритма принятия решений о предоставлении доступа. Составлены логические функции, определенные на множествах прав и привилегий, что позволило определить РДВ подсистемы защиты Windows. Число выявленных несоответствий РДВ представлено в табл.1.

Таблица 1

Количество выявленных несоответствий РДВ

Тип объекта защиты Windows	Кол-во
Файлы	118
Каталоги	81
Элементы реестра	29
Разделяемые ресурсы	7
Принтеры	12
Сервисы	19
Процессы	28
Потоки	23

Данные о РДВ подсистемы безопасности Windows могут быть использованы для осуществления корректного администрирования ОС и разработки средств защиты информации в Windows. Таким образом, полученные результаты позволяют избежать множества уязвимостей, вызванных использованием неполной и неточной документации на этапах проектирования, разработки и настройки различных программных продуктов, использующих возможности Windows.

Список литературы

1. MSDN Library - Visual Studio.Net 2003: http://msdn.microsoft.com.

2. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. № 187. – 2002. – 56 с.

3. Соломон Д., Руссинович М. Внутреннее устройство Microsoft Windows 2000. Мастер-класс. – СПб.: Питер; М.: Изд.-торговый дом "Русская редакция", 2001. – 746 с.

4. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000. – 452 с.

5. Бейзер Б. Тестирование черного ящика. –СПб.: Питер, 2004. – 320 с.