УДК 004.056.52/53:004.72

В.А. Гончаров, В.Н. Пржегорлинский

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРОТИВОДЕЙСТВИЯ СЕТЕВЫМ ИНФОРМАЦИОННЫМ АТАКАМ СО СТОРОНЫ ЗАЩИЩЕННЫХ ОС И СИСТЕМ ОБНАРУЖЕНИЯ ИНФОРМАЦИОННЫХ АТАК

Рассмотрена реализация разграничения доступа, реализованная в защищенных ОС. Введено понятие информационной атаки, и определены фазы информационных атак. Рассмотрено противодействие информационным атакам со стороны систем обнаружения информационных атак. Введены классы способов реализации фаз информационных атак. Выполнено сравнение возможностей по противодействию информационным атакам со стороны защищенных ОС и локальных и сетевых систем обнаружения информационных атак.

Цель исследования заключается в определении (установлении) возможностей существующих методов и средств разграничения доступа, встроенных в защищенные ОС и используемых в системах обнаружения информационных атак, по противодействию сетевым информационным атакам на информационные системы.

Для описания методов и средств разграничения доступа субъектов доступа к объектам доступа будем использовать концепцию монитора обращений [1, 2]. Защищенными ОС являются операционные системы, в которых монитор обращений реализован как компонент ядра ОС. Реализацию монитора обращения в защищенных ОС называют ядром безопасности (security kernel) [1], которое выполняет разграничение доступа субъектов ОС к объектам ОС. Субъектом ОС является задача (процесс или поток выполнения, task, process, thread), которой соответствует идентификатор пользователя ОС, от имени которого задача выполняет обращения к объектам ОС. При проверке доступа монитором обращений ОС используется идентификатор пользователя субъекта ОС. Разделим доступ субъектов ОС к объектам ОС на локальный доступ, то есть доступ к локальным объектам этой ОС, и на сетевой доступ, то есть доступ к объектам других ОС, выполняемый через вычислительную сеть.

Рассмотрим реализацию разграничения доступа субъектов ОС к объектам ОС при сетевом доступе. В защищенной вычислительной сети каждый узел работает под управлением защищенной ОС и имеет свой монитор обращений, свое множество субъектов ОС и объектов ОС. Пусть субъект ОС s узла сети h_1 ($s@h_1$) обращается к объекту o узла сети h_2 ($o@h_2$) для выполнения действия a. Для этого субъект $s@h_1$ должен выполнить программный код сетевого клиента, реализующего определенный сетевой протокол. Обмен данных через сеть передачи данных (СПД) происходит с узлом h_2; данные принимаются и обрабатываются программным кодом сетевого сервера, реализующего такой же протокол. Программный код сетевого сервера выполняет субъект $s@h_2$, который обращается к объекту $o@h_2$.

Информационной атакой (attack) на информационную систему будем называть действие или последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы безопасности информации, обрабатываемой в информационной системе, путем использования уязвимостей этой информационной системы. Последовательность действий нарушителя, составляющих информационную атаку, можно разделить на фазы информационной атаки [3].

А. Сбор информации об информационной системе и используемых средствах защиты.

Б. Использование уязвимостей информационной системы.

В. Сокрытие следов использования уязвимостей информационной системы и обеспечение долговременного присутствия.

В фазе "А" производятся сбор и анализ доступной информации об информационной систе-

ме и используемых средствах защиты. Целью данного анализа является определение наиболее вероятных уязвимостей информационной системы.

В фазе "Б" происходит попытка использования уязвимостей, определенных на первом этапе, для последующей реализации угроз безопасности информации. Попытки использования уязвимостей производятся вплоть до реализации требуемых угроз безопасности информации.

Поскольку факты сбора информации об информационной системе и используемых средствах защиты и попытки использования уязвимостей (как неудачные, так и удачные) могут оставлять следы в журналах аудита и в измененных объектах информационной системы, нарушителю необходима третья фаза проведения информационной атаки – сокрытие следов. В случае успешного сокрытия следов факт реализации угрозы останется неизвестным. Обеспечение долговременного присутствия в информационной системе позволяет повторно реализовывать требуемую угрозу безопасности информации, возможно, даже без оставления следов в журналах аудита. Фактически обеспечение долговременного присутствия в информационной системе реализуется добавлением новой уязвимости в информационную систему.

Каждую из рассмотренных фаз информационной атаки можно считать самостоятельной информационной атакой, которой необходимо оказать противодействие.

В защищенных ОС стандартным механизмом блокирования информационных атак является монитор обращений, который проверяет доступ субъекта ОС на соответствие правилам политики безопасности и разрешает или запрещает его. Свои действия монитор обращений должен записывать в журнал аудита. Таким образом, информация о попытках организации информационных атак должна содержаться в журналах аудита.

Для автоматизации задачи анализа журналов аудита были созданы первые системы обнаружения информационных атак (СОА, Intrusion Detection System – IDS). Классические СОА состоят из следующих компонентов: датчика, решателя и интерфейса пользователя. Решатель СОА является ее основным компонентом, так как именно он обнаруживает (идентифицирует) информационные атаки на основе информации, поставляемой датчиками. В сетевых СОА (Network IDS – NIDS) датчики предоставляют информацию, получаемую при разборе сетевых протоколов. В классической схеме применения сетевых СОА датчик получает все пакеты, проходящие на данном участке (сегменте) сети. Решатель в сетевых СОА обычно совмещен с датчиком для достижения максимальной производительности.

Основными проблемами использования СОА [5] являются нехватка производительности для решателя и "ложные срабатывания", то есть ложное обнаружение информационной атаки или пропуск информационной атаки. Рассмотрим, какие способы противодействия информационным атакам могут использовать СОА.

Административное противодействие – вывод сообщения администратору безопасности. Администратор безопасности по дополнительным признакам определяет, не является ли это ложным срабатыванием, а затем предпринимает какие-либо действия по блокированию, ограничению последствий или ограничению распространения информационной атаки.

Блокирование информационной атаки. Происходит блокирование доступа субъекта доступа к объекту доступа, которое может привести к реализации информационной атаки. Это возможно только при встраивании СОА в монитор обращений.

Прерывание информационной атаки. Если реализация информационной атаки состоит из последовательности действий, причем обнаружить ее можно по выполнению первых шагов, а реализована она будет только после выполнения последующих шагов, то после обнаружения информационной атаки по первым шагам необходимо воспрепятствовать выполнению последующих шагов, то есть принять упреждающие меры [4].

Для каждой из рассмотренных фаз информационной атаки введем классы способов реализации данной фазы информационной атаки. Данные классы будут включать в себя типичные способы реализации фаз информационных атак, которые могут быть реализованы в информационной системе.

Фаза "А". Сбор информации об информационной системе.

*Класс А*1. *Сбор служебной информации об информационной системе.* Информация об информационной системе включает в себя информацию об объектах и пользователях информационной системы, правах доступа, используемом ПО и т.д.

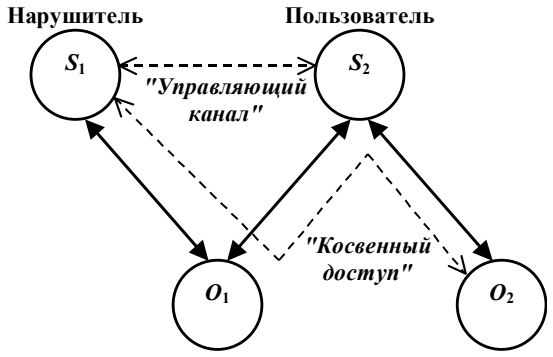
*Класс А*2. *Сканирование объектов доступа информационной системы.* Сканирование объектов позволяет за счет выполнения множества разрешенных действий перебором определить, какие объекты присутствуют в информационной системе.

*Класс А*3. *Сканирование прав доступа к объектам информационной системы.* Сканирование прав доступа позволяет на базе попыток выполнения всех возможных видов доступа к объектам доступа информационной системы определить, разрешен или запрещен такой доступ.

Фаза "Б". Использование уязвимостей информационной системы.

*Класс Б*1. *Использование субъекта в качестве посредника.* Субъекту доступа нарушителя запрещен доступ к объекту доступа, однако он может создавать "управляющий канал" через общий объект доступа с другим субъектом доступа, который имеет требуемые права доступа к объекту доступа (см. рисунок). С помощью такого "управляющего канала" нарушитель сможет получить косвенный доступ к объекту доступа, несмотря на то, что непосредственный доступ запрещен политикой безопасности.

*Класс Б*2. *Работа в незащищенной СПД.* СПД будем называть незащищенной, если при подключении к ней нарушитель сможет выполнить хотя бы одно из следующих видов воздействий: получать информацию, передаваемую одним из узлов, подключенным к данной СПД, в том числе адресованную не узлу нарушителя; отправлять информацию одному из узлов, подключенным к данной СПД, в том числе от имени другого узла; блокировать передачу информации от одного из узлов, подключенных к данной СПД, другому узлу. С помощью этих воздействий нарушитель сможет реализовать угрозы нарушения конфиденциальности, целостности и доступности передаваемой и обрабатываемой в информационной системе информации.



Фаза "В". Сокрытие следов и обеспечение долговременного присутствия.

*Класс В*1. *Сокрытие следов использования уязвимостей информационной системы.* Нарушитель реализует угрозу нарушения целостности по отношению к журналам аудита.

*Класс В*2. *Начало присутствия в информационной системе – добавление скрытой уязвимости.* Нарушитель добавляет новую уязвимость, позволяющую реализовывать требуемые угрозы безопасности информации, возможно, без оставления следов в журналах аудита.

*Класс В*3. *Присутствие в информационной системе – организация скрытых каналов передачи данных.* Нарушитель организует передачу данных между объектами информационной системы, возможно, с нарушением политики безопасности, без оставления следов в журналах аудита.

Рассмотрим основные возможности противодействия информационным атакам со стороны монитора обращений ОС, локальных и сетевых СОА для различных способов реализации их фаз.

*Классы А*1-*А*3. Монитор обращений способен противодействовать классу А1 только в случае, если политика безопасности явно запрещает все виды доступа, которые приводят к получению служебной информации об информационной системе. Монитор обращений ОС не будет противодействовать классам А2, А3 для локальных информационных атак, так как они выполняются на базе анализа ответов монитора обращений ОС. СОА выполняют обнаружение классов А2, А3 на базе статистических моделей и использования заданных порогов определенных событий за единицу времени. Из-за низкого качества таких моделей обычно используется административный способ противодействия, так как ложное срабатывание при этом не приводит к нарушению работы информационной системы.

*Класс Б*1. Монитор обращений ОС не будет противодействовать классу Б1, так как все субъекты доступа выполняют разрешенные политикой безопасности виды доступа. Сетевые СОА выполняют обнаружение класса Б1 для сетевых информационных атак определением (идентификацией) управляющего воздействия субъекта-нарушителя на субъект-посредник. Для обнаружения чаще всего используются сигнатурные методы, которые могут определять только известные управляющие воздействия, но могут использоваться и методы поиска аномалий с предварительным обучением. Низкое качество используемых сигнатур, вызванное использованием упрощенных проверок, которые, в свою очередь, вызваны ограничением используемых ресурсов, а также несоответствия между работой информационной системы в обучающем и в нормальном режиме приводят к появлению большого количества ложных срабатываний.

*Класс Б*2. Мониторы обращений защищенных ОС узлов сети не будут противодействовать

классу Б2, так как работа в незащищенной СПД позволяет выполнять:

1) пассивный доступ к информации, который не контролируется монитором обращений;

2) подмену адреса отправителя, что позволяет для монитора обращений считать, что доступ был произведен с другого узла сети;

3) блокирование обмена информацией между узлами сети, что также не контролируется монитором обращений.

Сетевые СОА способны обнаруживать перечисленные действия 2 и 3. Однако при этом СОА должна получать все пакеты, проходящие по сети, что в большинстве случаев невозможно, поэтому сетевые СОА обнаруживают класс Б2 только на некоторых участках сети.

*Класс В*1. Монитор обращений ОС не будет противодействовать классу В1, если в правилах политики безопасности не будет явно запрещен доступ к объектам доступа, который может приводить к удалению, модификации записей или подмене журнала аудита. СОА могут обнаружить класс В1 для локальных информационных атак уже после реализации по анализу непротиворечивости записей журналов аудита. Такая возможность отсутствует в большинстве СОА, отсутствуют также и модели использования в СОА такого анализа.

*Класс В*2. Монитор обращений ОС не будет противодействовать классу В2, так как появление уязвимости позволит ее использовать в обход правил политики безопасности, по которым работает монитор обращений. Сетевые СОА не позволяют обнаруживать добавление уязвимости (этим занимаются специализированные средства анализа защищенности – сканеры безопасности), но позволяют определять сетевое использование типовых видов часто добавляемых уязвимостей.

*Класс В*3. Монитор обращений ОС не будет противодействовать классу В3, так как скрытые каналы передачи данных либо не нарушают политики безопасности, либо используют уровень передачи информации, который не подлежит проверке монитором обращений. Локальные СОА обычно не обнаруживают класс В3 для локальных информационных атак. Сетевые СОА позволяют обнаруживать класс В3 для сетевых информационных атак. Обычно используются методы поиска аномалий с предварительным обучением, но для упрощения проверка ограничена транспортным уровнем модели сетевого взаимодействия. Используемые модели приводят к большому количеству ложных срабатываний. Классические сетевые СОА обычно не обнаруживают скрытых каналов передачи данных на прикладном уровне модели сетевого взаимодействия.

Приведем возможности противодействия рассмотренным классам способов реализации фаз информационных атак со стороны монитора обращений защищенных ОС и локальных и сетевых СОА в виде таблицы, где строкам соответствуют:

1) монитор обращений ОС;

2) локальные СОА;

3) сетевые СОА.

Возможности противодействия способам реализации фаз информационных атак

	Фаза "А"			Фаза"Б"		Фаза "В"		
№	А1	А2	А3	Б1	Б2	В1	В2	В3
1	+	–	–	–	–	–	–	–
2	+	+	+	–	–	+	–	–
3	+	+	+	+	+	–	+	+

Таким образом, СОА позволяют противодействовать большему количеству способов реализации фаз информационной атаки, чем стандартные средства защищенных ОС. Однако СОА чаще всего оказывают административное противодействие, которое является неэффективным. Поэтому для качественного противодействия рассмотренным способам реализации фаз информационной атаки необходимо, во-первых, разработать модели политик безопасности, учитывающих эти классы, во-вторых, пересмотреть архитектуру классических СОА, в третьих, усовершенствовать математические модели, на базе которых они обнаруживают информационные атаки.

Библиографический список

1. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения [Электронный ресурс] / Гостехкомиссия России, 1992. – Режим доступа: http://www.fstec.ru/_docs/doc_3_3_002.htm, свободный – Загл. с экрана.

2. NCSC-TG-004 (Aqua Book) Glossary of Computer Security Terms [Электронный ресурс] / National Computer Security Center, 1988. – Режим доступа: http://www.fas.org/irp/nsa/rainbow/tg004.htm, свободный – Загл. с экрана.

3. *Сердюк В.А.* Вы атакованы – защищайтесь (методология обнаружения атак) // BYTE. – 2003. – № 9.

4. *F. Cuppens, S. Combault, T. Sans.* Selecting Appropriate Counter-Measures in an Intrusion Detection Framework. [Электронный ресурс] / Computer Security Foundations Workshop, 2004. – Режим доступа:

http://ieeexplore.ieee.org/iel5/9168/29101/01310733.pdf, платный – Загл. с экрана.

5. Intrusion Detection Is Dead. Long Live Intrusion Prevention! [Электронный ресурс] / SANS GIAC Certification Practical, 2003. – Режим доступа: http://www.securitydocs.com/go/1713, свободный – Загл. с экрана.