Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ),

http://www.re.mipt.ru/infsec

Сетевые средства управления доступом
Network Access Controls.

Кудрявцев Алексей Николаевич 114гр.

21.05.05 г.

Необходим четкий контроль подключений к системам, объединенным сетью, для того что бы другие подключенные пользователи не нарушали права сетевых сервисов.

Для этого используются сетевые средства управления доступом, которые должны включать в себя следующее:

- Межсетевые сервисные интерфейсы.
- Алгоритмы аутентификации удаленных пользователей , компьютерных систем и оборудования.
- Полный контроль доступа к информационным системам.

История развития

Некоторые возможности по управлению ресурсами появились только в windows for workgroups. Windows nt и os/2 обладают уже довольно развитыми средствами защиты сетевых ресурсов, включающими разграничение доступа на уровне ресурсов и уровне пользователей.

К примеру, в ОС IBM os/2 использовался IBM LAN Server, с помощью которого реализовывалось разграничение доступа к сетевым ресурсам на уровне пользователей, применяя для этого иерархическую модель организации пользователей в домены и группы.

Следующим шагом в развитии сетевых ОС стал сервер IBM Directory and Security Server for OS/2 warp (DSS), позволяющий реализовать распределенную вычислительную среду. Основой механизма разграничения доступа в DSS служит понятие области, способной объединять ресурсы всей организации, в отличие от доменов IBM LAN Server –а.

Основными компонентами DSS являются:

- Серверы службы каталогов.
- Серверы безопасности.
- Серверы службы времени.

Сервер безопасности, на основе которого и создавались все последующие сетевые средства управления доступом компонировал в себе следующее:

- Службу поддержки базы данных учетных записей (Registry Service).
- Службу аутентификации (Authentication Service).
- Службу разграничения доступа (Privilege Service).
- Службу поддержки списков управления доступом (ACL facility).
- Службу регистрации в сети (Login facility).

Давайте немного подробнее рассмотрим то, что включают в себя сетевые средства управления доступом.

Ограничение предоставленных услуг.

Интегральной характеристикой защищаемой системы является политика безопасности - качественное выражение свойств защищенности в терминах, представляющих систему. Наиболее часто рассматриваются политики безопасности, связанные с понятием «доступ».

Политика управления доступом, принятая в организации, представляет собой правила предоставления доступа к компьютерным системам и сети отдельным пользователям.

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами).

Иными словами, доступ- категория субъектно-объектной модели, описывающая процесс выполнения операций субъектов над объектами.

Политика безопасности включает:

- Множество возможных операций над объектами.
- Для каждой пары "субъект-объект" множество разрешенных операций, являющееся подмножеством всего множества возможных операций.

Отношение "субъекты-объекты" можно представлять в виде:

- матрицы доступа.
- списков доступа.
- ролевого управления доступом.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек, таких как restricted shell в ОС Unix.

Аутентификация пользователей

Одной из важнейших задач системы защиты информации в сетях является установление подлинности пользователей работающих в ней для обеспечения им соответствующих привилегий доступа. Для этого используется аутентификация подключений, осуществляемых удаленными пользователями через общедоступные (или не принадлежащие организации) сети.

Аутентификация может выполняться на уровне компьютера, поддерживающего приложение, или на сетевом уровне. Для определения необходимого уровня аутентификации требуется оценка рисков согласно политике безопасности организации. К примеру, для реализации защиты класса 3 (фрагментарная защита) Вероятность ложной аутентификации не должна превосходить 10^{-6} на попытку доступа, а также система должна фиксировать в регистрационном протоколе все попытки ложной аутентификации (для механизма парольного доступа - все попытки входа с неверно набранным паролем).

Несанкционированный доступ к производственному приложению может быть осуществлен посредством автоматического подключения удаленного компьютера, поэтому необходимо аутентифицировать подключения удаленных компьютерных систем. Этот процесс бывает двусторонним (взаимным), поскольку для безопасной работы в беспроводных сетях необходима и аутентификация узла доступа. В стандарте IEEE 802.11b предусматриваются аутентификация сетевого устройства по ее MAC-адресу и аутентификация сети по ее названию.

Так как в большинстве случаев аутентификация происходит в распределенных системах и связана с передачей по сети информации о параметрах учетных записей пользователей, то естественно эту передаваемую по сети в процессе аутентификации информацию необходимо защищать, иначе возникает угроза ее перехвата и использования для нарушения безопасности. В беспроводных сетях эта задача осложняется тем, что до успешного ее завершения исключается передача потребителю ключей шифрования, а открытый трафик радиообмена легко прослушать с помощью любого устройства, работающего в том же стандарте. Как на сетевом уровне, так и на уровне компьютера аутентификацию удаленных пользователей можно осуществлять с помощью, например, систем оперативного реагирования на проблемы и шифрования линии связи. Использование выделенных частных линий связи или средства проверки сетевых адресов пользователей также дает уверенность в источнике подключений.

Защита удаленного диагностического порта

Порты для диагностики удаленного подключения, используемые специалистами по техническому обслуживанию можно использовать для несанкционированного доступа. Поэтому их следует защитить с помощью надлежащих механизмов безопасности, например, посредством блокировки с ключом, и процедуры, которая гарантирует, что эти порты становятся доступными только после получения санкции от администратора компьютерной системы на доступ специалистов по техническому обслуживанию программно-аппаратного обеспечения.

Сегментация сетей

Сети различных организаций растут с ростом самих организаций, а также с увеличением числа деловых партнеров этих организаций

появляются необходимости объединения сетевых сервисов, что также приводит к расширению границ организации.Такое расширение границ может увеличить риск несанкционированного доступа к функционирующим компьютерным системам, подключенным к сети, некоторые из которых могут потребовать защиты от других пользователей сети вследствие их уязвимости или важности для организации. В таких случаях можно использовать одно из средств управления безопасностью крупных сетей, заключающееся в их разбиении на несколько логических сегментов согласно политике управления доступом, каждый из которых защищен межсетевым экраном в пределах заданного периметра безопасности. Тогда доступ к сегментам сети можно контролировать с помощью шлюзов безопасности, привлекая надлежащие средства контроля маршрута и подключения .

Главными преимуществами сегментации сети являются изоляция уязвимых мест, мониторинг сети и предотвращение вторжений в нее, сканирование сети и обнаружение в ней неисправностей, автоматическое устранение нарушений и укрепление стратегии защиты сети, а также то что каждый сегмент сети может иметь свою собственную политику безопасности и администраторов безопасности. Среди этих функций наибольшее впечатление производит возможность изоляции сегментов сети. Это позволяет компаниям разбивать свои сети на сегменты и реагировать на вторжения раньше, чем вирус поразит всю сеть

Контроль сетевых подключений

В соответствие с требованиями политики управления доступом может потребоваться реализация средств контроля для ограничения возможности сетевых подключений. Такой контроль может быть осуществлен посредством межсетевых шлюзов, которые фильтруют передаваемые по сети данные с помощью предопределенных таблиц и правил, а также с помощью персональных пользовательских брандмауэров, фильтрующих трафик защищаемого компьютера, что, в свою очередь, подразумевает контроль за сетевыми подключениями к пользовательской системе, а также следящих за сетевой активностью системных сервисов и прикладных программ, за содержимым веб- и почтового трафика, поступающим на компьютер.

Примерами таких ограничений являются:

- пересылка только электронной почты;
- односторонняя передача файлов;
- двухсторонняя передача файлов;
- интерактивный доступ;
- доступ к сети только в определенное время суток или в определенную дату.

Управление сетевой маршрутизацией

Привлечение средств контроля маршрутизации для подключения компьютерных систем, основанные на механизмах проверки адреса источника данных и назначения, используется для того, что бы информационные потоки не нарушали политику управления доступом к производственным приложениям.

Такие средства можно реализовать на программном или аппаратном уровне. Межсетевой протокол (Internet Protocol) (IP) разработан как раз с целью управления сетевой маршрутизацией.

Принудительная маршрутизация

В современных сетях есть огромный риск несанкционированного доступа или незаконного использования информационных систем из-за обширных возможностей коллективных использований различного рода ресурсов и увеличенной эластичности маршрутизации. Такой риск можно уменьшить, простым привлечением средств контроля для ограничения маршрута между пользовательским терминалом и компьютерными системами, доступ к которым пользователю разрешен, т.е. создавая и четко контролируя принудительный маршрут.

Основная функция создания принудительного маршрута — всячески предотвратить несанкционированное отклонение пользователей от маршрута между используемыми им терминалами и доступными(с разрешенным доступом) для пользователя системами. Для этого обычно требуется реализация ряда средств контроля в нескольких точках пути. Принцип состоит в том, чтобы ограничить возможности выбора маршрута в каждой точке сети посредством предопределенных вариантов.

Примерами такого ограничения пути являются:

- предоставление выделенных линий связи или телефонных номеров;
- автоматическое подключение портов к определенным прикладным системам или шлюзам безопасности;
- ограничение возможностей выбора маршрута с помощью системы меню и подменю для отдельных пользователей;
- предотвращение неограниченного блуждания по сети.

В основе требований к принудительной маршрутизации должна лежать политика управления доступом, принятая в организации .

Использование сетевых сервисов

Существует целый ряд общедоступных и коммерческих сетевых сервисов. Сетевой сервис современных вычислительных сетей уже не ограничивается обеспечением взаимодействия между подключенными к

ним компьютерами. Такие технологии, как виртуальные вычислительные сети, фильтрация пакетов, частные виртуальные вычислительные сети, аутентификация и авторизация пользователей при подключении к сети являются средствами ослабления угроз безопасности не только самой сети, но и подключенных к ней компьютеров и хранящейся и обрабатываемой на них информации. Сетевые сервисы могут иметь уникальные защитные характеристики. Организации, пользующиеся сетевыми сервисами, должны потребовать от своих поставщиков сетевых услуг четкого описания атрибутов безопасности всех используемых сервисов и определить последствия от нарушения режима безопасности для конфиденциальности, целостности, и доступности.

Основная литература

«Основы информационной безопасности»
Галатенко В.А.

Продукты для защиты информации
http://www.in4business.ru

Управление информационной безопасностью
Практические правила
http://itc.bratsk-city.ru/index.php?id=op8

«Защита программ и данных» 2000г.
П.Ю. Белкин, О.О. Михальский и др.

«К вопросу о разработке требований к защите от несанкционированного доступа конфиденциальной информации.»
М.Р. Биктимиров, В.В. Засыпкина, А.Ю. Щербаков.

КЛЮЧИ ШИФРОВАНИЯ
"Art Communications Ltd." Роман Павлов