12. Лекция: Экранирование, анализ защищенности

Экранирование

Основные понятия

Формальная постановка задачи *экранирования*, состоит в следующем. Пусть имеется два множества информационных систем. ***Экран*** – это средство *разграничения доступа* клиентов из одного множества к серверам из другого множества. *Экран* осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем (рис. 12.1). Контроль потоков состоит в их *фильтрации*, возможно, с выполнением некоторых преобразований.

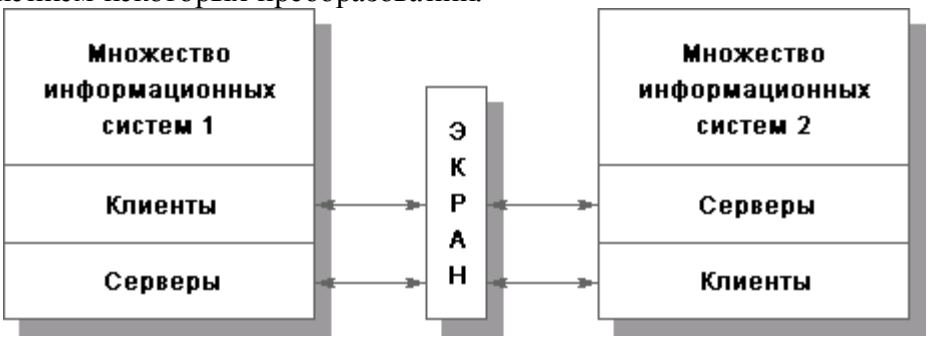

Рис. 12.1. Экран как средство разграничения доступа.

На следующем уровне детализации *экран* (полупроницаемую мембрану) удобно представлять как последовательность *фильтров*. Каждый из *фильтров*, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за *экран*. Кроме того, допускается преобразование данных, передача порции данных на следующий *фильтр* для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю (рис. 12.2).

Рис. 12.2. Экран как последовательность фильтров.

Помимо функций *разграничения доступа*, *экраны* осуществляют *протоколирование* обмена информацией.

Обычно *экран* не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача *экранирования* формулируется как защита внутренней области от потенциально враждебной внешней. Так, *межсетевые экраны (МЭ)* (предложенный автором перевод английского термина firewall) чаще всего устанавливают для защиты корпоративной сети организации, имеющей выход в Internet (см. следующий раздел).

Экранирование помогает поддерживать *доступность* сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью.

Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть *экран*, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима *конфиденциальности* в ИС организации.

Подчеркнем, что *экранирование* может использоваться как сервис безопасности не только в сетевой, но и в любой другой среде, где происходит обмен сообщениями. Важнейший пример подобной среды – объектно-ориентированные программные системы, когда для активизации методов объектов выполняется (по крайней мере, в концептуальном плане) передача сообщений. Весьма вероятно, что в будущих объектно-ориентированных средах *экранирование* станет одним из важнейших инструментов *разграничения доступа* к объектам.

Экранирование может быть частичным, защищающим определенные информационные сервисы. *Экранирование* электронной почты описано в статье "Контроль над корпоративной электронной почтой: система "Дозор-Джет"" (Jet Info, 2002, 5).

Ограничивающий интерфейс также можно рассматривать как разновидность *экранирования*. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть. Можно провести аналогию между динамически формируемыми гипертекстовыми документами и представлениями в реляционных базах данных, с той существенной оговоркой, что в случае Web возможности существенно шире.

Экранирующая роль *Web-сервиса* наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, например таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация данных.

Архитектурные аспекты

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС – это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.). Единственный перспективный путь связан с разработкой специализированных сервисов безопасности, которые в силу своей простоты допускают формальную или неформальную верификацию. *Межсетевой экран* как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем *МЭ*, во втором – о внутреннем. В зависимости от точки зрения, внешний *межсетевой экран* можно считать первой или последней (но никак не единственной) линией обороны. Первой – если смотреть на мир глазами внешнего злоумышленника. Последней – если стремиться к защищенности всех компонентов корпоративной сети и пресечению неправомерных действий внутренних пользователей.

Межсетевой экран – идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, *МЭ* способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на *доступность*.

На *межсетевой экран* целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

В силу принципов **эшелонированности обороны** для защиты внешних подключений обычно используется двухкомпонентное *экранирование* (см. рис. 12.3). Первичная *фильтрация* (например, блокирование пакетов управляющего протокола SNMP, опасного атаками на доступность, или пакетов с определенными IP-адресами, включенными в "черный список") осуществляется **граничным маршрутизатором** (см. также следующий раздел), за которым располагается так называемая **демилитаризованная зона** (сеть с умеренным доверием безопасности, куда выносятся внешние информационные сервисы организации – Web, электронная почта и т.п.) и основной *МЭ*, защищающий внутреннюю часть корпоративной сети.

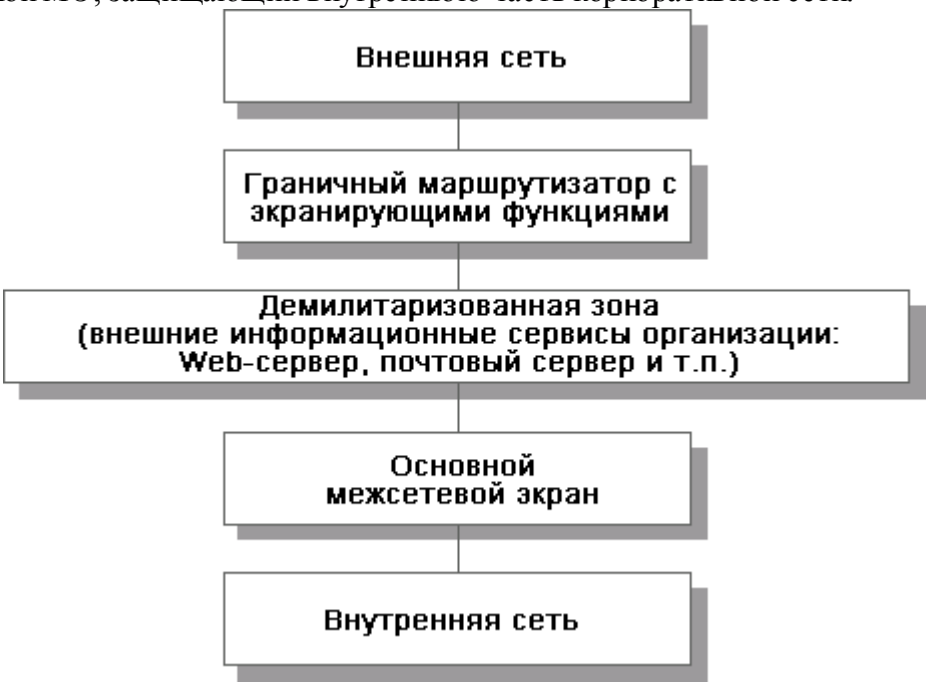

Рис. 12.3. Двухкомпонентное экранирование с демилитаризованной зоной.

Теоретически *межсетевой экран* (особенно внутренний) **должен быть многопротокольным**, однако на практике доминирование семейства протоколов TCP/IP столь велико, что поддержка других протоколов представляется излишеством, вредным для безопасности (чем сложнее сервис, тем он более уязвим).

Вообще говоря, и внешний, и внутренний *межсетевой экран* может стать узким местом, поскольку объем сетевого трафика имеет тенденцию быстрого роста. Один из подходов к решению этой проблемы предполагает разбиение *МЭ* на несколько аппаратных частей и организацию специализированных **серверов-посредников**. Основной *межсетевой экран* может проводить грубую классификацию входящего трафика по видам и передоверять *фильтрацию* соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Исходящий трафик сначала обрабатывается сервером-посредником, который может выполнять и функционально полезные действия, такие как кэширование страниц внешних *Web-серверов*, что снижает нагрузку на сеть вообще и основной *МЭ* в частности.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к Internet. В этом случае каждое подключение должно защищаться своим *экраном*. Точнее говоря, можно считать, что корпоративный внешний *межсетевой экран* является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Противоположностью составным корпоративным *МЭ* (или их компонентами) являются персональные *межсетевые экраны* и **персональные экранирующие устройства**. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

При развертывании *межсетевых экранов* следует соблюдать рассмотренные нами ранее принципы **архитектурной безопасности**, в первую очередь позаботившись о **простоте** и **управляемости**, об эшелонированности обороны, а также о **невозможности перехода в небезопасное состояние**. Кроме того, следует принимать во внимание не только **внешние**, но и **внутренние угрозы**.

Классификация межсетевых экранов

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. *Межсетевые экраны* также целесообразно классифицировать по уровню *фильтрации* – канальному, сетевому, транспортному или прикладному. Соответственно, можно говорить об **экранирующих концентраторах** (мостах, коммутаторах) (уровень 2), **маршрутизаторах** (уровень 3), о транспортном *экранировании* (уровень 4) и о прикладных *экранах* (уровень 7). Существуют также комплексные *экраны*, анализирующие информацию на нескольких уровнях.

Фильтрация информационных потоков осуществляется *межсетевыми экранами* на основе **набора правил**, являющихся выражением сетевых аспектов политики безопасности организации. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения, например, текущее время, количество активных соединений, **порт**, через который поступил сетевой запрос, и т.д. Таким образом, в *межсетевых экранах* используется очень мощный логический подход к *разграничению доступа*.

Возможности *межсетевого экрана* непосредственно определяются тем, какая информация может использоваться в правилах *фильтрации* и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует *МЭ*, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее он может быть сконфигурирован.

Экранирующие маршрутизаторы (и концентраторы) имеют дело с отдельными пакетами данных, поэтому иногда их называют **пакетными фильтрами**. Решения о том, пропустить или задержать данные, принимаются для каждого пакета независимо, на основании анализа адресов и других полей заголовков сетевого (канального) и, быть может, транспортного уровней. Еще один важный компонент анализируемой информации – порт, через который поступил пакет.

Экранирующие концентраторы являются средством не столько *разграничения доступа*, сколько оптимизации работы локальной сети за счет организации так называемых виртуальных локальных сетей. Последние можно считать важным результатом применения внутреннего межсетевого *экранирования*.

Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и **фильтровать пакеты как на входе, так и на выходе**. В принципе, в качестве пакетного фильтра может использоваться и универсальный компьютер, снабженный несколькими сетевыми картами.

Основные достоинства экранирующих маршрутизаторов – доступная цена (на границе сетей маршрутизатор нужен практически всегда, вопрос лишь в том, как задействовать его экранирующие возможности) и **прозрачность** для более высоких уровней модели OSI. Основной недостаток – ограниченность анализируемой информации и, как следствие, относительная слабость обеспечиваемой защиты.

Транспортное *экранирование* позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним. С точки зрения реализации экранирующий транспорт представляет собой довольно простую, а значит, надежную программу.

По сравнению с пакетными фильтрами, транспортное *экранирование* обладает большей информацией, поэтому соответствующий *МЭ* может осуществлять более тонкий контроль за виртуальными соединениями (например, он способен отслеживать количество передаваемой информации и разрывать соединения после превышения определенного порога, препятствуя тем самым несанкционированному экспорту информации). Аналогично, возможно накопление более содержательной регистрационной информации. Главный недостаток – сужение области применения, поскольку вне контроля остаются датаграммные протоколы. Обычно транспортное *экранирование* применяют в сочетании с другими подходами, как важный дополнительный элемент.

Межсетевой экран, функционирующий на прикладном уровне, способен обеспечить наиболее надежную защиту. Как правило, подобный *МЭ* представляет собой универсальный компьютер, на котором функционируют **экранирующие агенты**, интерпретирующие протоколы прикладного уровня (HTTP, FTP, SMTP, telnet и т.д.) в той степени, которая необходима для обеспечения безопасности.

При использовании прикладных *МЭ*, помимо *фильтрации*, реализуется еще один важнейший аспект *экранирования*. Субъекты из внешней сети видят только шлюзовой компьютер; соответственно, им доступна только та информация о внутренней сети, которую он считает нужным экспортировать. Прикладной *МЭ* на самом деле экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира. В то же время, субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира. Недостаток прикладных *МЭ* – отсутствие полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Если организация располагает исходными текстами прикладного *МЭ* и в состоянии эти тексты модифицировать, перед ней открываются чрезвычайно широкие возможности по настройке *экрана* с учетом собственных нужд. Дело в том, что при разработке систем **клиент/сервер в многозвенной архитектуре** появляются специфические прикладные протоколы, нуждающиеся в защите не меньше стандартных. Подход, основанный на использовании экранирующих агентов, позволяет построить такую защиту, не снижая безопасности и эффективности других приложений и не усложняя структуру связей в *межсетевом экране*.

Комплексные *межсетевые экраны*, охватывающие уровни от сетевого до прикладного, соединяют в себе лучшие свойства "одноуровневых" *МЭ* разных видов. Защитные функции выполняются комплексными *МЭ* прозрачным для приложений образом, не требуя внесения каких-либо изменений ни в существующее программное обеспечение, ни в действия, ставшие для пользователей привычными.

Комплексность *МЭ* может достигаться разными способами: "снизу вверх", от сетевого уровня через накопление контекста к прикладному уровню, или "сверху вниз", посредством дополнения прикладного *МЭ* механизмами транспортного и сетевого уровней.

Помимо выразительных возможностей и допустимого количества правил, качество *межсетевого экрана* определяется еще двумя очень важными характеристиками – **простотой использования** и **собственной защищенностью**. В плане простоты использования первостепенное значение имеют наглядный интерфейс при определении

правил *фильтрации* и возможность **централизованного администрирования** составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил *фильтрации* и **проверки набора правил на непротиворечивость**. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность *межсетевого экрана* обеспечивается теми же средствами, что и защищенность универсальных систем. Имеется в виду физическая защита, идентификация и аутентификация, *разграничение доступа*, контроль целостности, протоколирование и аудит. При выполнении централизованного администрирования следует также позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и *конфиденциальность*. Крайне важно оперативное наложение заплат, ликвидирующих выявленные уязвимые места *МЭ*.

Хотелось бы подчеркнуть, что природа *экранирования* как сервиса безопасности очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, *межсетевой экран* может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Мощным методом сокрытия информации является **трансляция** "внутренних" сетевых **адресов**, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Отметим также следующие дополнительные возможности *межсетевых экранов*:

- контроль информационного наполнения (антивирусный **контроль "на лету"**, верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т.п.);
- выполнение функций **ПО промежуточного слоя**.

Особенно важным представляется последний из перечисленных аспектов. ПО промежуточного слоя, как и традиционные *межсетевые экраны* прикладного уровня, скрывает информацию о предоставляемых услугах. За счет этого оно может выполнять такие функции, как **маршрутизация запросов** и **балансировка нагрузки**. Представляется вполне естественным, чтобы эти возможности были реализованы в рамках *межсетевого экрана*. Это существенно упрощает действия по обеспечению высокой *доступности* экспортируемых сервисов и позволяет осуществлять переключение на резервные мощности прозрачным для внешних пользователей образом. В результате к услугам, традиционно предоставляемым *межсетевыми экранами*, добавляется поддержка высокой *доступности* сетевых сервисов.

Пример современного *межсетевого экрана* представлен в статье "Z-2 – универсальный *межсетевой экран* высшего уровня защиты" (Jet Info, 2002, 5).

Анализ защищенности

Сервис **анализа защищенности** предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Системы анализа защищенности (называемые также **сканерами защищенности**), как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять.

Соответственно, ядром таких систем является **база уязвимых мест**, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

В принципе, могут выявляться бреши самой разной природы: наличие вредоносного ПО (в частности, вирусов), слабые пароли пользователей, неудачно сконфигурированные операционные системы, небезопасные сетевые сервисы, неустановленные заплаты, уязвимости в приложениях и т.д. Однако наиболее эффективными являются **сетевые сканеры** (очевидно, в силу доминирования семейства протоколов TCP/IP), а также антивирусные средства. **Антивирусную защиту** мы причисляем к средствам анализа защищенности, не считая ее отдельным сервисом безопасности.

Сканеры могут выявлять уязвимые места как путем пассивного анализа, то есть изучения конфигурационных файлов, задействованных портов и т.п., так и путем имитации действий атакующего. Некоторые найденные уязвимые места могут устраняться автоматически (например, лечение зараженных файлов), о других сообщается администратору.

Системы анализа защищенности снабжены традиционным "технологическим сахаром": **автообнаружением** компонентов анализируемой ИС и графическим интерфейсом (помогающим, в частности, эффективно работать с протоколом сканирования).

С возможностями свободно распространяемого сканера Nessus можно ознакомиться, прочитав статью "Сканер защищенности Nessus: уникальное предложение на российском рынке" (Jet Info, 2000, 10).

Контроль, обеспечиваемый системами анализа защищенности, носит реактивный, запаздывающий характер, он не защищает от новых атак, однако следует помнить, что оборона должна быть эшелонированной, и в качестве одного из рубежей контроль защищенности вполне адекватен. Отметим также, что подавляющее большинство атак носит рутинный характер; они возможны только потому, что известные бреши в защите годами остаются неустраненными.