Тема 3.1. Особенности обеспечения информационной безопасности в компьютерных сетях

1 Особенности информационной безопасности в компьютерных сетях

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем – распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматрива-

ются два подвида удаленных угроз – это удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых протоколах и инфраструктуре сети, а вторые – уязвимости в телекоммуникационных службах.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих «информационной безопасности»: целостности данных; конфиденциальности данных; доступности данных.

Целостность данных – одна из основных целей информационной безопасности сетей – предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных – вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.

Доступность данных – третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение информационной безопасности как раз и связана с невозможностью реализации этих функций. В локальной сети должны быть доступны: принтеры, серверы, рабочие станции, данные пользователей и др. В глобальных вычислительных сетях должны быть доступны информационные ресурсы и различные сервисы, например, почтовый сервер, сервер доменных имен, web-сервер и др.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

– глобальную связанность;

– разнородность корпоративных информационных систем;

– распространение технологии «клиент/сервер».

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на международном уровне. Национальные границы, законы, стандарты не должны препятствовать защите потоков данных между клиентами и серверами. Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.

Корпоративные информационные системы оказываются разнородными еще в одном важном отношении – в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности. Использования технологии «клиент/сервер» с точки зрения информационной безопасности имеет следующие особенности:

– каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
– каждый сервис имеет свою трактовку понятий субъекта и объекта;
– каждый сервис имеет специфические угрозы;
– каждый сервис нужно по-своему администрировать;
– средства безопасности в каждый сервис нужно встраивать по-особому.

2 Специфика средств защиты в компьютерных сетях

Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;
- защита важнейших сервисов (в первую очередь – Web-сервиса);
- аутентификация в открытых сетях.

Вопросы реализации таких методов защиты будут рассмотрены далее.

И в заключение рассмотрим еще одну особенность информационной безопасности, связанную с вычислительными сетями. В последнее время все четче просматривается незащищенность вычислительных сетей от глобальных атак.

Исторически первой глобальной атакой на компьютерные сети считается распространение вируса Морриса (4 ноября 1988) в сети «Arpanet», когда примерно из 60 000 компьютеров в сети было заражено около 10% (примерно 6 000). Неконтролируемый процесс распространения вируса привел к блокировке сети.

За последние два года как минимум успешными были три глобальные атаки:

1) 21 октября 2017. Сеть «Internet». Запланированная DoS-атака на Интернет. В момент атаки нагрузка на Европейский сегмент Интернета возросла на 6%.

2) 25 января 2018. Сеть «Internet». Флеш-червь «SQL. Slammer». Неконтролируемый процесс распространения вируса привел к перегрузке каналов передачи данных в Ю. Корее. Нагрузка на Европейский сегмент Интернета возросла примерно на 25%.

3) 12 августа 2019. Сеть «Internet». Сетевой червь «Lovesan».

Успешные глобальные сетевые атаки, безусловно, являются самым разрушительным явлением, которое может произойти в современных сетях.

3 Выводы по теме 3.1

1) Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно – при помощи механизма сообщений.

2) Все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

3) Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

4) Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих информационной безопасности.

5) Особенности вычислительных сетей и, в первую очередь, глобальных, предопределяет необходимость использования специфических методов и средств защиты, таких как аутентификация в открытых сетях, защита подключений к внешним сетям, защита потоков данных между клиентами и серверами и др.

Тема 3.2. Сетевые модели передачи данных

1 Понятие протокола передачи данных

Обмен информацией между ЭВМ на больших расстояниях всегда казался более важной задачей, чем локальный обмен. Поэтому ему уделялось больше внимания и, соответственно, велось большее финансирование во многих странах. Один из немногих открытых проектов по исследованию вычислительных сетей, финансировавшийся военным ведомством США, известен под названием сеть ARPA – Advanced Research Projects Agency. С самого начала в рамках этого проекта велись работы по объединению ресурсов многих вычислительных машин различного типа. В 1960-1970-е годы многие результаты, полученные при эксплуатации сети ARPA, были опубликованы в открытой печати. Это обстоятельство, а также тот факт, что почти все страны занялись практически слепым копированием не только аппаратной архитектуры американских машин, но и базового программного обеспечения, обусловили сильное влияние сети ARPA на многие другие сети, именно поэтому принято считать, что сеть ARPA является предшественницей знаменитой всемирной компьютерной сети Интернет.

Основной задачей сетевой общественности явилась разработка протоколов обмена информацией. Эта задача совершенно справедливо представлялась важнейшей, поскольку настоятельно требовалось заставить понимать друг друга компьютеры, обладавшие различной архитектурой и программным обеспечением. Первоначально разработчики многочисленных корпоративных сетей договаривались о внутренних протоколах информационного обмена в своих сетях. Никакой стандартизации не было. Но уже в 70-е годы специалистам стало совершенно ясно, что стандартизация необходима и неизбежна. В эти годы шел бурный процесс создания многочисленных национальных и международных комитетов и комиссий по стандартизации программных и аппаратных средств в области вычислительной техники и информационного обмена.

В общем случае протокол сетевого обмена информацией можно определить, как перечень форматов передаваемых блоков данных, а также правил их обработки и со-

ответствующих действий. Другими словами, протокол обмена данными – это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных.

Человек – оператор компьютера, включенного в сеть, тем или иным способом, например, с помощью программ-приложений, формирует и передает по сети сообщения, предназначенные для других людей или компьютеров. В ответ он также ожидает поступления сообщения. В этом смысле сообщение представляет собой логически законченную порцию информации, предназначенную для потребления конечными пользователями – человеком или прикладной программой. Например, это может быть набор алфавитно-цифровой и графической информации на экране или файл целиком. Сейчас сообщения неразрывно связывают с прикладным уровнем или, как его еще называют, уровнем приложений сетевых протоколов.

Сообщения могут проходить довольно сложный путь по сетям, стоять в очередях на передачу или обработку, в том числе, не доходить до адресата, о чем отправитель также должен быть уведомлен специальным сообщением.

Первоначально вычислительные сети были сетями коммутации сообщений. Это было оправдано, пока сообщения были сравнительно короткими. Но параллельно с этим всегда существовали задачи передачи на расстояние больших массивов информации. Решение этой задачи в сетях с коммутацией сообщений является неэффективным, поскольку длины сообщений имеют большой разброс – от очень коротких до очень длинных, что характерно для компьютерных сетей.

В связи с этим было предложено разбивать длинные сообщения на части – пакеты и передавать сообщения не целиком, а пакетами, вставляя в промежутках пакеты других сообщений. На месте назначения сообщения собираются из пакетов. Короткие сообщения при этом были вырожденным случаем пакета, равного сообщению.

В настоящее время почти все сети в мире являются сетями коммутации пакетов. Но способов обмена пакетами тоже может быть множество. Это связано со стратегией подтверждения правильности передачи.

2 Принципы организации обмена данными в вычислительных сетях

Существуют два принципа организации обмена данными:

1) Установление виртуального соединения с подтверждением приема каждого пакета.

2) Передача датаграмм.

1) Установление виртуального соединения или создание виртуального канала является более надежным способом обмена информацией. Поэтому он более предпочтителен при передаче данных на большие расстояния и (или) по физическим каналам, в которых возможны помехи. При виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Если какой-то пакет принят неправильно, отправитель повторяет его передачу. Так длится до тех пор, пока все сообщение не будет успешно передано. На время передачи информации между двумя пунктами коммутируется канал, подобный каналу при телефонном разговоре. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

2) Термин датаграмма образован по аналогии с термином телеграмма. Аналогия заключается том, что короткие пакеты – собственно датаграммы – пересылаются адресату без подтверждения получения каждой из них. О получении всего сообщения целиком должна уведомить целевая программа.

3 Транспортный протокол TCP и модель TCP/IP

За время развития вычислительных сетей было предложено и реализовано много протоколов обмена данными, самыми удачными из которых явились семейство протоколов TCP/IP (Transmission Control Protocol/Internet Protocol – протокол управления передачей/межсетевой протокол).

TCP/IP – это набор протоколов, состоящий из следующих компонентов:

– межсетевой протокол (Internet Protocol), обеспечивающий адресацию в сетях (IP-адресацию);

– межсетевой протокол управления сообщениями (Internet Control Message Protocol – ICMP), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т. п.;

– протокол разрешения адресов (Address Resolution Protocol – ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);

– протокол пользовательских датаграмм (User Datagramm Protocol – UDP);

– протокол управления передачей (Transmission Control Protocol – TCP).

Протокол UDP обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и соответственно подтверждения доставки пакета с повтором в случае ошибки.

Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название – TCP/IP. Модель TCP/IP иерархическая и включает четыре уровня (Таблица 3.2.1).

Прикладной уровень определяет способ общения пользовательских приложений. В системах «клиент-сервер» приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.

Транспортный уровень позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.

На сетевом уровне определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.

На канальном уровне определяется адресация физических интерфейсов сетевых устройств, например, сетевых плат. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые, драйверы.

Таблица 3.2.1 – Модель сетевого обмена данными

Уровень	Название	Функция
4	Прикладной	Приложения пользователей, создание сообщений
3	Транспортный	Доставка данных между программами в сети
2	Сетевой	Адресация и маршрутизация
1	Канальный	Сетевые аппаратные средства и их драйверы

Как уже отмечалось ранее, в сетях с коммутацией пакетов, а модель TCP/IP относится к таким, для передачи по сети сообщение (сформированное на прикладном уровне) разбивается на пакеты или датаграммы. Пакет или датаграмма – это часть сообщения с добавленным заголовком пакета или датаграммы.

На транспортном уровне к полезной информации добавляется заголовок – служебная информация. Для сетевого уровня полезной информацией является уже пакет или датаграмма транспортного уровня. К ним добавляется заголовок сетевого уровня.

Полученный блок данных называется IP-пакетом. Полезной нагрузкой для канального уровня является уже IP-пакет. Здесь перед передачей по каналу к нему добавляются собственный заголовок и еще завершитель. Получившийся блок называется кадром. Он и передается по сети.

Переданный по сети кадр в пункте назначения преобразуется в обратном порядке, проходя по уровням модели снизу-вверх.

4 Выводы по теме 3.2

1) Протокол сетевого обмена информацией – это перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий.

2) Протокол обмена данными – это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных.

3) В настоящее время почти все сети в мире являются сетями коммутации пакетов.

4) Существуют два принципа организации обмена данными: установление виртуального соединения с подтверждением приема каждого пакета и передача датаграмм.

5) При виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

6) При передаче датаграммы короткие пакеты пересылаются адресату без подтверждения получения каждой из них, а о получении всего сообщения целиком должна уведомить целевая программа.

7) TCP/IP – это набор протоколов, состоящий из следующих компонентов: межсетевой протокол (IP), межсетевой протокол управления сообщениями (ICMP), протокол разрешения адресов (ARP), протокол пользовательских датаграмм (UDP) и протокол управления передачей (TCP).

Тема 3.3. Модель взаимодействия открытых систем OSI/ISO

1 Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO

В конце 80-х годов наблюдался подлинный бум, вызванный разработкой Международной организации по стандартизации коммуникационных протоколов – (International Standard Organization). Разработанная ISO спецификация, названная моделью взаимодействия открытых систем (OSI – Open Systems Interconnection), заполонила научные публикации. Казалось, что эта модель займет первое место и оттеснит широко распространившийся TCP/IP. Но этого не произошло. Одной из причин этого явилась тщательная проработка протоколов TCP/IP, их функциональность и открытость к наращиванию функциональных возможностей, хотя к настоящему времени достаточно очевидно, что они имеют и множество недостатков.

Таблица 3.3.1 – Сравнительная схема уровневых моделей протоколов OSI и TCP/IP

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, то есть в данном случае необходимо организовать согласованную работу двух «иерархий», работающих на разных компьютерах. Оба участника сетевого обмена должны принять множество соглашений. Например, они должны согласовать уровни и форму электрических сигналов, способ определения длины сообщений, договориться о методах контроля достоверности и т. п. Другими словами, соглашения

должны быть приняты для всех уровней, начиная от самого низкого – уровня передачи битов – до самого высокого, реализующего сервис для пользователей сети.

2 Характеристика уровней модели OSI/ISO

Модель взаимодействия открытых систем (Open System Interconnection, OSI) определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

Модель OSI была разработана на основании большого опыта, полученного при создании компьютерных сетей, в основном глобальных, в 70-е годы.

В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

1) Физический уровень имеет дело с передачей битов по физическим каналам связи, таким, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие.

Одной из задач канального уровня является проверка доступности среды передачи. Другая задача канального уровня – реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра.

2) Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей. Внутри одной сети доставка данных обеспечивается канальным уровнем, а вот доставкой данных между различными сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения

даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня.

3) Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Маршрутизатор – это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями.

4) Транспортный уровень обеспечивает приложениям или верхним уровням стека – прикладному и сеансовому – передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное – способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

5) Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

6) Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы

прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например, в кодах ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

7) Прикладной уровень – это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Три верхних уровня – прикладной, представительный и сеансовый - ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

Таблица 3.3.2 – Распределение функций безопасности

Функции безопасности	**Уровень OSI**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединения	-	+	+	+	-	+	+
Избирательная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

«+» – данный уровень может предоставить функцию безопасности;

«-» – данный уровень не подходит для предоставления функции безопасности.

Столь подробное рассмотрение модели OSI/ISO связано с тем, что при разработке стандартов и спецификации по сетевой безопасности специалисты ориентируются на эту перспективную модель. Так в «Общих критериях» приводится распределение функций безопасности по уровням эталонной семиуровневой модели OSI.

3 Выводы по теме 3.3

1) Модель взаимодействия открытых систем (Open System Interconnection, OSI) определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

2) Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, то есть в данном случае необходимо организовать согласованную работу двух «иерархий», работающих на разных компьютерах.

3) В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

4) Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

5) Три нижних уровня – физический, канальный и сетевой – являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

6) Три верхних уровня – прикладной, представительный и сеансовый – ориентированы на приложения и мало зависят от технических особенностей построения сети.

7) Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних.

Тема 3.4. Адресация в глобальных сетях

3.4.1. Введение

1 Основы IP-протокола

Одной из главных проблем построения глобальных сетей является проблема адресации. С одной стороны, постоянное расширение глобальной сети Интернет привело к нехватке уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в таких сетях должна быть защищена от возможного вмешательства злоумышленников, связанных с подменой адресов и реализацией обходных маршрутов передачи сообщений.

Адресация современного Интернета основана на протоколе IP (Internet Protocol), история которого неразрывно связана с транспортным протоколом TCP.

Концепция протокола IP представляет сеть как множество компьютеров (хостов), подключенных к некоторой интерсети. Интерсеть, в свою очередь, рассматривается как совокупность физических сетей, связанных маршрутизаторами. Физические объекты (хосты, маршрутизаторы, подсети) идентифицируются при помощи специальных IP-адресов. Каждый IP-адрес представляет собой 32-битовый идентификатор. Принято записывать IP-адреса в виде 4-х десятичных чисел, разделенных точками.

Для этого 32-х битовый IP-адрес разбивается на четыре группы по 8 бит (1 байт), после чего каждый байт двоичного слова преобразовывается в десятичное число по известным правилам. Например, IP-адрес:

10010011	10000111	00001110	11100101

преобразовывается указанным способом к следующему виду:
147.135.14.229.

2 Классы адресов вычислительных сетей

Каждый адрес является совокупностью двух идентификаторов: сети – NetID, и хоста – HostID. Все возможные адреса разделены на 5 классов, схема которых приведена на рисунке 3.4.1

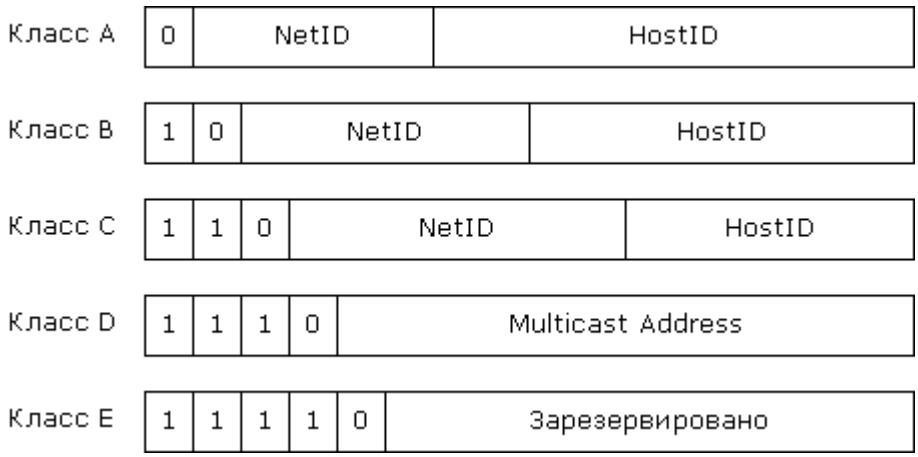

Рисунок 3.4.1 – Классы IP адресов

Из рисунка видно, что классы сетей определяют, как возможное количество этих сетей, так и число хостов в них. Практически используются только первые три класса:

1) Класс A определен для сетей с числом хостов до 16777216. Под поле NetID отведено 7 бит, под поле HostID – 24 бита.

2) Класс B используется для среднемасштабных сетей (NetID – 14 бит, HostID – 16 бит). В каждой такой сети может быть до 65 536 хостов.

3) Класс C применяется для небольших сетей (NetId – 21 бит, HostID – 8 бит) с числом хостов до 255.

3 Система доменных имен

Во времена, когда ARPANET состояла из довольно небольшого числа хостов, все они были перечислены в одном файле (HOSTS. TXT). Этот файл хранился в сетевом информационном центре Станфордского исследовательского института (SRI-NIC – Stanford Research Institute Network Information Center). Каждый администратор сайта посылал в SRI-NIC дополнения и изменения, происшедшие в конфигурации его системы. Периодически администраторы переписывали этот файл в свои системы, где из него генерировали файл /etc/hosts. С ростом ARPANET это стало чрезвычайно затруднительным. С переходом на TCP/IP совершенствование этого механизма стало необходимостью, поскольку, например, какой-то администратор мог присвоить новой машине имя уже существующей. Решением этой проблемы явилось создание доменов,

или локальных полномочий, в которых администратор мог присваивать имена своим машинам и управлять данными адресации в своем домене.

1) Домен – группа узлов сети (хостов) объединенных общим именем, которое для удобства несет определенную смысловую нагрузку. Например, домен «ru» объединяет узлы на территории России. В более широком смысле под доменом понимается множество машин, которые администрируются и поддерживаются как одно целое. Можно сказать, что все машины локальной сети составляют домен в большей сети, хотя можно и разделить машины локальной сети на несколько доменов. При подключении к Интернету домен должен быть поименован в соответствии с соглашением об именах в этой сети. Интернет организован как иерархия доменов. Каждый уровень иерархии является ветвью уровня root. На каждом уровне находится сервер имен – машина, которая содержит информацию о машинах низшего уровня и соответствии их имен IP-адресам. Схема построения иерархии доменов приведена на рисунке 3.4.2.

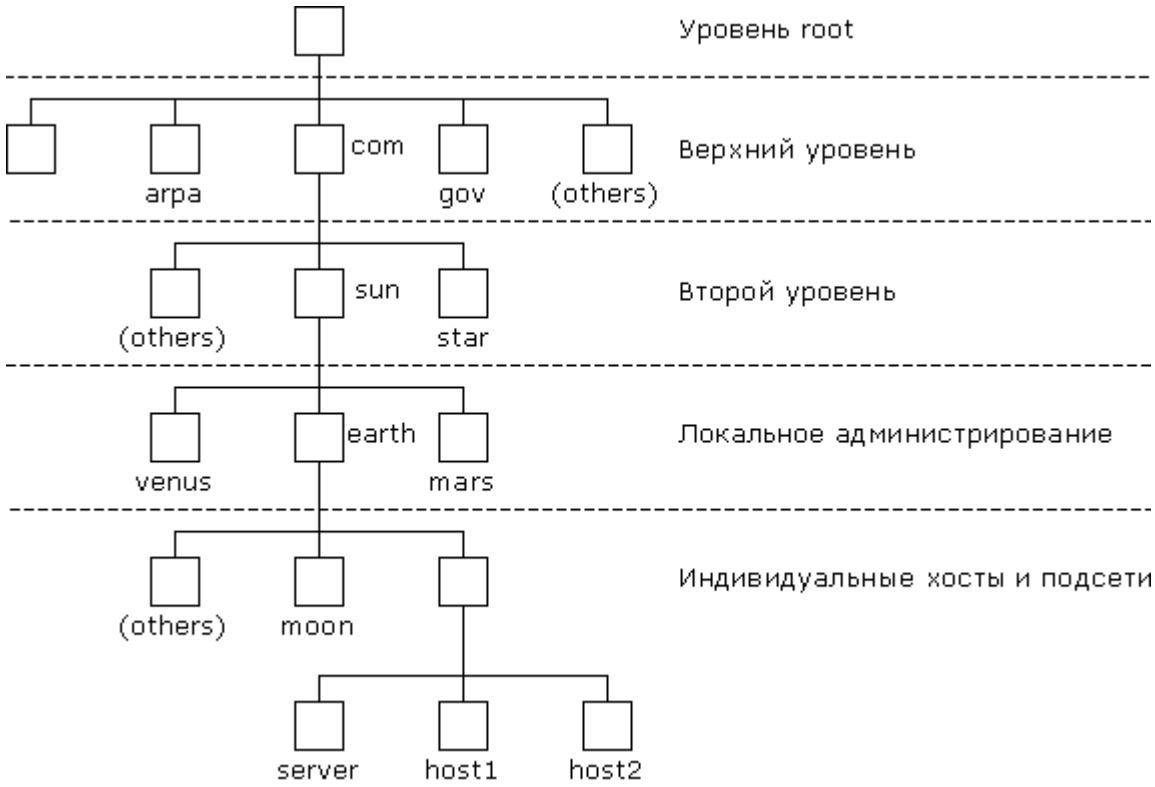

Рисунок 3.4.2 – Структура имен доменов

Домен корневого уровня формируется InterNIC (сетевым информационным центром сети Интернет).

Домены верхнего уровня имеют следующие ветви:

- edu – образовательные учреждения;
- gov – правительственные учреждения;
- arpa – ARPANET;
- com – коммерческие организации;
- mil – военные организации;
- int – международные организации;
- org – некоммерческие организации;
- net – сетевые информационные центры.

Начиная с весны 1997 к ним добавились еще 7 доменов:

- firm – фирмы и направления их деятельности;
- store – торговые фирмы;
- web – объекты, связанные с WWW;
- arts – объекты, связанные с культурой и искусством;
- rec – развлечения и отдых;
- info – информационные услуги;
- nom – прочие.

Эти имена соответствуют типам сетей, которые составляют данные домены. Кроме этого, к доменам верхнего уровня относятся домены по географическому признаку, у которых представление названия страны двухбуквенное.

- it – Италия;
- jp – Япония;
- kr – Корея;
- nz – Новая Зеландия;
- ru – Россия;
- se – Швеция;

- su – бывший СССР;
- tw – Тайвань;
- uk – Англия/Ирландия;
- us – Соединенные Штаты.

Члены организаций на втором уровне управляют своими серверами имен. Домены локального уровня администрируются организациями. Локальные домены могут состоять из одного хоста или включать не только множество хостов, но и свои поддомены.

Имя домена образуется «склеиванием» всех доменов от корневого до текущего, перечисленных справа налево и разделенных точками. Например, в имени kernel. generic. edu:

edu – соответствует верхнему уровню,

generic – показывает поддомен edu,

kernel – является именем хоста.

Мы подошли к очень важному понятию – определению службы имен доменов (или служба доменных имен) – DNS (Domain Name Service).

Как уже было показано ранее адресация в сети (сетевой уровень) основана на протоколе IP, тогда как для удобства администрирования сетей и пользователей (прикладной уровень) в вычислительных сетях введены имена доменов, несущие определенную смысловую нагрузку.

2) Служба доменных имен как раз и предназначена для определения соответствия между доменным именем хоста и его реальным IP-адресом и наоборот. По сути, сервер (DNS-сервер), предоставляющий пользователям сети эту услугу хранит базу данных об этих соответствиях.

История развития сети Интернет показывает, что DNS-сервер является объектом атак со стороны злоумышленников, поскольку, выведя из строя этот сервер или изменив данные его базы можно, нарушить работу сети. Проблемы информационной безопасности, связанные с использованием DNS-серверов, будут рассмотрены далее.

4 Выводы по теме 3.4

1) Адресация современного Интернета основана на протоколе IP (Internet Protocol).

2) Концепция протокола IP представляет сеть как множество компьютеров (хостов), подключенных к некоторой интерсети. Интерсеть, в свою очередь, рассматривается как совокупность физических сетей, связанных маршрутизаторами.

3) Физические объекты (хосты, маршрутизаторы, подсети) идентифицируются при помощи специальных IP-адресов. Каждый IP-адрес представляет собой 32-битовый идентификатор.

4) IP-адрес записывается в виде 4-х десятичных чисел, разделенных точками. Для этого 32-х битовый IP-адрес разбивается на четыре группы по 8 бит (1 байт), после чего каждый байт двоичного слова преобразовывается в десятичное число.

5) Каждый адрес является совокупностью двух идентификаторов: сети – NetID и хоста – HostID.

6) Домен – группа узлов сети (хостов), объединенных общим именем, которое для удобства несет определенную смысловую нагрузку.

7) Служба доменных имен предназначена для определения соответствия между доменным именем хоста и его реальным IP адресом и наоборот.

Тема 3.5. Классификация удаленных угроз в вычислительных сетях

1 Классы удаленных угроз и их характеристика

При изложении данного материала в некоторых случаях корректнее говорить об удаленных атаках нежели, об удаленных угрозах объектам вычислительных сетей, тем не менее, все возможные удаленные атаки являются в принципе удаленными угрозами информационной безопасности.

Удаленные угрозы можно классифицировать по следующим признакам.

1) По характеру воздействия:

– пассивные (класс 1.1);

– активные (класс 1.2).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в вычислительных сетях является прослушивание канала связи в сети.

Под активным воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации, нарушение работоспособности и т. д.) и нарушающее принятую в ней политику безопасности. Практически все типы удаленных угроз являются активными воздействиями. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало. Очевидной особенностью активного воздействия по сравнению с пассивным является принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят определенные изменения. В отличие от активного, при пассивном воздействии не остается никаких следов (просмотр чужого сообщения ничего не меняет).

2) По цели воздействия:

– нарушение конфиденциальности информации (класс 2.1);

– нарушение целостности информации (класс 2.2);

– нарушение доступности информации, т.е. работоспособности системы (класс 2.3).

Этот классификационный признак является прямой проекцией трех основных типов угроз – раскрытия, целостности и отказа в обслуживании.

Одна из основных целей злоумышленников – получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить прослушивание канала в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной угрозы, цель которой нарушение целостности информации, может служить типовая удаленная атака «ложный объект распределенной вычислительной сети».

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации. Его основная цель – добиться, чтобы узел сети или какой-то из сервисов поддерживаемый им вышел из строя и для всех остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая удаленная атака «отказ в обслуживании».

3) По условию начала осуществления воздействия

В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:

– атака по запросу от атакуемого объекта (класс 3.1);
– атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);
– безусловная атака (класс 3.3).

В первом случае, злоумышленник ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet служат DNS-запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

Во втором случае, злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.

Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, то есть атака осуществляется немедленно.

4) По наличию обратной связи с атакуемым объектом:

– с обратной связью (класс 4.1);
– без обратной связи (однонаправленная атака) (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а, следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте.

В отличие от атак с обратной связью удаленным атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную удаленную атаку

можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является типовая удаленная атака «отказ в обслуживании».

5) По расположению субъекта атаки относительно атакуемого объекта:

– внутрисегментное (класс 5.1);

– межсегментное (класс 5.2).

Рассмотрим ряд определений:

А) Субъект атаки (или источник атаки) – это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Б) Маршрутизатор (router) – устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

В) Подсеть (subnetwork) (в терминологии Internet) – совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Г) Сегмент сети – физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме «общая шина». При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, то есть в одном или в разных сегментах они находятся. В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах. Данный классификационный признак позволяет судить о так называемой «степени удаленности» атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект её и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по локализации субъекта атаки.

6) По уровню модели ISO/OSI, на котором осуществляется воздействие:

– физический (класс 6.1);

– канальный (класс 6.2);

– сетевой (класс 6.3);

– транспортный (класс 6.4);

– сеансовый (класс 6.5);

– представительный (класс 6.6);

– прикладной (класс 6.7).

2 Выводы по теме 3.5

1) Субъект атаки (или источник атаки) – это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

2) Маршрутизатор – устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

3) Подсеть – совокупность узлов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети.

4) Сегмент сети – физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме «общая шина».

5) Удаленные угрозы классифицируются по следующим признакам:

– по характеру воздействия (пассивные, активные);

– по цели воздействия (нарушение конфиденциальности, нарушение целостности и нарушение доступности информации);

– по условию начала осуществления воздействия (атака по запросу от атакуемого объекта, атака по наступлению ожидаемого события на атакуемом объекте и безусловная атака);

– по наличию обратной связи с атакуемым объектом (с обратной и без обратной связи);

– по расположению субъекта атаки относительно атакуемого объекта (внутрисегментное и межсегментное);

– по уровню модели ISO/OSI, на котором осуществляется воздействие.

Тема 3.6. Типовые удаленные атаки и их характеристика

1 Типовая удаленная атака

Как уже было показано ранее, распределенные вычислительные сети проектируются на основе одних и тех же принципов, а, следовательно, имеют практически одинаковые проблемы безопасности, причем, в большинстве случаев, независимо от используемых сетевых протоколов, топологии и инфраструктуры вычислительной сети.

С учетом этого специалисты в области информационной безопасности используют понятие типовой удаленной угрозы (атаки), характерной для любых распределенных вычислительных сетей. Введение этого понятия в совокупности с описанием механизмов реализации типовых удаленных угроз позволяет выработать методику исследования безопасности вычислительных сетей, заключающуюся в последовательной умышленной реализации всех типовых удаленных угроз и наблюдению за поведением системы.

Типовая удаленная атака – это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

2 Удаленная атака «анализ сетевого трафика»

Основной особенностью распределенной вычислительной сети является распределенность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого анализом сетевого трафика.

Анализ сетевого трафика позволяет:

– изучить логику работы распределенной вычислительной сети, это достигается путем перехвата и анализа пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять другие типовые удаленные атаки);

– перехватить поток данных, которыми обмениваются объекты сети, т. е. удаленная атака данного типа заключается в получении несанкционированного доступа к информации, которой обмениваются пользователи (примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

По характеру воздействия анализ сетевого трафика является пассивным воздействием (класс 1.1). Осуществление данной атаки без обратной связи (класс 4.2) ведет к нарушению конфиденциальности информации (класс 2.1) внутри одного сегмента сети (класс 5.1) на канальном уровне OSI (класс 6.2). При этом начало осуществления атаки безусловно по отношению к цели атаки (класс 3.3).

3 Удаленная атака «подмена доверенного объекта»

Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация (определение подлинности) удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в вычислительных сетях эта проблема решается использованием виртуального канала, по которому объекты обмениваются определенной информацией, уникально идентифицирующей данный канал. Для адресации сообщений в распределенных вычислительных сетях используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI – это аппаратный адрес сетевого адаптера, на сетевом уровне – адрес определяется протоколом сетевого уровня (например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов сети. Однако сетевой адрес достаточно просто подделывается и поэтому использовать его в качестве единственного средства идентификации объектов недопустимо. В том случае, когда в вычислительной сети использует нестойкие алгоритмы идентификации удаленных объектов, то оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети (т. е. подмена объекта или субъекта сети).

Подмена доверенного объекта распределенной вычислительной сети является активным воздействием (класс 1.2), совершаемым с целью нарушения конфиденциальности (класс 2.1) и целостности (класс 2.2) информации, по наступлению на атакуемом объекте определенного события (класс 3.2). Данная удаленная атака может являться как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи (класс 4.2) с атакуемым объектом и осуществляется на сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

4 Удаленная атака «ложный объект»

Принципиальная возможность реализации данного вида удаленной атаки в вычислительных сетях также обусловлена недостаточно надежной идентификацией сетевых управляющих устройств (например, маршрутизаторов). Целью данной атаки является внедрение в сеть ложного объекта путем изменения маршрутизации пакетов, передаваемых в сети. Внедрение ложного объекта в распределенную сеть может быть реализовано навязыванием ложного маршрута, проходящего через ложный объект.

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждого адресата указывается оптимальный маршрут. Таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов (узлов) в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в распределенных ВС применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First)), уведомлять хосты о новом маршруте – ICMP (Internet Control Message Protocol), удаленно управлять маршрутизаторами (SNMP (Simple Network Management Protocol)). Эти протоколы позволяют удаленно изменять маршрутизацию в сети Интернет, то есть являются протоколами управления сетью.

Реализация данной типовой удаленной атаки заключается в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются объекты сети, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов вычислительной сети.

Навязывание ложного маршрута – активное воздействие (класс 1.2), совершаемое с любой из целей из класса 2, безусловно по отношению к цели атаки (класс 3.3). Данная типовая удаленная атака может осуществляться как внутри одного сегмента (класс 5.1), так и межсегментно (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи с атакуемым объектом (класс 4.2) на транспортном (класс 6.3) и прикладном (класс 6.7) уровне модели OSI.

Получив контроль над проходящим потоком информации между объектами, ложный объект вычислительной сети может применять различные методы воздействия на перехваченную информацию, например:

– селекция потока информации и сохранение ее на ложном объекте (нарушение конфиденциальности);

– модификация информации:

а) модификация данных (нарушение целостности),

б) модификация исполняемого кода и внедрение разрушающих программных средств – программных вирусов (нарушение доступности, целостности);

– подмена информации (нарушение целостности).

5 Удаленная атака «отказ в обслуживании»

Одной из основных задач, возлагаемых на сетевую операционную систему, функционирующую на каждом из объектов распределенной вычислительной сети, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в сети каждый субъект системы должен иметь возможность подключиться к любому объекту сети и получить в соответствии со своими правами удаленный доступ к его ресурсам. Обычно в вычислительных сетях возможность

предоставления удаленного доступа реализуется следующим образом: на объекте в сетевой операционной системе запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т. п.), предоставляющих удаленный доступ к ресурсам данного объекта. Данные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы постоянно ожидать получения запроса на подключение от удаленного объекта и, получив такой запрос, передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты сети. В этом случае непосредственно операционная система обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (номер порта) прикладному процессу, которым является соответствующий сервер. В зависимости от различных параметров объектов вычислительной сети, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи – количество одновременно устанавливаемых виртуальных подключений ограничено, соответственно, ограничено и число запросов, обрабатываемых в единицу времени. С этой особенностью работы вычислительных сетей связана типовая удаленная атака «отказ в обслуживании». Реализация этой угрозы возможна, если в вычислительной сети не предусмотрено средств аутентификации (проверки подлинности) адреса отправителя. В такой вычислительной сети возможна передача с одного объекта (атакующего) на другой (атакуемый) бесконечного числа анонимных запросов на подключение от имени других объектов.

Результат применения этой удаленной атаки – нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов вычислительной сети – отказ в обслуживании. Одна из разновидностей этой типовой удаленной атаки заключается в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволяет трафик. В этом случае, если в системе не предусмот-

рены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов. И последней, третьей разновидностью атаки «отказ в обслуживании» является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы.

Типовая удаленная атака «отказ в обслуживании» является активным (класс 1.2) однонаправленным воздействием (класс 4.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3) на транспортном (класс 6.4) и прикладном (класс 6.7) уровнях модели OSI.

6 Выводы по теме 3.6

1) Типовая удаленная атака – это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

2) Анализ сетевого трафика заключается в прослушивании канала связи.

3) По характеру воздействия анализ сетевого трафика является пассивным воздействием (класс 1.1). Осуществление данной атаки без обратной связи (класс 4.2) ведет к нарушению конфиденциальности информации (класс 2.1) внутри одного сегмента сети (класс 5.1) на канальном уровне OSI (класс 6.2). При этом начало осуществления атаки безусловно по отношению к цели атаки (класс 3.3).

4) Одной из проблем безопасности распределенной ВС является недостаточная идентификация и аутентификация (определение подлинности) удаленных друг от друга объектов.

Таблица 3.6.1 – Общая характеристика типовых удаленных атак

Типовая удаленная атака	**Характер воздействия**		**Цель воздействия**			**Условие начала**			**Наличие обратной связи**		**Расположение субъекта атаки**		**Уровень модели OSI**						
Класс воздействия	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
Анализ сетевого трафика	+	-	+	-	-	-	-	+	-	+	+	-	-	+	-	-	-	-	-
Подмена доверенного объекта сети	-	+	+	+	-	-	+	-	+	+	+	+	-	-	+	+	-	-	-
Внедрение ложного объекта	-	+	+	+	+	-	-	+	+	+	+	+	-	-	+	-	-	-	-
Отказ в обслуживании	-	+	-	-	+	-	-	+	-	+	+	+	-	+	+	+	+	+	+

5) В том случае, когда в вычислительной сети используют нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети (т. е. подмена объекта или субъекта сети).

6) Подмена доверенного объекта распределенной вычислительной сети является активным воздействием (класс 1.2), совершаемым с целью нарушения конфиденциальности (класс 2.1) и целостности (класс 2.2) информации, по наступлению на атакуемом объекте определенного события (класс 3.2). Данная удаленная атака может являться как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи (класс 4.2) с атакуемым объектом и осуществляется на сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

7) Целью удаленной атаки «ложный объект» является внедрение в сеть ложного объекта путем изменения маршрутизации пакетов, передаваемых в сети. Внедрение ложного объекта в распределенную сеть может быть реализовано навязыванием ложного маршрута, проходящего через ложный объект.

8) Навязывание ложного маршрута – активное воздействие (класс 1.2), совершаемое с любой из целей из класса 2, безусловно по отношению к цели атаки (класс

3.3). Данная типовая удаленная атака может осуществляться как внутри одного сегмента (класс 5.1), так и межсегментно (класс 5.2), как с обратной связью (класс 4.1), так и без обратной связи с атакуемым объектом (класс 4.2) на транспортном (класс 6.3) и прикладном (класс 6.7) уровне модели OSI.

9) Целью удаленной атаки «отказ в обслуживании» является нарушение работоспособности соответствующего узла сети или сервиса, предоставляемого им другим пользователям.

10) Типовая удаленная атака «отказ в обслуживании» является активным (класс 1.2) однонаправленным воздействием (класс 4.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3) на транспортном (класс 6.4) и прикладном (класс 6.7) уровнях модели OSI.

Тема 3.7. Причины успешной реализации удаленных угроз в вычислительных сетях

1 Причины успешной реализации удаленных угроз в вычислительных сетях

Применительно к вычислительным сетям, чтобы ликвидировать угрозы (удаленные атаки), осуществляемые по каналам связи, необходимо ликвидировать причины, их порождающие. Анализ механизмов реализации типовых удаленных атак позволяет сформулировать причины, по которым данные удаленные атаки оказались возможными.

1) Отсутствие выделенного канала связи между объектами вычислительной сети. Данная причина обуславливает типовую удаленную атаку «анализ сетевого трафика». Такая атака программно возможна только в случае, если атакующий находится в сети с физически широковещательной средой передачи данных как, например, всем известная и получившая широкое распространение среда Ethernet (общая «шина»). Такая атака невозможна в сетях с топологией «звезда» (Token Ring), которая не является широковещательной, но и не имеет достаточного распространения. Анализ сетевого трафика программными средствами практически невозможен, если у каждого объекта системы существует для связи с любым другим объектом выделенный канал. Следовательно, причина успеха типовой удаленной атаки заключается в широковещательной среде передачи данных или отсутствие выделенного канала связи между объектами сети.

2) Недостаточная идентификация объектов и субъектов сети неоднократно упоминались при рассмотрении удаленных угроз информационной безопасности. Эта причина предопределяет такие типовые удаленные атаки как «ложный объект» и «подмена доверенного объекта», а в некоторых случаях и «отказ в обслуживании».

3) Взаимодействие объектов без установления виртуального канала – еще одна причина возможных угроз информационной безопасности. Объекты распределенных вычислительных сетей могут взаимодействовать двумя способами:

– с использованием виртуального канала;

– без использования виртуального канала.

При создании виртуального канала объекты вычислительной сети обмениваются динамически вырабатываемой ключевой информацией, позволяющей уникально идентифицировать канал, тем самым подтверждается подлинность объектов информационного обмена друг перед другом.

Однако ошибочно считать распределенную вычислительную сеть безопасной, даже если все взаимодействие объектов происходит с созданием виртуального канала. Виртуальный канал является необходимым, но не достаточным условием безопасного взаимодействия. Чрезвычайно важным в данном случае становится выбор алгоритма идентификации при создании виртуального канала. Так, например, отсутствие контроля за виртуальными каналами связи между объектами сети может привести к нарушению работоспособности системы путем формирования множества запросов на создание соединения (виртуального канала), в результате чего-либо переполняется число возможных соединений, либо система, занятая обработкой ответов на запросы, вообще перестает функционировать (типовая удаленная атака «отказ в обслуживании»). В данном случае успех удаленной атаки возможен из-за отсутствия контроля при создании соединения, т. е. один узел анонимно или от имени другого узла сети формирует множество запросов, а система не имеет возможности фильтровать подобные запросы.

4) Отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений – еще одна из возможных причин успешной реализации удаленных угроз информационной безопасности.

Если в вычислительных сетях не предусмотрены возможности контроля за маршрутом сообщения, то адрес отправителя сообщения оказывается ничем не подтвержден. Таким образом, в системе будет существовать возможность отправки сообщения от имени любого объекта системы, а именно, путем указания в заголовке сообщения чужого адреса отправителя. Также в таких сетях будет невозможно определить, откуда на самом деле пришло сообщение, а, следовательно, вычислить координаты атакующего. Отсутствие в вычислительной сети контроля за маршрутом сообщений порождает как невозможность контроля за созданием соединений, так и возможность

анонимной отправки сообщения, следовательно, является причиной успеха таких удаленных угроз, как «подмена доверенного объекта» и «ложный объект сети».

5) Отсутствие в распределенных вычислительных сетях полной информации о ее объектах также является потенциальной причиной успеха удаленных угроз, поскольку в распределенной системе с разветвленной структурой, состоящей из большого числа объектов, может возникнуть ситуация, когда для доступа к определенному объекту системы у субъекта взаимодействия может не оказаться необходимой информации об интересующем объекте. Обычно такой недостающей информацией об объекте является его адрес. В этом случае осуществляется широковещательный запрос в сеть, на который реагирует искомый узел. Такая ситуация характерна особенно для сети Интернет, при работе в которой пользователь знает доменное имя узла, но для соединения с ним необходим IP-адрес, поэтому при вводе доменного имени операционная система формирует запрос к серверу доменных имен. В ответ DNS сервер сообщает IP-адрес запрашиваемого узла. В такой схеме существует возможность выдачи ложного ответа на запрос пользователя, например, путем перехвата DNS-запроса пользователя и выдачей ложного DNS-ответа.

В системе с заложенной в нее неопределенностью существуют потенциальные возможности внесения в систему ложного объекта и получение ложного ответа, в котором вместо информации о запрашиваемом объекте будет информация о ложном объекте.

Примером распределенной вычислительной сети с заложенной неопределенностью является сеть Интернет. Во-первых, у узлов, находящихся в одном сегменте, может не быть информации об аппаратных адресах друг друга. Во-вторых, применяются непригодные для непосредственной адресации доменные имена узлов, используемые для удобства пользователей при обращении к удаленным системам.

6) Отсутствие в распределенных вычислительных сетях криптозащиты сообщений – последняя из рассматриваемых в данной теме причин успеха удаленных угроз информационной безопасности.

Поскольку в вычислительных сетях связь между объектами осуществляется по каналам связи, то всегда существует принципиальная возможность для злоумышленника прослушать канал и получить несанкционированный доступ к информации, которой обмениваются по сети ее абоненты. В том случае, если проходящая по каналу информация не зашифрована и атакующий каким-либо образом получает доступ к каналу, то удаленная атака «анализ сетевого трафика» является наиболее эффективным способом получения информации. Очевидна и причина, делающая эту атаку столь эффективной. Эта причина – передача по сети незашифрованной информации.

2 Выводы по теме

1) Базовым принципом обеспечения информационной безопасности для любых объектов информационных отношений является борьба не с угрозами, являющимися следствием недостатков системы, а с причинами возможного успеха нарушений информационной безопасности.

2) Причины успешной реализации удаленных угроз в вычислительных сетях:

– отсутствие выделенного канала связи между объектами вычислительной сети;

– недостаточная идентификация объектов и субъектов сети;

– взаимодействие объектов без установления виртуального канала;

– отсутствие контроля за виртуальными каналами связи между объектами сети;

– отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений;

– отсутствие в распределенных вычислительных сетях полной информации о ее объектах;

– отсутствие в распределенных вычислительных сетях криптозащиты сообщений.

Тема 3.8. Принципы защиты распределенных вычислительных сетей

1 Принципы построения защищенных вычислительных сетей

В предыдущих темах были рассмотрены основные угрозы информационной безопасности в распределенных вычислительных сетях и причины, следствием которых они являются.

В данной теме рассмотрим принципы построения защищенных вычислительных сетей. Принципы построения защищенных вычислительных сетей по своей сути являются правилами построения защищенных систем, учитывающие, в том числе, действия субъектов вычислительной сети, направленные на обеспечение информационной безопасности.

Напомним, что одним из базовых принципов обеспечения информационной безопасности для любых объектов информационных отношений является борьба не с угрозами, являющимися следствием недостатков системы, а с причинами возможного успеха нарушений информационной безопасности.

Перечислим установленные ранее причины успеха удаленных угроз информационной безопасности:

1) Отсутствие выделенного канала связи между объектами вычислительной сети.

2) Недостаточная идентификация объектов и субъектов сети.

3) Взаимодействие объектов без установления виртуального канала.

4) Отсутствие контроля за виртуальными каналами связи между объектами сети.

5) Отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений.

6) Отсутствие в распределенных вычислительных сетях полной информации о ее объектах.

7) Отсутствие в распределенных вычислительных сетях криптозащиты сообщений.

Для устранения первой причины («отсутствие выделенного канала...») идеальным случаем было бы установление выделенных каналов связи между всеми объектами сети. Однако это практически невозможно и нерационально, в первую очередь, из-за высокой стоимости такой топологии вычислительной сети.

Существуют два возможных способа организации топологии распределенной вычислительной сети с выделенными каналами. В первом случае каждый объект связывается физическими линиями связи со всеми объектами системы. Во втором случае в системе может использоваться сетевой концентратор, через который осуществляется связь между объектами (топология «звезда»).

Преимущества сети с выделенным каналом связи между объектами заключаются:

– в передаче сообщений напрямую между источником и приемником, минуя остальные объекты системы;

– в возможности идентифицировать объекты распределенной системы на канальном уровне по их адресам без использования специальных крипто-алгоритмов шифрования трафика;

– в отсутствии неопределенности информации о ее объектах, поскольку каждый объект в такой системе изначально однозначно идентифицируется и обладает полной информацией о других объектах системы.

Недостатки сети с выделенными каналами:

– сложность реализации и высокие затраты на создание;

– ограниченное число объектов системы (зависит от числа входов у концентратора).

Альтернативой сетям с выделенным каналом являются сети с широковещательной передачей данных, надежная идентификация объектов в которых может обеспечиваться использованием специальных крипто-карт, осуществляющих шифрование на канальном уровне.

Отметим, что создание распределенных систем только с использованием широковещательной среды передачи или только с выделенными каналами неэффективно,

поэтому представляется правильным при построении распределенных вычислительных сетей с разветвленной топологией и большим числом объектов использовать комбинированные варианты соединений объектов. Для обеспечения связи между объектами большой степени значимости можно использовать выделенный канал. Связь менее значимых объектов системы может осуществляться с использованием комбинации «общая шина» – выделенный канал.

Безопасная физическая топология сети (выделенный канал) является необходимым, но не достаточным условием устранения причин угроз информационной безопасности, поэтому необходимы дополнительные меры по повышению защищенности объектов вычислительных сетей. Дальнейшее повышение защищенности вычислительных сетей связано с использованием виртуальных каналов, обеспечивающих дополнительную идентификацию и аутентификацию объектов вычислительной сети.

Для повышения защищенности вычислительных сетей при установлении виртуального соединения необходимо использовать крипто-алгоритмы с открытым ключом (рассмотрим далее). Одной из разновидностей шифрования с открытым ключом является цифровая подпись сообщений, надежно идентифицирующая объект распределенной вычислительной сети и виртуальный канал.

Отсутствие контроля за маршрутом сообщения в сети является одной из причин успеха удаленных угроз. Рассмотрим один из вариантов устранения этой причины.

Все сообщения, передаваемые в распределенных сетях, проходят по цепочке маршрутизаторов, задачей которых является анализ адреса назначения, выбор оптимального маршрута и передача по этому маршруту пакета или на другой маршрутизатор или непосредственно абоненту, если он напрямую подключен к данному узлу. Информация о маршруте передачи сообщения может быть использована для идентификации источника этого сообщения с точностью до подсети, т. е. от первого маршрутизатора.

Задачу проверки подлинности адреса сообщения можно частично решить на уровне маршрутизатора. Сравнивая адреса отправителя, указанные в сообщении с ад-

ресом подсети, из которой получено сообщение, маршрутизатор выявляет те сообщения, у которых эти параметры не совпадают, и соответственно, отфильтровывает такие сообщения.

Контроль за виртуальным соединением можно рассматривать как принцип построения защищенных систем, поскольку в этом случае определяются те правила, исходя из которых система могла бы либо поставить запрос в очередь, либо нет. Для предотвращения такой атаки как «отказ в обслуживании», вызванной «лавиной» направленных запросов на атакуемый узел целесообразно ввести ограничения на постановку в очередь запросов от одного объекта. Очевидно, что данная мера имеет смысл в тех случаях, когда надежно решена проблема идентификации объекта – отправителя запроса. В противном случае злоумышленник может отправлять запросы от чужого имени.

Для повышения защищенности распределенных вычислительных сетей целесообразно проектировать их с полностью определенной информацией о ее объектах, что позволит устранить шестую из указанных причин успешной реализации удаленных угроз.

Однако в вычислительных сетях с неопределенным и достаточно большим числом объектов (например, Интернет) спроектировать систему с отсутствием неопределенности практически невозможно, а отказаться от алгоритмов удаленного поиска не представляется возможным.

Из существующих двух типов алгоритмов удаленного поиска (с использованием информационно-поискового сервера и с использованием широковещательных запросов) более безопасным является алгоритм удаленного поиска с использованием информационно-поискового сервера. Однако для большей безопасности связь объекта, формирующего запрос с сервером, необходимо осуществлять с подключением по виртуальному каналу. Кроме этого, объекты, подключенные к данному серверу, и сам сервер должны содержать заранее определенную статическую ключевую информацию, используемую при создании виртуального канала (например, закрытый криптографический ключ).

2 Выводы по теме 3.8

1) Принципы построения защищенных вычислительных сетей по своей сути являются правилами построения защищенных систем, учитывающие, в том числе, действия субъектов вычислительной сети, направленные на обеспечение информационной безопасности.

2) Существуют два возможных способа организации топологии распределенной вычислительной сети с выделенными каналами. В первом случае каждый объект связывается физическими линиями связи со всеми объектами системы. Во втором случае в системе может использоваться сетевой концентратор, через который осуществляется связь между объектами (топология «звезда»).

3) Безопасная физическая топология сети (выделенный канал) является необходимым, но не достаточным условием устранения причин угроз информационной безопасности.

4) Для повышения защищенности вычислительных сетей при установлении виртуального соединения необходимо использовать крипто-алгоритмы с открытым ключом.

5) Одной из разновидностей шифрования с открытым ключом является цифровая подпись сообщений, надежно идентифицирующая объект распределенной вычислительной сети и виртуальный канал.

6) Задачу проверки подлинности адреса сообщения можно частично решить на уровне маршрутизатора.

7) Для предотвращения типовой атаки «отказ в обслуживании», вызванной «лавиной» направленных запросов на атакуемый узел целесообразно ввести ограничения на постановку в очередь запросов от одного объекта.

8) Для повышения защищенности распределенных вычислительных сетей целесообразно проектировать их с полностью определенной информацией о ее объектах.