ЧАСТЬ 5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГЛОБАЛЬНЫХ СЕТЯХ

15. ТИПОВЫЕ УДАЛЕННЫЕ АТАКИ В ГЛОБАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

15.1 Понятие типовой удаленной атаки

Рассмотрим ряд определений.

Распределенная вычислительная система (РВС) - *совокупность структурно и пространственно распределенных информационных систем, рабочих станций и вычислительных узлов обьединенных каналами связи в единую сеть для решения информационно-вычислительных задач.*

Типовая удаленная атака (УА) - *это удаленное информационное разрушающее воздействие, осуществляемое по каналам связи и характерное для любой распределенной вычислительной системы.*

Субъект атаки (или источник атаки) - *это атакующая программа или оператор, непосредственно осуществляющие воздействие.*

Хост (host) - *сетевой компьютер (рабочая станция).*

Маршрутизатор (router) - *устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.*

Подсеть (subnetwork) - *совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети.* Подсеть - логическое объединение хостов маршрутизатором. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

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.

Удаленные атаки становятся возможными благодаря уязвимостям в существующих протоколах обмена данными и системах зашиты сетей, а также в ОС и ПО хостов.

Основные причины уязвимости хостов сети:

1. *открытость системы, свободный доступ к информации по организации сетевого взаимодействия, протоколам и механизмам защиты;*
2. *наличие ошибок в программном обеспечении, операционных системах и утилитах, которые открыто публикуются в сети;*
3. *разнородность используемых версий программного обеспечения и операционных систем;*
4. *сложность организации защиты межсетевого взаимодействия;*
5. *ошибки конфигурирования систем и средств защиты;*
6. *неправильное или ошибочное администрирование систем;*

7. *несвоевременное отслеживание и выполнение рекомендаций специалистов по защите и анализу случаев вторжения для ликвидации лазеек и ошибок в программном обеспечении;*
8. *«экономия» на средствах и системах обеспечения безопасности или игнорирование их;*
9. *умолчание о случаях нарушения безопасности своего хоста или сети.*

Примеры уязвимостей некоторых распространенных служб Internet:

- ***Простой протокол передачи электронной почты (Simple Mail Transfer Protocol - SMTP)*** *позволяет осуществлять почтовую транспортную службу Internet.* Одна из проблем безопасности, связанная с этим протоколом, заключается в том, что пользователь не может проверить адрес отправителя в заголовке сообщения электронной почты. В результате хакер может послать во внутреннюю сеть большое количество почтовых сообщений, что приведет к перегрузке и блокированию работы почтового сервера. Программы электронной почты использует для работы IP-адрес отправителя. Перехватывая сообщения email, хакер может употребить эту информацию для нападений, например для спуфинга (подмены адресов).
- ***Служба сетевых имен (Domain Name System - DNS)*** *представляет собой распределенную базу данных, которая преобразует имена пользователей и хост-компьютеров в IP-адреса, указываемые в заголовках пакетов, и наоборот. DNS также хранит информацию о структуре сети компании, например количестве компьютеров с IP-адресами в каждом домене.* Одной из проблем DNS является то, что эту базу данных очень трудно «скрыть» от неавторизированных пользователей. В результате DNS часто используется хакерами как источник информации об именах доверенных хост-компьютеров.
- ***Служба эмуляции удаленного терминала (TELNET)*** *употребляется для подключения к удаленным системам, присоединенным к сети; применяет базовые возможности по эмуляции терминала. При использовании этого сервиса Internet пользователи должны регистрироваться на сервере TELNET, вводя свои имя и пароль. После аутентификации пользователя его рабочая станция функционирует в режиме терминала, подключенного к внешнему хост-компьютеру.* Подключившись к серверу TELNET, хакер может сконфигурировать его программу таким образом, чтобы она записывала имена и пароли пользователей.
- ***Всемирная паутина (World Wide Web - WWW)*** *- это система, основанная на сетевых приложениях, которые позволяют пользователям просматривать содержимое различных серверов в*

Internet или интрасетях. Полезным свойством WWW является использование гипертекстовых документов, что дает пользователям возможность легко переходить от одного узла к другому. Это же свойство является и наиболее слабым местом системы WWW, поскольку ссылки на Web-узлы, хранящиеся в гипертекстовых документах, содержат информацию о том, как осуществляется доступ к соответствующим узлам. Используя эту информацию, хакеры могут разрушить Web-узел или получить доступ к хранящейся в нем конфиденциальной информации. - *К уязвимым службам и протоколам Internet относятся также протокол копирования* ***UUCP****, протокол маршрутизации* ***RIP****, графическая оконная система* ***X Windows*** *и др.*

15.2 Классификация удаленных атак

1. ***По характеру воздействия:***
   - **1.1.*Пассивное воздействие.*** Пассивным воздействие не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие *непосредственного* влияния на работу распределенной ВС приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в РВС служит прослушивание канала связи в сети. В отличие от активного, при пассивном воздействии не остается никаких следов (от того, что атакующий просмотрит чужое сообщение в системе, в тот же момент ничего не изменится).
   - **1.2.*активное воздействие.*** Активное воздействие, оказывает непосредственное влияние на работу системы (изменение конфигурации РВС, нарушение работоспособности и т. д.) и нарушает принятую в ней политику безопасности. Практически все типы удаленных атак 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 (естественно, с большей или меньшей степенью сложности), так как в результате его осуществления в системе происходят определенные изменения.

2. ***По цели воздействия:***
   - ***2.1. нарушение конфиденциальности информации либо ресурсов системы – перехват информации.*** 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.

2.2. ***нарушение целостности информации – искажение информации.*** 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 атаки, цель которой нарушение целостности информации, может служить типовая удаленная атака (УА) «Ложный объект РВС».

2.3. ***нарушение работоспособности (доступности) системы.*** В этом случае не предполагается получение атакующим несанкционированного доступа к информации. Его основная цель - добиться, чтобы операционная система на атакуемом объекте вышла из строя и для всех остальных объектов системы доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая УА «Отказ в обслуживании».

3. ***По условию начала осуществления воздействия:***

3.1. ***Атака по запросу от атакуемого объекта.*** В этом случае атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Internet могут служить - DNS- и ARP-запросы. Важно отметить, что данный тип удаленных атак наиболее характерен для распределенных ВС.

3.2. ***Атака по наступлению ожидаемого события на атакуемом объекте.*** В этом случае атакующий 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. Примером такого события может быть прерывание сеанса работы пользователя с сервером в ОС Novell NetWare без выдачи команды LOGOUT.

3.3. ***Безусловная атака.*** В этом случае начало осуществления атаки безусловно по отношению к цели атаки, то есть атака осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта. Следовательно, в этом случае атакующий является инициатором начала осуществления атаки.

4. ***По наличию обратной связи с атакуемым объектом:***
   - 4.1. ***С обратной связью.*** 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. Подобные удаленные атаки наиболее характерны для распределенных ВС.
   - 4.2. ***Без обратной связи (однонаправленная атака).*** 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 УА можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является типовая УА «Отказ в обслуживании».

5. ***По расположению субъекта атаки относительно атакуемого объекта:***
   - 5.1. ***Внутрисегментное.*** В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. В дальнейшем будет показано, что на практике межсегментную атаку осуществить значительно труднее, чем внутрисегментную. 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 отражению атаки.
   - 5.2. ***Межсегментное.*** При межсегментной атаке субъект и объект атаки находятся в разных сегментах.

6. ***По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие:***
   - 6.1. *физический,*
   - 6.2. *канальный,*
   - 6.3. *сетевой,*
   - 6.4. *транспортный,*
   - 6.5. *сеансовый,*
   - 6.6. *представительный,*
   - 6.7. *прикладной.*

15.3 Типовые удаленные атаки и механизмы их реализации

15.3.1 Анализ сетевого трафика

Как уже отмечалось, основной особенностью распределенной ВС (РВС) является то, что ее объекты распределены в пространстве и связь между ними физически осуществляется по сетевым соединениям и программно – т.е. сообщения и данные, пересылаемые между объектами РВС, передаются по сетевым соединениям в виде пакетов. Эта особенность привела к появлению специфичного для РВС типового удаленного воздействия, заключающегося в прослушивании канала связи. Назовем данное типовое удаленное воздействие ***анализом сетевого трафика*** (или, сокращенно, сетевым анализом).

Анализ сетевого трафика позволяет:

1. ***изучить логику работы РВС****, то есть получить взаимно однозначное соответствие событий, происходящих в системе, и команд, пересылаемых друг другу ее объектами, в момент появления этих событий.* Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы РВС позволяет на практике моделировать и осуществлять типовые удаленные атаки, рассмотренные в следующих пунктах на примере конкретных РВС.
2. ***перехватить поток данных, которыми обмениваются объекты РВС.*** Таким образом, удаленная атака данного типа заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. 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).

15.3.2 Подмена доверенного объекта или субъекта системы

Одной из проблем безопасности РВС является недостаточная идентификация и аутентификация ее удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной

идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в РВС эта проблема решается следующим образом: в процессе создания виртуального канала объекты РВС обмениваются определенной информацией, уникально идентифицирующей данный канал. Такой обмен обычно называется «рукопожатием» (handshake). Однако, необходимо отметить, что не всегда для связи двух удаленных объектов в РВС создается виртуальный канал. Практика показывает, что зачастую, особенно для служебных сообщений (например, от маршрутизаторов) используется передача одиночных сообщений, не требующих подтверждения.

Для адресации сообщений в РВС используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI - это аппаратный адрес сетевого адаптера, на сетевом уровне - адрес определяется в зависимости от используемого протокола сетевого уровня (например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов РВС. Однако сетевой адрес достаточно просто подделывается и поэтому использовать его в качестве единственного средства идентификации объектов недопустимо.

В том случае, когда РВС 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 РВС.

При этом существуют две разновидности типовой удаленной атаки путем подмены доверенного объекта или субъекта РВС:

- ***Атака при установленном виртуальном канале.*** В случае установленного виртуального соединения атака будет заключаться в присвоении прав доверенного субъекта взаимодействия, легально подключившегося к объекту системы, что позволит атакующему вести сеанс работы с объектом распределенной системы от имени доверенного субъекта. Реализация удаленных атак данного типа обычно состоит в передаче пакетов обмена с атакующего объекта на цель атаки от имени доверенного субъекта взаимодействия (при этом переданные сообщения будут восприняты системой как корректные). Для осуществления атаки данного типа необходимо преодолеть систему идентификации и аутентификации сообщений, которая, в принципе, может использовать контрольную сумму, вычисляемую с помощью открытого ключа, динамически выработанного при установлении канала, случайные многобитные счетчики пакетов и сетевые адреса станций. Однако на практике, например, в протоколе TCP для идентификации используются два 32-битных счетчика.
- ***атака без установленного виртуального канала.*** Для служебных сообщений в РВС часто используется передача одиночных сообщений, не требующих подтверждения, то есть не требуется

создание виртуального соединения. *Атака без установленного виртуального соединения заключается в передаче служебных сообщений от имени сетевых управляющих устройств, например, от имени маршрутизаторов.* Очевидно, что в этом случае для идентификации пакетов возможно лишь использование статических ключей, определенных заранее, что довольно неудобно и требует сложной системы управления ключами. Однако, при отказе от такой системы идентификация пакетов без установленного виртуального канала будет возможна лишь по сетевому адресу отправителя, который легко подделать. Например, типовая удаленная атака, использующая навязывание ложного маршрута, путем посылки ложных управляющих сообщений основана на описанной идее.

Подмена доверенного объекта РВС 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.

15.3.3 Внедрение ложного объекта в систему

В том случае, если в РВС недостаточно надежно решены проблемы идентификации сетевых управляющих устройств (например, маршрутизаторов), возникающие при взаимодействии последних с объектами системы, то подобная распределенная система может подвергнуться типовой удаленной атаке, связанной с изменением маршрутизации и внедрением в систему ложного объекта. В том случае, если инфраструктура сети такова, что для взаимодействия объектов необходимо использование алгоритмов удаленного поиска, то это также позволяет внедрить в систему ложный объект. Таким образом, существуют две принципиально разные причины, обуславливающие появление типовой удаленной атаки «Ложный объект РВС».

15.3.3.1 Внедрение ложного объекта путем навязывания ложного маршрута

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. Отметим, что таблицы

маршрутизации существуют не только у маршрутизаторов, но и у любых хостов в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в РВС 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)).

Важно отметить, что все описанные выше протоколы позволяют удаленно изменять маршрутизацию в сети Internet, то есть являются протоколами управления сетью.

Поэтому абсолютно очевидно, что маршрутизация в глобальных сетях играет важнейшую роль и, как следствие этого, может подвергаться атаке. *Основная цель атаки, связанной с навязыванием ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте РВС так, чтобы новый маршрут проходил через ложный объект - хост атакующего. Реализация данной типовой удаленной атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации.*

Данная атака проходит в две стадии:

1. Для атакующему необходимо послать Рассылка по сети определенные данными протоколами управления сетью специальные служебные сообщения от имени сетевых управляющих устройств (например, маршрутизаторов), что приводит к изменению маршрутизации в сети. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются два объекта РВС.
2. прием, анализ и передача сообщений, получаемых от дезинформированных объектов РВС.

Навязывание объекту РВС 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.

15.3.3.2 Внедрение ложного объекта путем использования недостатков алгоритмов удаленного поиска

В РВС часто оказывается, что ее удаленные объекты изначально не имеют достаточно информации, необходимой для адресации сообщений. Обычно такой информацией являются аппаратные (адрес сетевого адаптера) и логические (IP-адрес, например) адреса объектов РВС. Для получения подобной информации в распределенных ВС используются различные *алгоритмы удаленного поиска*, заключающиеся в передаче по сети специального вида поисковых запросов, и в ожидании ответов на запрос с искомой информацией. После получения ответа на запрос, запросивший субъект РВС обладает всеми необходимыми данными для адресации. Руководствуясь полученными из ответа сведениями об искомом объекте, запросивший субъект РВС начинает адресоваться к нему. Примером подобных запросов, на которых базируются алгоритмы удаленного поиска, могут служить ARP- и DNS-запросы в сети Internet.

В случае использования распределенной ВС механизмов удаленного поиска существует возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать данные, использование которых приведет к адресации на атакующий ложный объект. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через ложный объект РВС.

Другой вариант внедрения в РВС ложного объекта использует недостатки алгоритма удаленного поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. В самом деле, атакующему для того, чтобы послать ложный ответ, не всегда обязательно дожидаться приема запроса (он может, в принципе, не иметь подобной возможности перехвата запроса). При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса, и тогда его ложный ответ будет немедленно иметь успех. Данная типовая удаленная атака чрезвычайно характерна для глобальных сетей, когда у атакующего из-за нахождения его в другом сегменте относительно цели атаки просто нет возможности перехватить поисковый запрос.

Ложный объект РВС - активное воздействие (класс 1.2), совершаемое с целью нарушения конфиденциальности (класс 2.1) и целостности информации (класс 2.2), которое может являться атакой по запросу от атакуемого объекта (класс 3.1), а также безусловной атакой (класс 3.3). Данная удаленная атака является как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), имеет обратную связь с атакуемым объектом (класс 4.1) и осуществляется на канальном (класс 6.2) и прикладном (класс 6.7) уровнях модели OSI.

15.3.4 Использование ложного объекта для организации удаленной атаки на систему

Получив контроль над проходящим потоком информации между объектами, ложный объект РВС может применять различные методы воздействия на перехваченную информацию. В связи с тем, что внедрение в распределенную ВС ложного объекта является целью многих удаленных атак и представляет серьезную угрозу безопасности РВС в целом, **выделяют нижерасмотренные методы воздействия на информацию, перехваченную ложным объектом.**

15.3.4.1 Селекция потока информации и сохранение его на ложном объекте системы

Одной из атак, которую может осуществлять ложный объект РВС, является перехват передаваемой между субъектом и объектом взаимодействия информации. Важно отметить, что факт перехвата информации (файлов, например) возможен из-за того, что при выполнении некоторых операций над файлами (чтение, копирование и т. д.) содержимое этих файлов передается по сети, а, значит, поступает на ложный объект. Простейший способ реализации перехвата - это сохранение в файле всех получаемых ложным объектом пакетов обмена.

Тем не менее, данный способ перехвата информации оказывается недостаточно информативным. Это происходит вследствие того, что в пакетах обмена кроме полей данных существуют служебные поля, не представляющие в данном случае для атакующего непосредственного интереса. Следовательно, для того, чтобы получить непосредственно передаваемый файл, необходимо проводить на ложном объекте динамический семантический анализ потока информации для его селекции.

15.3.4.2 Модификация информации

Одной из особенностей любой системы воздействия, построенной по принципу ложного объекта, является то, что она способна модифицировать перехваченную информацию. Следует особо отметить, что *это один из способов, позволяющих программно модифицировать поток информации между объектами РВС с другого объекта.* Ведь для реализации перехвата информации в сети необязательно атаковать распределенную ВС по схеме «ложный объект». Эффективней будет атака, осуществляющая анализ сетевого трафика, позволяющая получать все пакеты, проходящие по каналу связи, но, в отличие от удаленной атаки по схеме «ложный объект», она не способна к модификации информации.

Рассматривают два вида модификации информации. 1. Модификация передаваемых данных. В результате селекции потока перехваченной информации и его анализа система может распознавать тип

передаваемых файлов (исполняемый или текстовый). Соответственно, в случае обнаружения текстового файла или файла данных появляется возможность модифицировать проходящие через ложный объект данные. Особую угрозу эта функция представляет для сетей обработки конфиденциальной информации.

2. Модификация передаваемого кода. Ложный объект РВС, проводя семантический анализ проходящей через него информации, может выделять из потока данных исполняемый код. Известный принцип неймановской архитектуры гласит, что не существует различий между данными и командами. Следовательно, для того, чтобы определить, что передается по сети - код или данные, необходимо использовать определенные особенности, свойственные реализации сетевого обмена в конкретной распределенной ВС или некоторые особенности, присущие конкретным типам исполняемых файлов в данной локальной ОС.

Представляется возможным выделить два различных по цели вида модификации кода:

2.1 Внедрение в РПС разрушающих программных средств - при передачи в РПС исполняемый файл модифицируется по вирусной технологии: к исполняемому файлу одним из известных способов дописывается тело РПС, а также одним из известных способов изменяется точка входа так, чтобы она указывала на начало внедренного кода РПС. Описанный способ, в принципе, ничем не отличается от стандартного заражения исполняемого файла вирусом, за исключением того, что ***файл оказался поражен вирусом или РПС в момент передачи его по сети!***
Такое возможно лишь при использовании системы воздействия, построенной по принципу «ложный объект».

2.2 Изменение логики работы исполняемого файла - происходит модификация исполняемого кода с целью изменения логики его работы. Данное воздействие требует предварительного исследования работы исполняемого файла.

15.3.4.3 Подмена информации

Ложный объект позволяет не только модифицировать, но и подменять перехваченную им информацию. *При возникновении в сети определенного контролируемого ложным объектом события одному из участников обмена посылается заранее подготовленная дезинформация.* При этом такая дезинформация в зависимости от контролируемого события может быть воспринята либо как исполняемый код, либо как данные.

Рассмотрим пример подобного рода дезинформации. Предположим, что ложный объект контролирует событие, которое состоит в подключении пользователя к серверу. В этом случае он ожидает, например, запуска соответствующей программы входа в систему. В случае, если эта программа находится на сервере, то при ее запуске исполняемый файл передается на

рабочую станцию. Вместо того, чтобы выполнить данное действие, ложный объект передает на рабочую станцию код заранее написанной специальной программы - захватчика паролей. Эта программа выполняет визуально те же действия, что и настоящая программа входа в систему, например, запрашивая имя и пароль пользователя, после чего полученные сведения посылаются на ложный объект, а пользователю выводится сообщение об ошибке. При этом пользователь, посчитав, что он неправильно ввел пароль (пароль обычно не отображается на экране) снова запустит программу подключения к системе (на этот раз настоящую) и со второго раза получит доступ. Результат такой атаки - имя и пароль пользователя, сохраненные на ложном объекте.

15.3.5 Отказ в обслуживании

В общем случае в РВС каждый субъект системы должен иметь возможность подключиться к любому объекту РВС 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 РВС в сетевой ОС запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта. В случае получения запроса на соединение сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. Очевидно, что сетевая ОС способна отвечать лишь на ограниченное число запросов. Эти ограничения зависят от параметров ОС и ЭВМ, основными из которых являются быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи.

Различают три типа удаленных атак «отказа в обслуживании»:

- Если инфраструктура РВС позволяет с одного объекта системы передавать на другой атакуемый объект бесконечное число анонимных запросов на подключение от имени других объектов, то в этом случае будет иметь успех типовая удаленная атака **«Отказ в обслуживании»**. Результат применения этой удаленной атаки - нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, то есть невозможность получения удаленного доступа с других объектов РВС - отказ в обслуживании!
- Вторая разновидность этой типовой удаленной атаки состоит в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволяет пропускная способность канала связи (**направленный «шторм» запросов**). В этом случае, если в системе не предусмотрены 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.

- 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 воздействием (класс 1.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3), безусловно относительно цели атаки (класс 3.3). Данная УА является однонаправленным воздействием (класс 4.2), как межсегментным (класс 5.1), так и внутрисегментным (класс 5.2), осуществляемым на транспортном (класс 6.4) и прикладном (класс 6.7) уровнях модели OSI.

Соответствие рассматренных типовых удаленных атак классификации приведена в таблице 15.1.

Таблица 15.1 - Классификация типовых удаленных атак на РВС

Типовая удаленная атака													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 РВС	-	+	+	+	-	-	+	-	+	+	+	+	-	-	+	+	-	-	-
Внедрение в РВС ложного объекта путем навязывания ложного маршрута	-	+	+	+	+	-	-	+	+	+	+	+	-	-	+	-	-	-	-
Внедрение в РВС ложного объекта за счет недостатков алгоритмов удаленного поиска	-	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	-	-	-
Отказ в обслуживании	-	+	-	-	+	-	-	+	-	+	+	+	-	+	+	+	+	+	+

15.4 Анализ типовых уязвимостей позволяющих реализовать успешные удаленные атаки

Анализ механизмов реализации типовых УА и их практическое осуществление на примере сети Internet позволили сформулировать набор типовых уязвимостей и причин, по которым данные удаленные атаки оказались возможными. Особо отметим, что рассматриваемые ниже уязвимости основываются на *базовых принципах* построения сетевого взаимодействия объектов РВС.

Для устранения причин атак зачастую необходимо либо отказаться от определенных служб (DNS, например), либо изменить конфигурацию системы (наличие широковещательной среды приводит к возможности прослушивания канала, осуществляемого программным образом), либо изменить систему в целом. Все дело в том, что причины успеха удаленных атак данного типа кроются в инфраструктуре РВС, поэтому создание таксономии причин их успеха представляется весьма важной задачей, решение которой позволит выработать принципы построения защищенного взаимодействия в РВС.

Итак, рассмотрим возможные причины успеха УА на инфраструктуру и базовые протоколы распределенных ВС.

15.4.1 Отсутствие выделенного канала связи между объектами системы

Атака «Анализ сетевого трафика» заключается в прослушивании канала передачи сообщений в сети. Результат этой атаки во-первых, выяснение логики работы распределенной ВС и, во-вторых, перехват потока информации, которой обмениваются объекты системы. 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. Очевидно, что данная УА была бы программно невозможна, если бы у каждого объекта системы существовал для связи с любым другим объектом выделенный канал (вариант физического прослушивания выделенного канала не рассматривается, так как без специфических аппаратных средств подключение к выделенному каналу невозможно).

Следовательно, причина успеха данной типовой УА - наличие широковещательной среды передачи данных или отсутствие выделенного канала связи между объектами РВС.

15.4.2 Недостаточная идентификация и аутентификация объектов и субъектов системы

Как уже подчеркивалось, проблема идентификации и аутентификации субъектов и объектов РВС имеет чрезвычайно важное значение. От успеха ее решения зависит безопасность РВС в целом. Примеры успешно

осуществленных удаленных атак, доказывают, что отсутствие у разработчиков определенной заранее выработанной концепции и принципов идентификации объектов РВС в целом оставляют атакующему потенциальные возможности для компрометации объектов системы. Стандартными способами компрометации субъектов и объектов РВС являются:

- выдача себя за определенный объект или субъект с присвоением его прав и полномочий для доступа в систему (например, типовая УА «Подмена доверенного субъекта или объекта РВС»);
- внедрение в систему ложного объекта, выдающего себя за доверенный объект системы (например типовая УА «Ложный объект РВС»).

15.4.2.1 Взаимодействие объектов без установления виртуального канала

Одним из важнейших вопросов, на который необходимо ответить, говоря об идентификации/аутентификации объектов/субъектов РВС, является вопрос о видах взаимодействия между субъектами и объектами в распределенной ВС. Взаимодействие между субъектами и объектами РВС бывает двух видов:

- с использованием виртуального канала (ВК),
- без использования виртуального канала.

Практика показывает, что 99 % взаимодействия между объектами в сети Internet проходит с установлением ВК (при любом FTP-, TELNET-, HTTP- и т. п. подключении используется протокол TCP, а, следовательно, создается ВК). Это происходит из-за того, что взаимодействие по виртуальному каналу является единственным динамическим способом защиты сетевого соединения объектов РВС. Дело в том, что в процессе создания ВК объекты РВС обмениваются динамически вырабатываемой ключевой информацией, позволяющей уникально идентифицировать канал.

Таким образом, идентификация объектов РВС, при отсутствии статической ключевой информации, возможна только при взаимодействии объектов с использованием виртуального канала. Это, в свою очередь, означает, что взаимодействие объектов без установления ВК является одной из возможных причин успеха удаленных атак на РВС.

Но ошибочно считать распределенную вычислительную систему безопасной, даже если все взаимодействие объектов происходит с созданием ВК. Об этом речь пойдет в следующем пункте.

15.4.2.1 Использование нестойких алгоритмов идентификации объектов при создании виртуального канала

Ошибочно считать взаимодействие объектов по виртуальному каналу в РВС решением всех проблем, связанных с идентификацией объектов РВС.

ВК является необходимым, но не достаточным условием безопасного взаимодействия. Чрезвычайно важным в данном случае становится выбор алгоритма идентификации при создании ВК. Основное требование, которое следует предъявлять к данным алгоритмам, состоит в следующем: перехват ключевой информации, которой обмениваются объекты РВС при создании ВК не должен позволить атакующему получить итоговые идентификаторы канала и объектов. Это требование по сути очевидно. Оно должно предъявляться к алгоритмам идентификации исходя из принципиальной возможности прослушивания атакующим канала передачи. Однако в большинстве существующих сетевых ОС в базовых алгоритмах идентификации, используемых при создании ВК, этим требованием разработчики практически пренебрегают.

Так, например, в ОС Novell NetWare 3.12- 4.1 идентификатор канала - это число в диапазоне 0-FFh, идентификатор объекта (рабочей станции или файл-сервера) - также число от 0 до FFh; в протоколе TCP идентификаторами канала и объектов являются два 32-битных числа, формируемых в процессе создания TCP-соединения.

Из всего сказанного ясно, что создание виртуального канала с использованием нестойкого алгоритма идентификации не позволяет надежно обезопасить РВС от подмены объектов взаимодействия и выступает одной из причин успеха удаленных атак на распределенные вычислительные системы.

15.4.3 Отсутствие контроля за виртуальными каналами связи между объектами системы

Объекты РВС, взаимодействующие по виртуальным каналам, могут подвергаться типовой УА «Отказ в обслуживании». Особенность этой атаки состоит в том, что, действуя абсолютно легальными средствами системы, можно удаленно добиться нарушения ее работоспособности. Данная УА реализуется передачей множественных запросов на создание соединения (виртуального канала), в результате чего либо переполняется число возможных соединений, либо система, занятая обработкой ответов на запросы, вообще перестает функционировать.

Взаимодействие объектов РВС по виртуальным каналам позволяет единственным способом обеспечить защиту соединения в глобальной сети. Однако в использовании ВК есть как несомненные плюсы, так и очевидные минусы. К минусам относится необходимость контроля над соединением. При этом задача контроля распадается на две подзадачи:

- контроль за созданием соединения;
- контроль за использованием соединения.

Если задача контроля за использованием соединения решается довольно просто (обычно соединение разрывается по тайм-ауту, определенному системой - так сделано во всех известных сетевых ОС), то решение задачи контроля за созданием соединения представляется

нетривиальным. Именно отсутствие приемлемого решения этой задачи является основной причиной успеха типовой УА «Отказ в обслуживании». Сложность контроля над созданием ВК состоит в том, что в системе, в которой отсутствует статическая ключевая информация о всех ее объектах, невозможно отделить ложные запросы на создание соединения от настоящих. Очевидно также, что если ***один*** субъект сетевого взаимодействия будет иметь возможность ***анонимно*** занимать ***неограниченное*** число каналов связи с удаленным объектом, то подобная система может быть полностью парализована данным субъектом (пример - существующая сеть Internet в стандарте IPv4)! Поэтому, если любой объект в распределенной системе может анонимно послать сообщение от имени любого другого объекта (например, в Internet маршрутизаторы не проверяют IP-адрес источника отправления), то в подобной РВС в принципе невозможен контроль за созданием виртуальных соединений. Поэтому основная причина, по которой возможна типовая УА «Отказ в обслуживании» и ей подобные - это отсутствие в РВС возможности контроля за маршрутом сообщений.

15.4.4 Отсутствие возможности контроля за маршрутом сообщений

В РВС в качестве начальной идентифицирующей объект информации обычно выступает его адрес. Под адресом в РВС понимается определенная системой уникальная информация, которой он наделяется при внесении в систему. Все сообщения от других объектов РВС, адресованные на этот адрес, поступят на данный объект. Путь, или, маршрут сообщения определяется топологией РВС и проходит через совокупность узлов-маршрутизаторов. Следовательно, в каждом приходящем на объект РВС пакете может быть полностью отмечен его маршрут - список адресов маршрутизаторов, пройденных на пути к адресату. Этот отмеченный в пакете ***маршрут станет информацией, аутентифицирующей (подтверждающей) с точностью до подсети, подлинность адреса субъекта, отославшего сообщение***. Другой вариант аутентификации адреса отправителя - фильтрация маршрутизатором пакетов с неверным адресом отправителя.

Если в РВС не предусмотреть подобных возможностей 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 подобной РВС будет невозможно определить, откуда на самом деле пришло сообщение, а, следовательно, вычислить координаты атакующего (в сети Internet невозможно доступным способом вычислить инициатора однонаправленной удаленной атаки).

Таким образом, мы убеждаемся, что отсутствие в распределенной ВС возможности контроля за маршрутом сообщений порождает, во-первых,

невозможность контроля за созданием соединений, и, во-вторых, возможность анонимной отправки сообщения, следовательно является причиной успеха удаленных атак на РВС.

15.4.5 Отсутствие в системе полной информации о ее объектах

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. Такая ситуация характерна и вполне объяснима для сетей с разветвленной структурой.

Объясним это на простом примере. Предположим, что пользователь сети Internet решил подключиться, например, к WWW-серверу фирмы Novell. Он знает ее название, но не имеет информации об IP-адресе или имени ее сервера. В этом случае пользователь может послать широковещательный запрос всем хостам в сети с надеждой, что запрос дойдет до интересующего его сервера, и тот в ответ пришлет столь нужный для пользователя адрес. Очевидно, что в глобальной сети использование данной схемы по меньшей мере неразумно. Поэтому для подобных целей пользователь может подключиться к ближайшему известному ему поисковому серверу (***Altavista***, например) и послать запрос на поиск адреса интересующей его фирмы в базе данных информационного сервера.

Рассмотренный выше пример наглядно описывает возможные алгоритмы удаленного поиска, которые используют объекты РВС:

- когда поиск осуществляется внутри сегмента сети, субъект системы посылает широковещательный запрос, который получают все объекты РВС, и тот из них, для кого предназначался запрос, передает в ответ необходимую для адресации информацию.
- когда необходимо осуществить глобальный поиск, субъект распределенной системы посылает запрос на ближайший информационно-поисковый сервер, который, просканировав свою базу данных в поисках адреса запрашиваемого ресурса, либо отошлет в ответ на запрос найденный адрес, либо обратится к следующему в системе поисково-информационному серверу.

Таким образом, если в распределенной ВС существуют объекты, информация о которых не определена, то для обеспечения ее нормального функционирования необходимо использование описанных выше алгоритмов удаленного поиска.

Примером РВС с заложенной неопределенностью является сеть Internet, в которой, во-первых, у хостов, находящихся в одном сегменте, может не быть информации об аппаратных адресах друг друга, и, во-вторых, применяются непригодные для непосредственной адресации мнемонические

имена хостов, используемые для удобства пользователей при обращении к удаленным системам.

Очевиден тот факт, что в системе с заложенной в нее неопределенностью существуют потенциальные возможности внесения в систему ложного объекта и выдачи одного объекта системы за другой. Этот факт объясняется тем, что, являясь следствием неопределенности системы, алгоритмы удаленного поиска несут в себе потенциальную угрозу, состоящую в том, что на посланный запрос может прийти ложный ответ, в котором вместо информации о запрашиваемом объекте будет информация о ложном объекте. Вследствие этого распределенная ВС с заложенной неопределенностью является потенциально опасной системой и может подвергаться удаленным атакам.

15.4.6 Отсутствие криптозащиты сообщений

В РВС связь между объектами системы осуществляется по каналам связи. Поэтому всегда существует принципиальная возможность для атакующего 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 УА «Анализ сетевого трафика» является наиболее эффективным способом получения информации. Очевидна и причина, делающая эту атаку столь эффективной. Эта причина - передача по сети незашифрованной информации.

Использование криптостойких алгоритмов шифрования пакетов обмена между объектами РВС на канальном, прикладном уровнях делает анализ сетевого трафика практически бессмысленным. В случае канального шифрования, которое обычно выполняется аппаратно, по сети передаются полностью зашифрованные пакеты. В том случае, если в сети используются алгоритмы шифрования пакетов на сетевом - прикладном уровнях, то шифрация применяется только к полям данных пакетов соответствующих уровней, то есть заголовки пакетов, содержащие служебную информацию, не являются зашифрованными, поэтому атакующий имеет возможность, перехватив пакет, подвергнуть анализу данную служебную информацию.