ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Лебедева Т.Ф.

Безопасность распределенных вычислительных систем в Интернет

Особенности безопасности компьютерных сетей

- *Угроза* безопасности компьютерной системы - это потенциально возможное происшествие, неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней. Иначе говоря, угроза - это нечто плохое, что когда-нибудь может произойти.
- *Уязвимость* компьютерной системы - это некая ее неудачная характеристика, которая делает возможным возникновение угрозы. Именно из-за наличия уязвимостей в системе происходят нежелательные события.
- *Атака* на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака - это реализация угрозы.

Безопасность распределенных вычислительных систем в Интернет 2

Особенности безопасности компьютерных сетей

- Угроза *раскрытия* заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова "раскрытие" используются термины "кража" или "утечка.
- Угроза *целостности* включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности - деловые или коммерческие.
- Угроза *отказа в обслуживании* возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Безопасность распределенных вычислительных систем в Интернет

Особенности безопасности компьютерных сетей

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 (ВС), передаются по сетевым соединениям в виде пакетов обмена.

К сетевым системам наряду с обычными (локальными) атаками, осуществляемыми в пределах одной компьютерной системы, применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве.

Это так называемые сетевые (или *удаленные*) атаки.

Безопасность распределенных вычислительных систем в Интернет

Особенности безопасности компьютерных сетей

Удаленные атаки характерны тем:

1) что злоумышленник может находиться за тысячи километров от атакуемого объекта,

2) 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 ВС с точки зрения противостояния удаленным атакам приобретает первостепенное значение.

Специфика распределенных вычислительных систем (РВС) состоит в том, что если в локальных ВС наиболее частыми были угрозы раскрытия и целостности, то в *сетевых системах на первое место выходит угроза отказа в обслуживании*.

Безопасность распределенных вычислительных систем в Интернет

Особенности безопасности компьютерных сетей

Под *удаленной атакой (УА)* будем понимать информационное разрушающее воздействие на распределенную ВС, программно осуществляемое по каналам связи.

Это определение охватывает обе особенности сетевых систем - распределенность компьютеров и распределенность информации. Поэтому выделяются два подвида таких атак –

- удаленные атаки на инфраструктуру и протоколы сети и
- удаленные атаки на телекоммуникационные службы.

Первые используют уязвимости в сетевых протоколах и инфраструктуре сети,

а вторые - уязвимости в телекоммуникационных службах.

При этом под инфраструктурой сети понимается сложившаяся система организации отношений между объектами сети и используемые в сети сервисные службы.

Классификация компьютерных злоумышленников

Всех профессионалов, связанных с информационной безопасностью, разделяют на *хакеров* (*hackers*) и *кракеров* (*crackers*).

Самое главное и принципиальное различие между хакерами и кракерами состоит в *целях*, которые они преследуют.

Основные задачи хакера состоят в том, чтобы, исследуя вычислительную систему,

- обнаружить слабые места (уязвимости) в ее системе безопасности и *информировать* пользователей и разработчиков системы с целью последующего устранения найденных уязвимостей.
- проанализировав существующую безопасность вычислительной системы, сформулировать необходимые требования и условия повышения уровня ее защищенности.

Определение из словаря Guy L. Steele:

HACKER *сущ.* 1. Индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от расширения их возможностей, в отличие от большинства пользователей компьютеров, которые предпочитают знать только необходимый минимум.

2. Энтузиаст программирования; индивидуум, получающий удовольствие от самого процесса программирования, а не от теоретизирования по этому поводу.

Классификация компьютерных злоумышленников

Основная задача кракера состоит в непосредственном осуществлении взлома системы *с целью получения несанкционированного доступа* к чужой информации - иначе говоря, для ее кражи, подмены или для объявления факта взлома.

Кракер, по своей сути, ничем не отличается от обычного вора, взламывающего чужие квартиры и крадущего чужие вещи. Он взламывает чужие вычислительные системы и крадет чужую информацию.

Низменность мотивов кракеров приводит к тому, что 90% из них являются "чайниками", которые взламывают плохо администрируемые системы, в основном благодаря использованию чужих программ (обычно эти программы называются *exploit*).

Однако, было бы несправедливо смешать в одну кучу всех кракеров, однозначно назвав их ворами и вандалами

Кракеров можно разделить на три следующих класса в зависимости от цели, с которой осуществляется взлом:

- вандалы,
- «шутники»,
- взломщики (профессионалы).

Классификация компьютерных злоумышленников

Взломщики - профессиональные кракеры, пользующиеся наибольшим почетом и уважением в кракерской среде, основная задача которых - взлом компьютерной системы с серьезными целями, как то кража или подмена хранящейся там информации.

В общем случае, для того, чтобы осуществить взлом системы, необходимо пройти три основные стадии:

- исследование вычислительной системы с выявлением изъянов в ней
- разработка программной реализации атаки и
- непосредственное ее осуществление.

Естественно, настоящим профессионалом можно считать того кракера, который для достижения своей цели проходит все три стадии.

С некоторой натяжкой также можно считать профессионалом того кракера, который, используя добытую третьим лицом информацию об уязвимости в системе, пишет программную реализацию данной уязвимости. Осуществить третью стадию, очевидно, может в принципе каждый, используя чужие разработки.

Классификация компьютерных злоумышленников

- *"Шутники"* - наиболее безобидная часть кракеров (конечно, в зависимости от того, насколько злые они предпочитают шутки),

основная цель которых - известность, достигаемая путем взлома компьютерных систем и внесением туда различных эффектов, выражающих их неудовлетворенное чувство юмора.

"Шутники" обычно не наносят существенный ущерб (разве что моральный). На сегодняшний день в Internet это наиболее распространенный класс кракеров, обычно осуществляющих взлом Web-серверов, оставляя там упоминание о себе.
К "шутникам" также можно отнести создателей вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т.п.).

Все это, в принципе, либо невинные шалости начинающих, либо - рекламные акции профессионалов.

Классификация компьютерных злоумышленников

Вандалы - самая известная (во многом благодаря повседневности вирусов, а также творениям некоторых журналистов) и, надо сказать, самая малочисленная часть кракеров. Их основная цель - взломать систему для ее разрушения. К ним можно отнести,

- во-первых, любителей команд типа: rm -f -d *, del *.*, format c:/U и т.д.,
- во-вторых, специалистов в написании вирусов или "троянских коней". Совершенно естественно, что весь компьютерный мир ненавидит кракеров-вандалов лютой ненавистью. Эта стадия кракерства обычно характерна для новичков и быстро проходит, если кракеру удается совершенствоваться (ведь довольно скучно осознавать свое превосходство над беззащитными пользователями).

Кракеров, которые даже с течением времени не миновали эту стадию, а только все более совершенствовали свои навыки разрушения, иначе, чем социальными психопатами, не назовешь.

Законы УК РФ, связанные с «преступлениями в сфере компьютерной информации» (Глава 28 УК РФ)

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы, или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Законы УК РФ, связанные с «преступлениями в сфере компьютерной информации» (Глава 28 УК РФ)

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Законы УК РФ, связанные с «преступлениями в сфере компьютерной информации» (Глава 28 УК РФ)

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет.

Классификация удаленных атак на РВС

Удаленные атаки можно классифицировать по следующим признакам:

1*). По характеру воздействия*

- *пассивное (класс **1.1**)*
- *активное (класс **1.2**)*

Пассивным воздействием на РВС назовем воздействие, которое 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.

Под *активным* воздействием на распределенную ВС будем понимать воздействие, оказывающее непосредственное влияние на работу системы (изменение конфигурации РВС, нарушение работоспособности и т. д.) и нарушающее 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.

Классификация удаленных атак на РВС

2). По цели воздействия

- *нарушение конфиденциальности информации либо ресурсов системы (класс **2.1**)*
- *нарушение целостности информации (класс **2.2**)*
- *нарушение работоспособности (доступности) системы (класс **2.3**)*

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

Основная цель практически любой атаки - получить несанкционированный доступ 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. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием. Примером удаленной атаки, цель которой нарушение целостности информации, может служить типовая удаленная атака (УА) "Ложный объект РВС" .

Классификация удаленных атак на РВС

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.

Принципиально другой целью атаки является нарушение работоспособности 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" .

Классификация удаленных атак на РВС

3). По условию начала осуществления воздействия

Удаленное воздействие, также как и любое другое, может начать осуществляться только при определенных условиях. В распределенных ВС существуют три вида условий начала осуществления удаленной атаки:

- *Атака по запросу от атакуемого объекта (класс **3.1**)*

В этом случае атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия.

- *Атака по наступлению ожидаемого события на атакуемом объекте (класс **3.2**)*

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.

- *Безусловная атака (класс **3.3**)*

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.

Удаленные атаки на распределенные вычислительные системы

4). По наличию обратной связи с атакуемым объектом

- *с обратной связью (класс **4.1**)*
- *без обратной связи (однонаправленная атака) (класс **4.2**)*

5). По расположению субъекта атаки относительно атакуемого объекта

- *внутрисегментное (класс **5.1**)*
- *межсегментное (класс **5.2**)*

Данный классификационный признак позволяет судить о так называемой "степени удаленности" атаки.

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

Хост (host) - сетевой компьютер.

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

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.

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 на распределенные вычислительные системы

6). По уровню эталонной 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**)*

Международная Организация по Стандартизации (ISO) приняла стандарт ISO 7498, описывающий взаимодействие открытых систем (OSI). Распределенные ВС также являются открытыми системами. Любой сетевой протокол обмена, как и любую сетевую программу, можно с той или иной степенью точности спроецировать на эталонную семиуровневую модель OSI. Такая многоуровневая проекция позволит описать в терминах модели OSI функции, заложенные в сетевой протокол или программу. Удаленная атака также является сетевой программой.

В связи с этим представляется логичным рассматривать удаленные атаки на распределенные ВС, проецируя их на эталонную модель ISO/OSI.

Характеристика и механизмы реализации типовых удаленных атак

Понятие типовой удаленной атаки

Исследования и анализ ИБ различных РВС продемонстрировали тот факт, что, независимо от используемых сетевых протоколов, топологии, инфраструктуры исследуемых распределенных ВС, *механизмы реализации удаленных воздействий на РВС инвариантны по отношению к особенностям конкретной системы. Это объясняется тем, что распределенные ВС проектируются на основе одних и тех же принципов, а, следовательно, имеют практически одинаковые проблемы безопасности*.

Поэтому оказывается, что причины успеха УА на различные РВС одинаковы.

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

Введение этого понятия в совокупности с описанием механизмов реализации типовых УА позволяет предложить методику исследования безопасности, инвариантную по отношению к виду распределенной ВС. Методика заключается в последовательном осуществлении всех типовых удаленных воздействий в соответствии с предложенным далее их описанием и характеристиками.

При этом основным элементом исследования безопасности РВС является анализ сетевого трафика.

Характеристика и механизмы реализации типовых удаленных атак

1. Анализ сетевого трафика

Специфичное для распределенных ВС типовое удаленное воздействие, заключающееся 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 (если проводить дальнейшую аналогию с инструментарием хакера, то анализ трафика в этом случае заменяет и трассировщик). Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы РВС позволяет на практике моделировать и осуществлять типовые удаленные атаки.

2) *провести анализ сетевого трафика*.

Удаленная атака данного типа заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети.

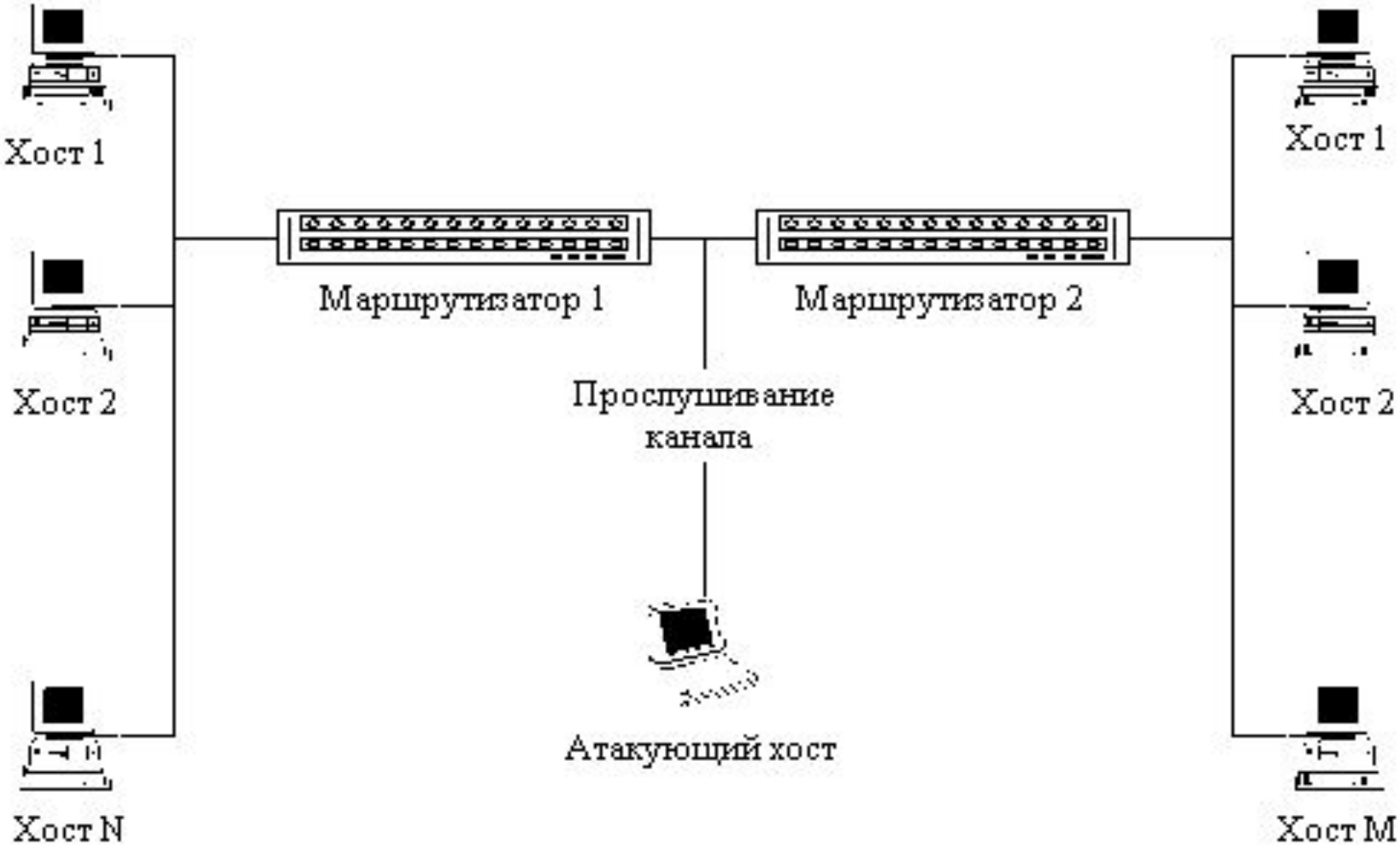


Рис. Схема атаки «Анализ сетевого трафика»

Характеристика и механизмы реализации типовых удаленных атак

1. Анализ сетевого трафика

Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен *только внутри одного сегмента сети*.

- по характеру воздействия является пассивным воздействием (класс **1.1**).
- ведет к нарушению конфиденциальности информации (класс **2.1**)
- начало осуществления атаки безусловно по отношению к цели атаки (класс **3.3**).
- осуществление данной атаки без обратной связи (класс **4.2**)
- внутри одного сегмента сети (класс **5.1**)
- на канальном уровне OSI (класс **6.2**).

Характеристика и механизмы реализации типовых удаленных атак

2. Подмена доверенного объекта или субъекта распределенной ВС

Одной из проблем безопасности распределенной ВС является *недостаточная идентификация и аутентификация ее удаленных друг от друга объектов*. 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 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.

Как известно, для адресации сообщений в распределенных ВС 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 распределенной ВС. Однако сетевой адрес достаточно просто подделывается и поэтому использовать его в качестве единственного средства идентификации объектов недопустимо.

Характеристика и механизмы реализации типовых удаленных атак

2. Подмена доверенного объекта или субъекта распределенной ВС

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 данной типовой удаленной атаки:

- *атака при установленном виртуальном канале,*

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*.

Характеристика и механизмы реализации типовых удаленных атак

2. Подмена доверенного объекта или субъекта распределенной ВС

- *атака без установленного виртуального канала.*

Атака заключается в передаче служебных сообщений от имени сетевых управляющих устройств, например, от имени маршрутизаторов.

Посылка ложных управляющих сообщений может привести к серьезным нарушениям работы распределенной ВС (например, к изменению ее конфигурации.

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**)
- как с обратной связью (класс **4.1**), так и без обратной связи (класс **4.2)** с атакуемым объектом
- может являться как внутрисегментной (класс **5.1**), так и межсегментной (класс **5.2**), и
- осуществляется на сетевом (класс **6.3**) и транспортном (класс **6.4**) уровнях модели OSI.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

Существуют две принципиально разные причины, обуславливающие появление типовой удаленной атаки "Ложный объект РВС":

1) В том случае, если в распределенной ВС 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.*

2) 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.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

1 стадия атаки

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

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

Основная цель атаки, связанной с навязыванием ложного маршрута, состоит в том, чтобы изменить исходную маршрутизацию на объекте распределенной ВС 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.

Для изменения маршрутизации атакующему необходимо послать по сети определенные данными протоколами специальные служебные сообщения от имени сетевых управляющих устройств (например, маршрутизаторов).

В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются два объекта распределенной ВС, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов РВС.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

Навязывание объекту РВС ложного маршрута –

- активное воздействие (класс **1.2**),
- совершаемое с любой из целей из класса **2** (**2.1** или **2.2** или **2.3**),
- безусловно по отношению к цели атаки (класс **3.3**)
- как с обратной связью (класс **4.1**), так и без обратной связи с атакуемым объектом (класс **4.2**)
- может осуществляться как внутри одного сегмента (класс **5.1**), так и межсегментно (класс **5.2**),
- на транспортном (класс **6.3**) и прикладном (класс **6.7**) уровне модели OSI.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

2. Внедрение в распределенную ВС ложного объекта путем использования недостатков алгоритмов удаленного поиска

В распределенной ВС 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.

1 вариант: 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.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

2 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.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

Типовая удаленная атака «Ложный объект РВС», использующая недостатки алгоритмов удаленного поиска –

- 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**)
- имеет обратную связь с атакуемым объектом (класс **4.1**)
- является как внутрисегментной (класс **5.1**), так и межсегментной (класс **5.2**),
- осуществляется на канальном (класс **6.2**) и прикладном (класс **6.7**) уровнях модели OSI.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

2 стадия атаки: **Использование ложного объекта для организации удаленной атаки на распределенную ВС**

Получив контроль над проходящим потоком информации между объектами, ложный объект РВС может применять различные методы воздействия на перехваченную информацию, перехваченную ложным объектом.

1. *Селекция потока информации и сохранение ее на ложном объекте РВС*

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.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

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.*

Два вида модификации информации:

- *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.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

- *модификация передаваемого кода.*

Ложный объект, проводя семантический анализ проходящей через него информации, может выделять из потока данных исполняемый код. Представляется возможным выделить два различных по цели вида модификации кода:

- внедрение РПС (разрушающих программных средств);

В первом случае при внедрении 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. *Файл оказался поражен вирусом или РПС в момент передачи его по сети.* Такое возможно лишь при использовании системы воздействия, построенной по принципу "ложный объект" . Конкретный вид РПС, его цели и задачи в данном случае не имеют значения, но можно рассмотреть, например, вариант использования ложного объекта для создания сетевого червя - наиболее сложного на практике удаленного воздействия в сетях, или в качестве РПС использовать сетевые шпионы.

Характеристика и механизмы реализации типовых удаленных атак

3. Ложный объект распределенной ВС

- изменение логики работы исполняемого файла.

Происходит модификация исполняемого кода с целью изменения логики его работы. Данное воздействие требует предварительного исследования работы исполняемого файла и, в случае его проведения, может принести самые неожиданные результаты. Например, при запуске на сервере (например, в ОС Novell NetWare) программы идентификации пользователей распределенной базы данных ложный объект может так модифицировать код этой программы, что появится возможность беспарольного входа с наивысшими привилегиями в базу данных.

3 Подмена информации

Если модификация информации приводит к ее частичному искажению, то подмена - к ее полному изменению. 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.

Характеристика и механизмы реализации типовых удаленных атак

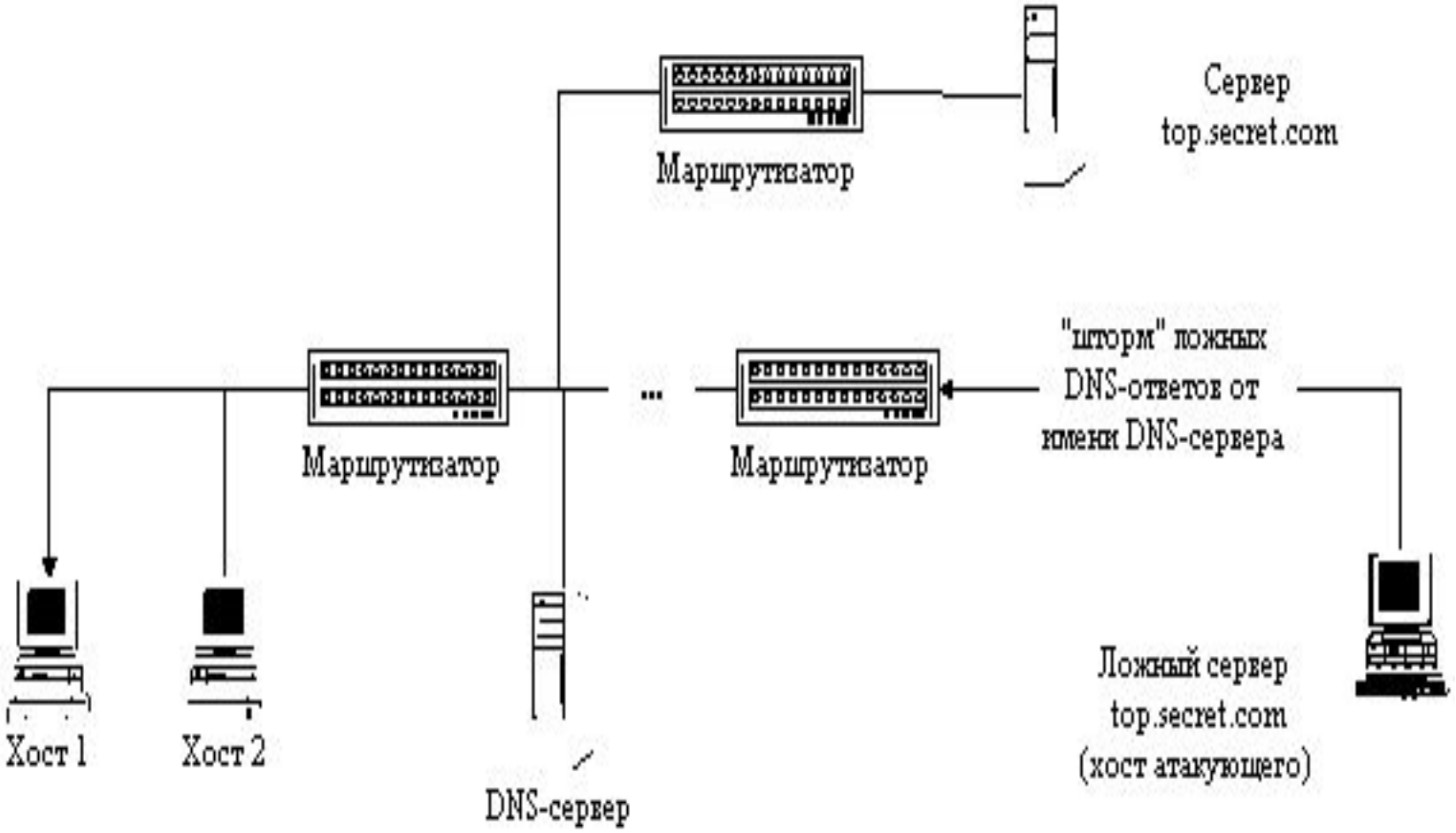
3. Ложный объект распределенной ВС

Рассмотрим пример подобного рода дезинформации.

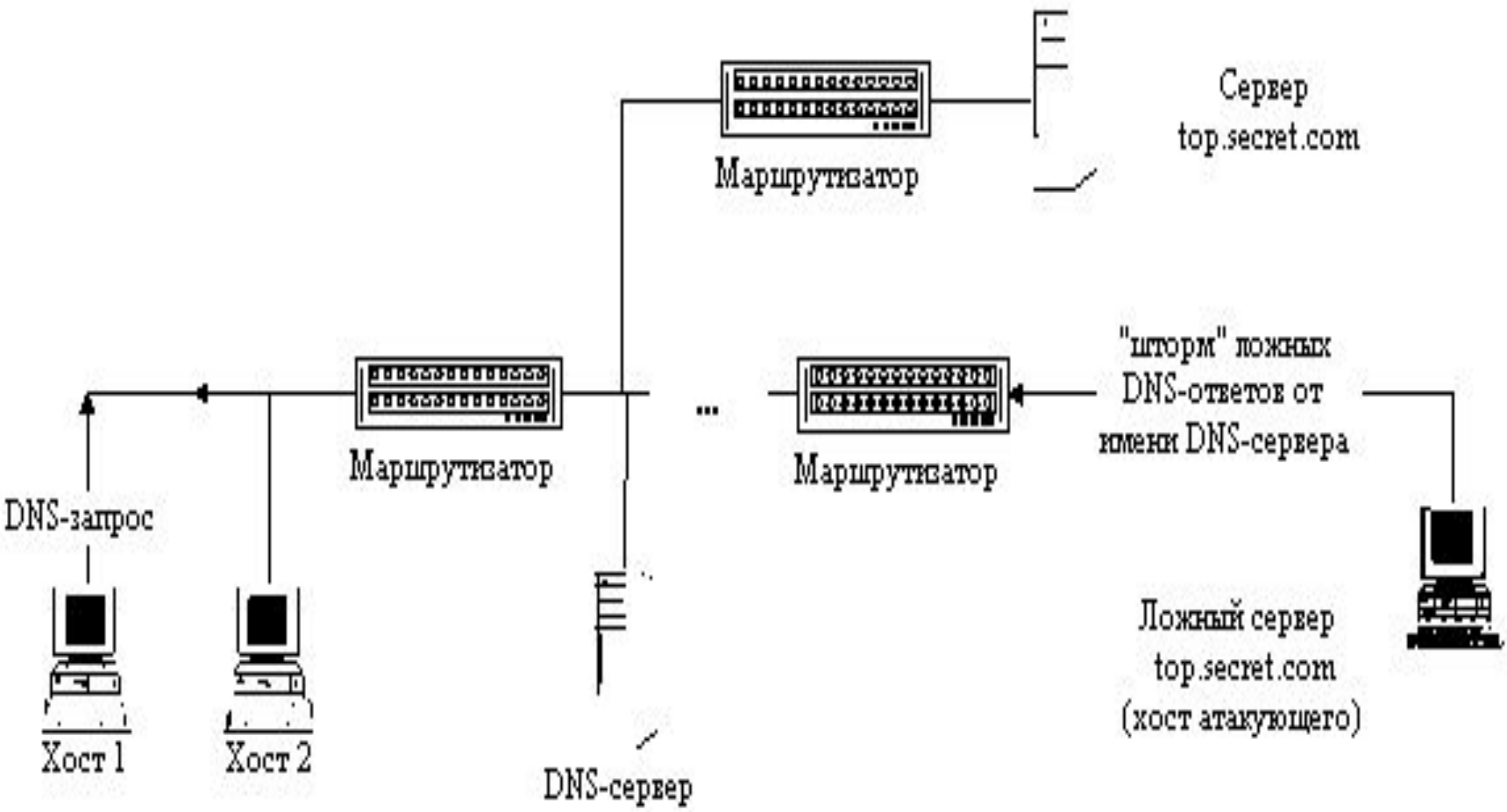
Предположим, что ложный объект контролирует событие, которое состоит в подключении пользователя к серверу. В этом случае он ожидает, например, запуска соответствующей программы входа в систему.

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.

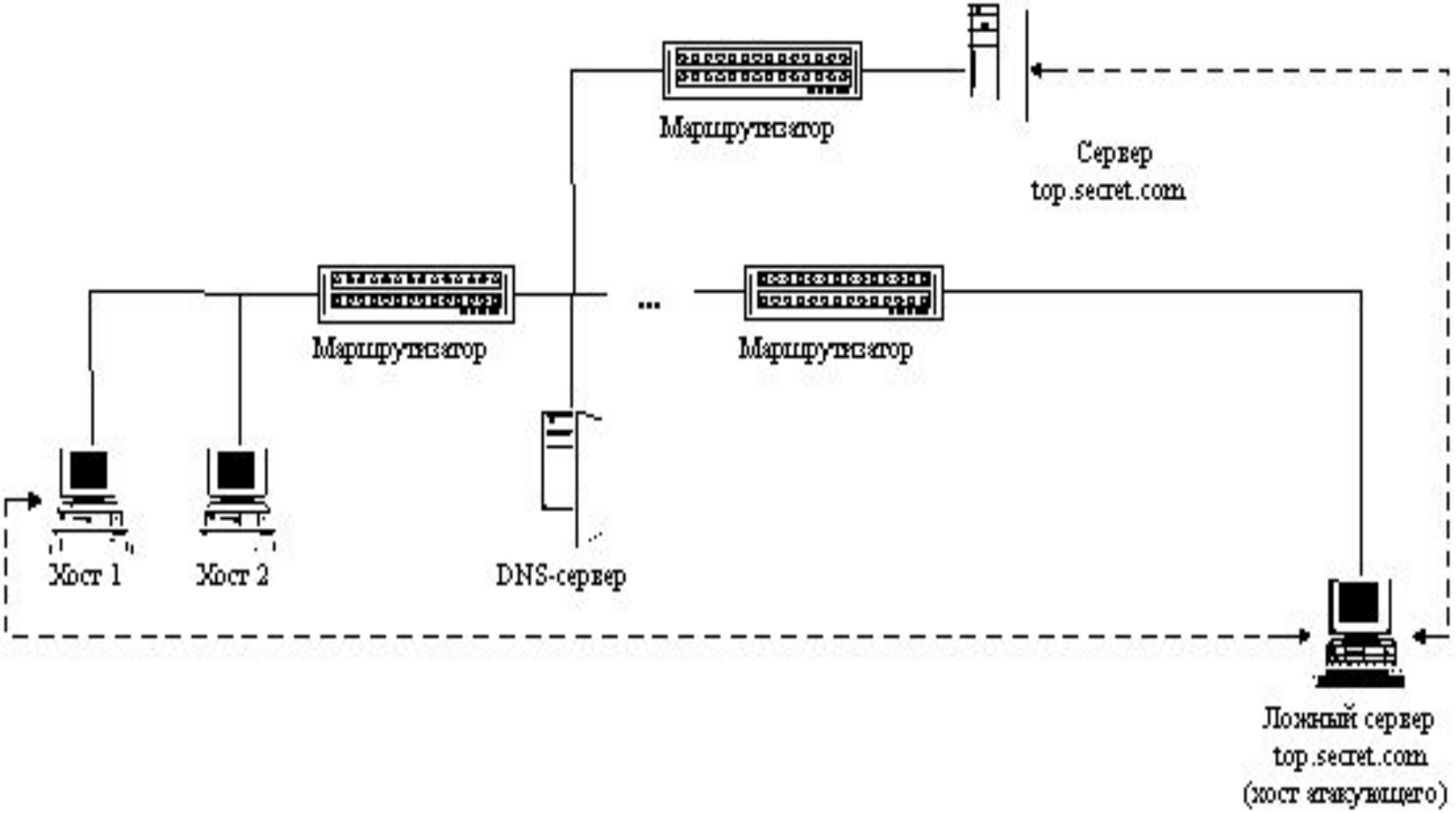
Эта программа выполняет визуально те же действия, что и настоящая программа входа в систему, например, запрашивая имя и пароль пользователя, после чего полученные сведения посылаются на ложный объект, а пользователю выводится сообщение об ошибке. При этом пользователь, посчитав, что он неправильно ввел пароль 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.



Пример: Внедрение в Internet ложного сервера путем создания направленного "шторма" ложных DNS-ответов на атакуемый хост.
Атакующий создает направленный "шторм" ложных DNS-ответов на Хост 1.



Пример: Внедрение в Internet ложного сервера путем создания направленного "шторма" ложных DNS-ответов на атакуемый хост.
Хост 1 посылает DNS-запрос и немедленно получает ложный DNS-ответ



Пример: Внедрение в Internet ложного сервера путем создания направленного "шторма" ложных DNS-ответов на атакуемый хост.

Фаза приема, анализа, воздействия
и передачи перехваченной информации на ложном сервере.

Характеристика и механизмы реализации типовых удаленных атак

4. Отказ в обслуживании

Одной из основных задач, возлагаемых на сетевую ОС, функционирующую на каждом из объектов распределенной ВС, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту.

В общем случае в распределенной ВС 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:

1) 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. Данные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа.
2) задача сервера состоит в том, чтобы, находясь в памяти операционной системы объекта РВС, постоянно ожидать получения запроса на подключение от удаленного объекта.
3) в случае получения подобного запроса сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет.

Характеристика и механизмы реализации типовых удаленных атак

4. Отказ в обслуживании

По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты РВС. В этом случае непосредственно ядро сетевой ОС обрабатывает приходящие извне запросы на создание виртуального канала (ВК) и передает их в соответствии с идентификатором запроса (порт или сокет) прикладному процессу, которым является соответствующий сервер.

Очевидно, что сетевая операционная система способна иметь *только ограниченное число открытых виртуальных соединений и отвечать лишь на ограниченное число запросов.* Эти ограничения зависят от таких параметров системы как *быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи* (чем она выше, тем больше число возможных запросов в единицу времени).

1 разновидность атаки. При отсутствии статической ключевой информации в РВС идентификация запроса возможна только по адресу его отправителя. Если в распределенной ВС не предусмотрено средств аутентификации адреса отправителя, то есть 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".

Характеристика и механизмы реализации типовых удаленных атак

4. 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.

2 разновидность атаки состоит в передаче с *одного адреса такого количества запросов на атакуемый объект, какое позволит трафик (направленный "шторм" запросов).* 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.

3 разновидность атаки - 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 и т. п.

Характеристика и механизмы реализации типовых удаленных атак

4. Отказ в обслуживании

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**).
- 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.

Причины успеха удаленных атак на РВС и сеть Internet

1. Отсутствие выделенного канала связи между объектами РВС

Выше была рассмотрена типовая УА "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. 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.

Причины успеха удаленных атак на РВС и сеть Internet

2 Недостаточная идентификация и аутентификация объектов и субъектов РВС

Как уже подчеркивалось выше, проблема идентификации и аутентификации субъектов и объектов РВС имеет чрезвычайно важное значение. От успеха ее решения зависит безопасность распределенной ВС в целом. 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").

Причины успеха удаленных атак на РВС и сеть Internet

3 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.

Но ошибочно считать распределенную вычислительную систему безопасной, даже если все взаимодействие объектов происходит с созданием ВК.

Причины успеха удаленных атак на РВС и сеть Internet

4 Использование нестойких алгоритмов идентификации объектов при создании виртуального канала

Ошибочно считать взаимодействие объектов по виртуальному каналу (ВК) в распределенной ВС панацеей от 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 .

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.

Причины успеха удаленных атак на РВС и сеть Internet

5 Отсутствие контроля за виртуальными каналами связи между объектами РВС

Объекты распределенной ВС, 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.

Напомним, что, 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.

В предыдущем пункте было показано, что 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;*

Причины успеха удаленных атак на распределенные вычислительные системы и сеть Internet

5 Отсутствие контроля за виртуальными каналами связи между объектами РВС

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. 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.

- *контроль за использованием соединения.*

Задача решается довольно просто (обычно соединение разрывается по тайм-ауту, определенному системой - так сделано во всех известных сетевых ОС).

Причины успеха удаленных атак на РВС и сеть Internet

6 Отсутствие в РВС возможности контроля за маршрутом сообщений

В распределенных ВС в качестве начальной идентифицирующей объект информации обычно выступает его адрес. Теперь все сообщения от других объектов РВС, адресованные на этот адрес, поступят на данный объект.

Путь, или, как принято говорить, 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 .

Причины успеха удаленных атак на РВС и сеть Internet

6 Отсутствие в РВС возможности контроля за маршрутом сообщений

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).

Отсутствие в распределенной ВС возможности контроля за маршрутом сообщений порождает

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

Причины успеха удаленных атак на РВС и сеть Internet

7 Отсутствие в РВС 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.

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.

.

Причины успеха удаленных атак на РВС и сеть Internet

8 Отсутствие в РВС криптозащиты сообщений

В распределенных ВС 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.

Вопросы?