27.02.17

Методы и средства ЗИ в сети интернет

**К типовым угрозам безопасности при использовании глобальных КС относятся:**

1. Анализ сетевого трафика
2. Подмена субъекта или объекта сети
3. Внедрение ложного объекта сети
4. Отказ в обслуживании

**Основные причины, облегчающие нарушителю реализацию угроз Б информации в распределенных КС:**

1. Отсутствие выделенного канала связи между объектами распределенной КС
2. Возможность взаимодействия объекта распределенной КС без установления виртуального канала между ними, что не позволяет надежно идентифицировать объект или субъект распр. КС
3. Использование недостаточно надежных протоколов аутентификации объекта распр. КС
4. Отсутствие контроля создания и использования виртуальных каналов между объектами распр. КС
5. Отсутствие возможности контроля маршрута получаемых сообщений, что не позволяет подтвердить адрес отправителя данных
6. Отсутствие полной информации об объектах КС с которыми требуется создать соединение, что в ряде случаев приводит к необходимости отправки широковещательного запроса
7. Отсутствие шифрования передаваемых сообщений

**Основные методы создания безопасных КС:**

1. Использование выделенных каналов связи путем физического соединения каждой пары объектов распр. КС
2. Разработка дополнительных средств идентификации объектов распр. КС перед созданием виртуального канала между ними
3. Контроль маршрута поступающих сообщений
4. Контроль создания и использования виртуального соединения между объектами распр. КС
5. Разработка распр. КС с полной информацией об ее объектах
6. Применение средств шифрования

Одним из вариантов защиты от перечисленных угроз является технология виртуальных частных сетей. Подобно созданию выделенного канала связи VPN позволяют установить защищенное цифровое соединение между двумя участниками и создать глобальную сеть из существующих локальных сетей. Трафик VPN передается поверх IP трафика и использует в качестве протокола транспортного уровня дейтаграммы.

Существую аппаратные и программные решения VPN. К аппаратным относятся криптомаршрутизаторы:

Интернет

А

К1

В

Х

К2

У

Рис. – VPN на криптомаршрутизаторах

**Алгоритм работы криптомаршрутизатора К1 при передаче пакета данных от рабочей станции А к раб. Станции Х:**

1. По таблице маршрутов определяется адрес криптомаршрутизатора, которая обслуживает подсеть, содержащую получателя пакета
2. Определяется интерфейс, через который доступна подсеть, содержащая криптомаршрутизатор К2
3. Выполняется шифрование всего пакета на сеансовом ключе связи К1 и К2, извлеченном из таблицы маршрутов
4. К полученному пакету добавляется заголовок, содержащий IP-адрес К1 в качестве адреса отправителя и IP-адреса К2 в качестве адреса получателя
5. Сформированный пакет отправляется через Интернет

В рассмотренном варианте защиты достигается полная прозрачность работы криптомаршрутизатора для функционирования любого сетевого ПО, использующего сеть протоколов TCP/IP. Обеспечивается скрытость адресного пространства подсетей организации и его независимость от адресов в сети Интернет.

Степень защиты передаваемой информации полностью определяется стойкостью ко взлому используемой функции шифрования.

При работе с большим числом подключаемых подсетей необходимо выделение специального криптомаршрутизатора с функциями центра распределения ключей (ЦРК) шифрования для связи между парами криптомаршрутизатора, которые в этом случае могут работать в двух режимах: загрузке конфигурации и основном и имеют на защищенном носителе один маршрут и один ключ шифрования (мастер ключ – для связи с ЦРК).

После успешной установки соединения криптомаршрутизатора с ЦРК ему высылается его таблица маршрутов, зашифрованная мастер-ключом.

После получения и расшифрования таблицы маршрутов криптомаршрутизатор переходит в основной режим работы.

**Программные средства построения VPN могут обеспечивать защищенную связь между двумя объектами сети на различных уровнях взаимодействия сетей:**

1. На канальном. С использованием протоколов PPTP, L2TP, L2F. На этом уровне VPN обычно используют для соединения удаленного компьютера с одним из серверов ЛВС (Локальной Вычислительной Сети)
2. На сетевом. С использованием протоколов SKIP, IPSec. На этом уровне VPN могут использоваться для соединения двух ЛВС или для соединения удаленного компьютера и сервера
3. На сеансовом. С использованием протоколов SSL, TLS, SOCKS. VPN на этом уровне создаются поверх VPN На других уровнях.

Программные средства построения VPN создают так называемый тоннель, по которому передаются шифрованные данные.

Протокол SKIP

Заголовок SKIP пакета является стандартным IP заголовком. SKIP шифрует IP пакеты ничего не зная о приложениях, пользователях, процессах и их формирующих. Он обрабатывает весь трафик без ограничений на вышележащее ПО. SKIP не зависим от сеанса.

SKIP основан на алгоритме Диффи-Хелмана.

Протокол IPSec

Разделяют на три большие части:

* AH. Протокол заголовка аутентификации AH предназначен для защиты от атак, связанных с несанкционированным изменением содержимого пакета, в том числе от подмены адреса отправителя.
* ESP. Протокол инкапсуляции зашифрованные данных ESP предназначен для обеспечения конфиденциальности данных. Необязательная опция аутентификации в протоколе дополнительно позволяет повысить контроль целостности данных.
* ISAKMP. Протокол используется для управления параметрами защищенных связей и криптографическими ключами

Процесс соединения IPSec разделяют на две фазы:

1. Узел IPSec устанавливает подключение к удаленному узлу или сети. Удаленный узел или сеть проверяет учетные данные запрашивающего узла и обе стороны согласуют способ проверки подлинности, используемый для соединения.
2. Между узлами IPSec создается ассоциация безопасности SA. Пи этом в БД SA, которая еще называют областью интерпретации (DOI), вносится информация о конфигурации соединения.

Протокол ISAKMP определяет основу для установления SA и не связан с какими-либо крипторафическими алгоритмами.

Протокол Oakley

Для устранения недостатков алгоритма Диффи-Хелмана разработан протокол Oakley (Атаки засорения, человек посередине)

Основная идея: Каждая сторона должна в начальном сообщении отправить рецепт, который другая сторона должна подтвердить своим ответным сообщением (если IP-адрес отправителя был подменен, то нарушитель не получит подтверждающего сообщения, не сможет правильно составить свое подтверждение и загрузить узел бессмысленной работой)

**Требования к рецепту:**

1. Он должен зависеть от параметров генерирующей стороны
2. Генерирующий рецепт узел должен использовать при этом локальную секретную информацию без необходимости хранения копий уже отправленных рецептов
3. Генерация и проверка рецептов должны выполняться достаточно быстро

Протокол Oakley так же поддерживает использование групп. В этом случае в каждой группе определяются два глобальных параметра (Части открытого ключа) и криптографический алгоритм (Диффи-Хелмана или основанные на эллиптический кривых). Для защиты от атак воспроизведения применяются оказии (случайные числа), которые появляются в ответных сообщениях и на определенных шагах шифруются.

**Для взаимной аутентификации сторон в Oakley могут использоваться:**

1. Механизм ЭЦП для подписания доступного обеим сторонам хэш-значения
2. Ассиметричное шифрование идентификаторов и оказий закрытым ключом
3. И т.д.

**Обмен по протоколу Oakley:**

1. A -> B: RA - рецепт, тип, G - группа, CA - предлагаемые криптоалгоритмы, А, В - адреса, NA – оказия, ESKA(H(A, B, NA, G, CA)) - ЭЦП
2. B -> A : RB, RA, тип, G, CB – выбранный криптоалгоритм, B, A, NB, NA, ESKB(H(B, A, NB, NA, G, CB))
3. A -> B : RA, RB, тип, G, CB, А, В, NA, NB, ESKA(H(A, B, NA, NB, G, CB))

Формат заголовка протокола AH

|  |  |  |
| --- | --- | --- |
| Следующий заголовок | Длина | Зарезервировано |
| Индекс параметра безопасности | | |
| Поле последовательного номера | | |
| Данные аутентификации | | |