Эссе по курсу защита информации
студента 011 гр. Сафонова А.А.

Удержание VPN tunnel мобильным пользователем

Удержание VPN tunnel мобильным пользователем

Большинство компаний сегодня используют различные формы VPN (Virtual Private Network) для безопасного доступа к корпоративным ресурсам через Интернет. VPN-канал обычно ассоциируется с IP-адресом устройства. Это составляет проблему для мобильного пользователя, потому что IP-адрес его устройства меняется каждый раз, когда пользователь меняет подсеть в процессе движения. Реализованные в настоящий момент версии VPN предполагают пользователю пройти процедуры аутентификации и распределения ключей заново и установить новое VPN соединение. Так, например, протокол IKE (Internet Key Exchange) должен быть полностью выполнен заново, и установлен новый IPSec tunnel. В условиях, когда пользовательское устройство не обладает большой вычислительной мощностью (а мобильные устройства чаще всего именно такие) и wireless-соединение достаточно медленно, все процедуры аутентификации отнимают значительное время, что особенно ощутимо для real-time приложений. В настоящем эссе на примере IPSec и IKE-protocol излагается простой и эффективный способ (один из авторов Yi Cheng; метод был предложен на шестой международной конференции по беспроводным технологиям в Японии в 2003г) удержать уже установленное безопасное соединение, несмотря на то, что IP-адрес устройства поменялся. Основная идея метода состоит в том, чтобы *динамически* ассоциировать IP-адрес устройства с уже установленной сессией безопасного соединения. Вместо того чтобы повторять процедуры IKE-protocol, достаточно обменяться парой коротких сообщений, что существенно повышает производительность и экономит время и трафик.

1. Введение

VPN (Virtual Private Network) каналы широко используются мобильными пользователями для безопасного доступа к корпоративным ресурсам через Интернет. VPN-канал устанавливается между пользовательским устройством и безопасным шлюзом, который соединяет корпоративную сеть с внешним миром. И, казалось бы, VPN-канал не должен обрываться и для мобильного пользователя, ведь оба конца канала: удаленное устройство и шлюз - остались теми же самыми. Но на практике, каждый раз, когда пользователь перемещается из одной подсети в другую, приходится устанавливать VPN-канал заново. Так происходит, потому что канал привязывается к IP-адресу пользовательского устройства, который меняется вместе с подсетью. Например, в IPSec безопасная сессия характеризуется тремя параметрами: Security Parameter Index (SPI), IP Destination Address, Security Protocol (AH или ESP). Каждый раз, когда пользовательское устройство получает новый адрес, установленная сессия уничтожается.

Поэтому мобильному пользователю придется периодически выполнять соединение заново. Но даже если пользователь не движется, IP-адрес его устройства все равно может поменяться. Так произойдет если, к примеру, пользователь переключится на другую технологию доступа: например, с GPRS на Wireless LAN, чтобы работать с большей скоростью. И тогда все равно придется «переустанавливать» VPN соединение.

Установка VPN соединения подразумевает выполнение процедур аутентификации и распределения ключей. Например, процедуры IKE (Internet Key Exchange) protocol должны быть полностью повторены, чтобы установить новый IPSec канал. Эти процедуры занимают много времени. Небольшая пропускная способность беспроводных сетей и скромная вычислительная мощность мобильного устройства усугубляют ситуацию. Так, например, с GPRS соединением процедуры протокола IKE занимают 4-6 се-

кунд! Поэтому пользовательские приложения, особенно чувствительные к задержкам в работе сети, могут дать серьезные сбои.

2. Динамическая привязка IP-адреса

Для того чтобы избежать повторной установки VPN-канала, можно предложить *динамически* «привязывать» IP-адрес мобильного устройства к уже установленной безопасной сессии (security associations) защищенным способом.
Перед тем, как установить VPN-канал, мобильный пользователь и корпоративный шлюз должны аутентифицировать друг друга. При этом устанавливается безопасная сессия (security associations). Следует подчеркнуть, что аутентифицируется именно пользователь, а не его устройство. Это подразумевает, что в процедуре не фигурирует текущий IP-адрес мобильного устройства. Следовательно, с сессией можно ассоциировать разные адреса, по крайней мере, до тех пор, пока пользователю не будет отказано в аутентификации.

После успешной аутентификации мобильное устройство и корпоративный шлюз устанавливают безопасное соединение, в процессе которого «договариваются» о деталях IP-уровня сессии. Только тогда происходит привязка сессии к текущему IP-адресу мобильного устройства. Идея динамической привязки состоит в том, чтобы позднее, когда IP-адрес устройства изменится, устройство послало специальное сообщение по тому же защищенному каналу корпоративному шлюзу (шлюз-то никуда не двигался и защищенный канал, ведущий к нему, все еще существует). Получив это сообщение, удаленный шлюз должен обновить привязку сессии к IP-адресу.

Чтобы такая схема работала должны быть выполнены следующие условия:

- Должна использоваться аутентификация *пользователя*, а не устройства.
- Установленный защищенный канал после аутентификации не должен быть жестко привязан к IP-адресу мобильного устройства. В противном случае, после смены IP-адреса, канал будет более недоступен.
- Специальное сообщение об обновлении привязки должно быть аутентифицировано и защищено от re-play атаки.

Т.к. IPSec одно из наиболее распространенных VPN решений, в дальнейшем будет обсуждать именно эта реализация VPN канала. Хотя, тот же подход может быть использован и для других реализаций.

2.1 IKE и IKE Config

IKEv1

Протокол IKE, как описано в RFC 2409, состоит из двух частей. В первой части две стороны (peers) аутентифицируют друг друга и устанавливают защищенный канал. При этом устанавливается безопасная сессия (security associations), которая называется ISAKMP SA. Во второй части по установленному защищенному каналу стороны «договариваются» о деталях IPSec или другого сервиса. Привязка нового IP-адреса может происходить в любое время после этих переговоров по установленному в первой части защищенному каналу.

IKE Config

IKE Config – это межсетевой шаблон (draft), представляющий способ использования канала ISAKMP SA для безопасного обмена конфигурационной информацией в рамках IKEv1. Обычно IKE Config используется для передачи мобильным устройствам внутрисетевых параметров, таких как свободные IP-адреса, адреса DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), etc. Эта информация передается в специальных полях шаблона.

IKEv2

Эта версия IKE protocol намного проще и удобнее, чем IKEv1. В ней восемь возможных сценариев, определенных в IKEv1, объединены всего в 4 инициализирующих сообщения. IKEv2 позволяет устанавливать дочерние сессии (security associations) на этапе инициализации. IKEv2 включает поддержку NAT, расширенную аутентификацию (extended authentication) и некоторые другие дополнительные возможности.

Т.к. IKEv1 распространен все еще гораздо шире, чем IKEv2, проиллюстрируем возможность динамической привязки IP-адреса с помощью IKE Config.

2.2 Configuration Exchange

Допустим, мобильное устройство и корпоративный шлюз установили IPSec канал, используя протокол IKE. В некоторый момент IP-адрес устройства меняется. Если мобильное устройство хочет удержать установленную сессию, оно инициализирует процедуру configuration exchange, посылая специальное сообщение AddrUpdateRec шлюзу (рис. 1). Это сообщение содержит необходимые для configuration exchange заголовки (ISAKMP Header), хеш-функцию (Hash Payload) и набор передаваемых атрибутов (Attribute Payload). Для наших целей нужно взять в качестве атрибутов идентификатор пользователя (User ID), старый IP-адрес мобильного устройства и новый IP-адрес.

При получении такого сообщения (AddrUpdateRec) корпоративный шлюз «поднимает» уже установленную сессию, основываясь на информации cookies в заголовке ISAKMP Header. Шлюз расшифровывает остальную часть сообщения и аутентифицирует его, проверяя хеш-функцию (Hash Payload). Кроме того, шлюз проверяет, правильные ли идентификатор пользователя и старый IP-адрес его устройства. В случае если настройки Corporate Security Policy допускают динамическую привязку IP-адреса, шлюз отвечает подтверждающим сообщением AddrUpdateAck. Это сообщение содержит новый IP-адрес в поле передаваемых атрибутов (Attribute Payload). Затем шлюз ассоциирует существующую сессию (IPSec Security Associations) с новым IP-адресом и меняет адрес в списке сессий (Security Associations Database). С этого момента мобильное устройство может продолжать «общаться» с корпоративным шлюзом.

В случае если аутентификация сообщения завершилась неудачей, шлюз должен игнорировать сообщение, и продолжать работать как прежде, с прежним IP-адресом.

В случае если шлюз отклоняет сообщение, следуя политике безопасности, или потому что истекло время жизни сессии, в ответ посылается сообщение AddrUpdateAck с пустым IP-адресом. Получив такое сообщение, мобильное устройство знает, что новый IP-адрес не был подтвержден корпоративным шлюзом, и в этом случае, устройству придется устанавливать новую сессию.

Шлюз должен сверять новый IP-адрес, указанный в сообщении, с адресом отправителя этого сообщения (source address). Эти адреса могут не совпадать в двух случаях. Воз-

можно, это злоумышленник перехватил сообщение и изменил у него адрес отправителя, пытаясь провести denial-of-service (DOS) атаку. В этом случае нужно игнорировать адрес отправителя и привязывать указанный в сообщении IP-адрес к установленной сессии.

Но адреса могут не совпадать и в случае, если используется технология NAT (Network Address Translation). Если мобильное устройство попадает в сеть, которая использует локальные IP-адреса, то IP-адрес устройства невидим для удаленного сервера, потому что NAT подменяет локальный адрес отправителя некоторым публичным IP-адресом. В этом случае указанный в сообщении IP-адрес бесполезен, и нужно привязывать к установленной сессии адрес отправителя. Минус такого решения заключается в том, что попытка несанкционированного доступа окажется успешной (об этом подробнее в следующем разделе).

Если шлюз не может определить, используется ли технология NAT или нет (например, она не поддерживается), нужно отклонить запрос на динамическую привязку IP-адреса.

2.3 Анализ защищенности

Динамическая привязка IP-адреса создает дополнительные риски для безопасности соединения. Они заключаются в том, что злоумышленник может попытаться подделать новый IP-адрес мобильного устройства и перехватить сессию.

Но сообщение AddrUpdateReq зашифровано (кроме заголовка), кроме того, отслеживается его целостность. Поэтому без знания ключа, который был сгенерирован в первой части IKE protocol, невозможно незаметно подделать это сообщение. Невозможно также провести re-play атаку, т.к. в хеш-функции сообщения содержится постоянно увеличивающийся счетчик сообщений.

Что реально может сделать злоумышленник, так это изменить адрес отправителя сообщения AddrUpdateReq (source address). Успех подобной атаки зависит от того, используется ли технология NAT. Если NAT не используется, и в сообщении указан реальный IP-адрес, то именно его шлюз и привяжет к установленной безопасной сессии. Измененный злоумышленником адрес отправителя будет просто проигнорирован шлюзом. Таким образом, атака не даст результатов.

Если же технология NAT используется, то шлюзу придется обращать внимание на адрес отправителя сообщения AddrUpdateReq. И в случае, если он был изменен злоумышленником, шлюз привяжет именно его к безопасной сессии пользователя. Сами пакеты закодированы, и злоумышленнику никакой пользы не принесут. Но мобильный пользователь потеряет сессию, и ему придется заново устанавливать VPN-канал. Таким образом, единственным результатом атаки может стать потеря соединения пользователем.

2.4 Производительность

Без динамической привязки адресов мобильное устройство вынуждено повторять, по крайней мере, вторую часть протокола IKE. Большинство же приложений выполняет и первую часть этого протокола тоже. Вторая часть включает синхронизацию сессий, генерацию ключей и т.д. Эти процедуры могут отнять гораздо больше времени у мобильного устройства с небольшими вычислительными возможностями, чем можно

предположить. Как указывалось ранее, с GPRS соединением, например, инструкции протокола IKE занимают 4-6 секунд.
Предложенная же схема намного проще. Только два коротких сообщения (один раунд) необходим, чтобы продолжить работу. И оба эти сообщения короткие. В сравнении со второй частью протокола IKE configuration exchange отнимает гораздо меньше времени и вычислений.

3. Заключение

В данном эссе предлагается безопасный способ динамически привязать IP-адрес мобильного устройства к установленной безопасной сессии VPN соединения. Это позволяет избежать выполнения длительных процедур аутентификации и распределения ключей, требуемых при установлении нового VPN-канала. Проиллюстрировано, как это можно сделать для IPSec Security Associations. Был проведен анализ возникающих рисков и перспективы возможных атак со стороны злоумышленника. Охвачена проблема использования технологии NAT. Используя предложенный метод, мобильный пользователь получает возможность работать через VPN-канал в движении. Это повышает эффективность работы и сокращает издержки трафика.

4. Литература

1. “WPMC ‘03” The 6th International Symposium on Wireless Personal Multimedia Communications. http://www.ilcc.com/WPMC/index.html, 2003г.
   paper: Maintaining Security Associations for Seamless Mobile VPN
   paper’s author: Yi Cheng, “Wireless Corporate Access Ericsson Enterprise AB”, 2003г, SE-126 25 Stockholm, Sweden