VPN: Основные понятия и технологии. Протоколы PPTP,L2TP. Анализ возможных уязвимостей протокола PPTP в реализации Microsoft.

Студент 017 группы
Кобылянский Владимир

Оглавление:

1.Введение.

Virtual Private Network(VPN) на русский язык можно перевести как Виртуальная Частная Сеть.

Этим термином обозначается технология, позволяющая использовать инфраструктуру сетей общего пользования для создания частных сетей, приватность которых обеспечивается при помощи протоколов туннелирования и процедур обеспечения секретности.

Прежде чем продолжать описание этой технологии, хочу сразу пояснить почему она появилась и где используется.

До создания VPN, если , например, какая-то организация, будь то государственное учреждение или представитель бизнеса,хотела передавать данные между своими подразделениями в разных городах и при этом обеспечить их конфиденциальность,не было другого выхода, кроме как взять в аренду у телефонной компании выделенную линию. Очевидно, что стоило это не малых денег. С появлением VPN все координально изменилось - теперь появилась возможность передавать важную информацию по сетям общего пользования практически так же безопасно, как и по выделенной линии, но за гораздо меньшие деньги. (Справедливости ради, стоит отметить, что многие эксперты по безопасности все же считают, что выделенная линия и по сей день остается наиболее надежным способом передачи конфиденциальной информации.)

Второй пример практически не мозможно реализовать средствами не использующими VPN-технологии. Представьте себе,что ввиду особенностей вашего бизнеса, вы вынужденны часто ездить в командировки по всеми миру. Представим что ваша задача - заключение договоров на поставку какого-либо оборудования в кротчайшие сроки, и вам просто необходимо в реальном времени отслеживать наличие товаров на ваших складах. Как это сделать? Конечно можно посадить несколько человек на телефон и постоянно звонить им, но ,во-первых, это не безопасной способ - ваши конкуренты будут в курсе всех ваших поставок, а ,во-вторых, это достаточно дорого. Но есть способ лучше, в практически в любой стране не сложно найти интернет. Вы можете подключиться к интернет и с помощью VPN зайти на ваш сервер базы данных,на котором храниться все информация о товарах на складах.

Как вы видите, преимущество VPN очевидны, и потому не удивительно, что в последнее время эти технологии получают все больше распространение.

2.Разные типы VPN.

VPN подразделяют на три группы : **trusted**(доверенные) VPNs, **secure** (безопасные) VPNs, **hybrid**(гибридные) VPNs.

Когда Интенет еще не был таким большим и универсальным, многие компании брали в аренду у провайдера часть его сети. Провайдер же предоставлял клиентам возможность использовать часть своей сети так, как если бы она полность принадлежала клиенту: копания

применяла свою политику безопасности, использовала свои IP адреса и т.д.(хотя достаточно часто провайдеры предоставляли клиентам помощь в организации всего этого). И хотя сданные в аренду разным компаниям сети могли использовать одно и то же сетевое оборудование (например коммутаторы), провайдер гарантировал, что его клиенты не имеют доступ к сетям друг друга. Очевидно, что такие сети строились при полном доверии к провайдеру, отсюда и их название.

С течением времени, Интернет завоевывал все большую популярность у корпоративных пользователей. И, учитывая, что trusted VPN не обеспечивает настоящей кофиденциальности данных производители начали создавать протоколы, которые позволяют шифровать данные на "краю" локальной сети и на удаленном узле, создавая таким образом так называемый "тунель" между локальной сетью и удаленным узлом (или другой сетью). Учитывая то, что весь трафик шифруется, даже если злоумышленник сможет перехватить данные, он не сможет их прочесть, и если он попробует изменить данные - об это станет сразу же известно принимающей стороне. Таким образом осуществляестя действительно защищенное соединение.Все VPN, использующие шифрование,называются secure VPN.

Очевидно, что trusted VPN и secure VPN можно использовать одновременно, такие сети называются hybrid VPN.

В этой статье я рассмотрю некоторые технологии, применяемые для создания secure VPN.

3.Протоколы, используемые для создания secure VPN.

С середины 90-х две компании развивали свои собственные (проприетарные) VPN-протоколы: Microsoft PPTP и Cisco L2F.
В дальнейшем эти протоколы обьединили в один, так появился протокол L2TP, который затем стал открытым стандартом.
Но по ряду причин, многие и по сей день используют протокол PPTP, причем в реализации самой Microsoft, что отрицательно сказывается на безопасности VPN соединении. Но об этом позже, а сейчас я в кратце расскажу о протоколах PPTP и L2TP.

3.a Протокол PPTP.

Point to Point Tunneling Protocol (PPTP) - тунельный протокол типа точка-точка - был создан для создания secure VPN по общедоступной TCP/IP сети с помощью стандартноо протокола PPP.

Сначала создается управляющее тунелем соединение (через TCP, порт 1723). После обмена служебными сообщениями,узлы создают соединение для пересылки данных, посредством протокола Generic Routing Encapsulation (GRE).Данные, предназначенные для пересылки через туннель, инкапсулируются необычным образом.

Во-первых, данные проходят все уровни OSI модели до уровня Network включительно, а на уровне Data Link только вычисляются заголовок и окончание PPP пакета. Затем весь полученный пакет шифруется. К полученному шифротексту протокол PPTP добавляет вычисленные заранее заголовок и окончание PPP пакета.Далее, этот PPP-кадр инкапсулируется в GRE-пакет. К GRE-пакету приписывается IP-

заголовок, затем он инкапсулируется в PPP-кадр и отправляется получателю.

Учитывая то, что PPTP использует GRE, который инкапсулирует протоколы сетевого уровня (IPX, AppleTalk, и т.д.) для передачи их по IP-сетям, очевиден главный недостаток PPTP - возможность создания туннеля только поверх TCP/IP сетей.

3.b Протокол L2TP.

Layer 2 Tunneling Protocol (L2TP) - протокол туннелирования на втором уровне - является обьединением двух протоколов (PPTP - туннелирование по TCP/IP-сетям и L2F - туннелирование по X.25, ATM, Frame Relay).

L2TP использует для транспортировки протокол UDP(как для туннелирования данных, так и для управления туннелем).

Сначала данные в процессе инкапсуляции доходят до второго уровня (Data Link),затем к полученному PPP-кадру приписывается L2TP заголовок. Итоговое L2TP-сообщение инкапсулируется UDP, который ,в свою очередь, инкапсулируется IPSec.

Таким образом L2TP отвечает только за создание и управление туннелем, а также за надежную доставку UDP-датаграмм (в заголовке L2TP есть поля Next-Received и Next-Sent которые схожи по функцианальности Acknowledgement Number и Sequence Number в протоколе TCP). Шифрование же - прерогатива IPSec.

4.Анализ возможных уязвимостей протокола PPTP в реализации Micrsoft.

4.a.Аутентификация

PPTP от Micrsoft поддерживает аутентификацию в трех вариантах:
1)Пароль в открытом виде.
2)Хеш от пароля (используемые хеш – Lan Manager и WindowsNT хеш)
2)Аутентификация по протоколу MS-CHAP.

Шифрование даных, передаваемый по туннелю, возможно только если используется последний метод аутентификации.

4.b.Хеш-функции.

Остановимся на хеш-функциях(они используются так же и в протоколе MS-CHAP и при шифровании данных).

Lan Manager – эта функция, основаная на DES, была разработана еще для IBM-OS/2.
Она вычисляестя следующим образом:
1) Пароль приводится к длине 14 байт(все что выходит за рамки 14 байт опускается, а если пароль меньше 14 байт – в конце дописываются нули)
2)Затем все символы алфавита приводятся к верхнему регистру. Цифры и спец-символы остаются без изменения.
3)Каждая половина полученной строки используется как ключ. Этими ключами по алгоритму DES шифруется фиксированная константа – получаются две 8 байтовые строки.
4)Эти 8 байтовые строки обьединяют, и получается 16 байтный хеш.

Очевидны недостатки этого хеша:
а) ограничение возможных значений пароля, путем перевода символов алфавита в верхний регистр.
б) независимость хэширования двух 7 байтовых строк.
в) нет индивидуальной привязки (т.е. у двух пользователей с одинаковым паролем будут одинаковые хеш-функции).

Все это делает Lan Manager уязвимым для атаки по словарю. А отсутсвие индивидуальной привязки делает эту атаку еще и очень быстрой.

WindowsNT хеш вычисляется по такой схеме:
а)Пароль приводится к 14 байтной длине.(длина паролей ограничена диспечером пользователей – сама WindowsNT хеш может принимать пароли длиной до 128 символов).
б)Преобразование полученной строки в Unicode.
в)Хеширование строки с помощью функции MD-4 и получение 16 байтной строки хеша.

Как мы видим, в новой функции устранены многие слабости Lan Manager, хотя и не все - индивидуальной привязки нет.

Но куда более серьезная проблема состоит в том, что допущены грубейшие ошибки в реализации. Хотя Lan Manager хеш был включен в протокол для совместимости и не нужен в NT сетях – оба значения хеш-функций передаются вместе. Таким образом не составляет труда подобрать пароль атакой по словарю Lan Manager хеша и впоследствии подобрать регистр по WindowsNT хешу.

4.b.Протокол аутентификации MS-CHAP.

Реализация PPP CHAP от Microsoft (MS-CHAP) работает следующим образом:
1)Клиент посылает серверу запрос.
2)Сервер в ответ присылает случайную 8 байтовую строку.
3)Клиент вычисляет хеш Lan Manager от пароля, дописывает к результату 5 нулей. Полученную 21 байтовую строку делит на три 7 байтовых части и использует их в качестве ключа для шифрования случайной 8 байтовой последовательности, присланной сервером. В итоге, получается 24 байтовая строка, которую клиент отправляет серверу. То же самое происходит с использованием WindowsNT хеша.
4)Сервер находит в своей базе хеш-функции от пароля, вычисляет 24 байтовую строку от 8 байтовой последовательности, посланной клиенту, и сравнивает свой результат и результат, присланный клиентом. Если сравнение проходит удачно, на этом аутентификация заканчивается.

Сервер может сравнивать ответ по Lan Manager или WindowsNT хешам. Это зависит от того, установлен ли флаг в принятом от клиента пакете(если установлен – используется WindowsNT хеш, если нет – Lan Manager хеш).

Как мы видим, здесь так же можно воспользоваться слабостями хеш-функции Lan Manager. Так же можно использовать то, что случайная 8 байтовая последовательность шифруется 7 байтовыми ключами независимо.

Учитывая то, что протокол не предусматривает аутентификации сервера, атакующий может легко замаскироваться под сервер.

4.c.Описание протокола MPPE.

Протокол шифрования в одноранговых сетях (MPPE) обеспечивает шифрование PPTP пакетов. Для собственно шифрования используется поточный шифр RC4 с 40- или 128-битным симметричным ключем.

40-битовый ключ получается таким образом:
1)Генерация 64-битового ключа из хэш-функции Lan Manager пароля пользователя (известного пользователю и серверу) с помощью SHA.
2)Установка старших 24 бит ключа в значение 0xD1269E.

128-битовый ключ получается так:
1)Объединение хэша Windows NT и 64-битового случайного значения, выданного сервером при работе по протоколу MS-CHAP.

2)Генерация 128-битового ключа с помощью SHA.

Полученный в итоге ключ используется для шифрования. После каждых 256 пакетов ключ меняется. Смена ключа происходит следующим образом:

1)Генерация определяющего ключа - 64-битового для 40-битового шифрования и 128-битового для 128-битового шифрования - путем хэширования предыдущего ключа и исходного ключа с помощью SHA.

2)Если требуется 40-битовый ключ, то установка старших 24 бит ключа в значение 0xD1269E.

При потере синхронизации происходит смена ключа.

Как мы видим, все опять упирается в несовершенство хеш-функций – достаточно легко проводить атаки по словарю, особенно, если учесть, что в распоряжении атакующего все стандартные заголовки PPP пакета.

Существуют еще несколько атак на протоколы MPPE и PPTP, но ,к сожалению, описать их все нет возможности ввиду ограничения по размеру, введенного для этой статьи.

5.Заключение.

Как вы могли видеть, существуют разные типы VPN, и разные протоколы для их создания, причем все они различаются по степени безопасности.
Мы так же показали, что существуют серьезные уязвимости в реализации протокола PPTP от Microsoft.
Очень хотелось бы надеяться, что все кто ответственнен за выбор протокола, для создания secureVPN знакомы с этими уязвимостями.

6.Литература.

1)Bruce Schneier, Peter Mudge (перевод Василий Томилин, редактирование Павел Семьянов), ”Криптоанализ туннельного протокола типа точка-точка (PPTP) от Microsoft”. <http://www.counterpane.com/pptp.html>

2)Prof. Dr. Heinzmann, “VPN Concepts and Protocols (PPTP,L2TP, IPSec)”,Internet Security Course.

<http://www.cnlab.ch>
<http://www.ita.hsr.ch/nws />

3)VPN Consortium (VPNC), “VPN Technologies: Definitions and Requirements”, VPN Consortium, January 2003.
<http://www.vpnc.org/>