Вступление от автора сайта

Для скрытия ip-адреса при работе в сети Интернет возможно использовать много разных технологий, начиная от анонимных проксиов, заканчивая ssl v.3 туннелями. Многие интернет провайдеры предлагают за деньги (или безвозмездно) доступ в сеть интернет через свои сервера находящиеся под другой юрисдикцией (в другом государстве, например в Новой Зеландии). Некоторые из них используют технологию VPN с реализацией от MS и соответственно шифрованием. Данная статья покажет Вам насколько "безопасно"

использовать шифрование в реализации от Microsoft. Если кто-то далек от всего этого, обычно, такие люди ссылаются на то, что это им никогда не понять, номинаю - ПРОСВЕЩЕНИЕ это лучший путь развития для человека (подсказка прочитайте хотябы введение и заключение).

Криптоанализ туннельного протокола типа точка-точка (PPTP) от Microsoft

Bruce Schneier, Peter Mudge
e-mail: {schneier,mudge}@counterpane.com

§1. Введение

Многие организации не являются централизованными. Филиалы, виртуальные корпорации и перемещающиеся сотрудники делают идею создания выделенного канала к любому требуемому пункту логически невозможной. Концепция виртуальных сетей обеспечивает решение возникшей проблемы путем туннелирования объединяемого сетевого пространства по другим, промежуточным и небезопасным сетям (например, Интернет), тем самым позвол удаленным пунктам стать локальными. Данное решение не требует вложений на проведение абонируемых или выделенных линий в любую точку. Такой способ иногда называют 'туннель'.

По мере решения виртуальными сетями проблем нецентрализованных машин возникла другая проблема. Трафик, который раньше находился в пределах компании, теперь открыт для любопытных глаз со всего мира. Для обеспечения не только отказоустойчивости, но и безопасности информации необходимо использовать механизмы аутентификации и шифрования. В результате виртуальные сетевые

соединения объединили с криптографической защитой, и конечный продукт назвали Виртуальные Приватные Сети (VPN).

Безопасность VPN основывается на безопасности протоколов аутентификации и шифрования. Если криптография VPN слаба, то степень защиты не выше, чем в любой другой неприватной сети передачи информации по Интернет. Поскольку компании надеются, что VPN расширит периметр внутренней безопасности до удаленного офиса, прорыв системы защиты туннеля соответствует уничтожению всех систем защиты внутреннего периметра. Прорыв в VPN означает практически то же самое, что и прорыв за firewall.

Протокол PPTP (туннельный протокол типа точка-точка) был предназначен для решения задачи создания и управления VPN по общественной сети TCP/IP с использованием стандартного протокола PPP. Хотя протокол резервирует пространство для всех возможных типов шифрования и аутентификации, в большинстве коммерческих продуктов используется версия данного протокола для Windows NT. Именно эта реализация и подвергнута анализу в данной статье.

Мы обнаружили, что протокол аутентификации Microsoft слаб и уязвим путем атаки по словарю; большинство паролей можно вскрыть в течение нескольких часов. Мы обнаружили, что способы шифрования с использованием 40- и 128-разрядных ключей одинаково слабы и открыли ряд заложенных в реализацию неразумных идей, которые позволяют осуществлять другие атаки на данный шифр. Мы можем открывать соединения через firewall, нарушая правила переговоров PPTP, и можем проводить различные атаки отказа в обслуживании на тех, кто использует Microsoft PPTP.

Оставшаяся часть работы разделена следующим образом: В параграфе 2 рассматривается PPTP, как стандарт протокола, так и реализация Microsoft. В параграфе 3 рассматриваются две функции хэширования паролей в Microsoft PPTP и способы атаки на них. В параграфе 4 проводится криптоанализ протокола аутентификации Microsoft, а в параграфе 5 - криптоанализ протокола шифрования Microsoft. Другие атаки на Microsoft PPTP рассмотрены в параграфе 6. Наконец, в параграфе 7 делаются некоторые выводы.

§2. Туннельный протокол типа точка-точка

PPTP - протокол, который позволяет выполнять туннелирование PPP-соединений по IP-сети путем создания VPN. Таким образом, удаленный компьютер в сети X может туннелировать трафик на шлюз в сети Y и имитировать подключение, с внутренним IP-адресом, к сети Y. Шлюз получает трафик для внутреннего IP-адреса и передает его удаленной машине в сети X. Существуют два основных способа использования PPTP: по Интернет и по коммутируемым соединениям. Настоящая статья ориентирована на использовании PPTP как VPN при непосредственном подключении клиента к Интернет.

Функционирование PPTP заключается в инкапсулировании пакетов виртуальной сети в пакеты PPP, которые в свою очередь, инкапсулируются в пакеты GRE (Generic Routing Incapsulation), передаваемые по IP от клиента к шлюзу - серверу PPP и обратно. Совместно с каналом инкапсулированных данных существует управляющий сеанс на базе TCP. Пакеты управляющего сеанса позволяют запросить статус и сопровождать сигнальную информацию между клиентом и сервером. Канал управления иницируется клиентом на сервере на TCP-порте 1723. В большинстве случаев это двунаправленный канал, по которому сервер посылает запросы на сервер и наоборот.

PPTP не оговаривает конкретных алгоритмов аутентификации и протоколов; вместо этого он обеспечивает основу для обсуждения конкретных алгоритмов. Переговоры не присущи только PPTP, они относятся к существующим вариантам переговоров PPP, содержащихся в CCP, CHAP и других расширениях и усовершенствованиях PPP.

§2.1. PPTP от Microsoft

Microsoft PPTP является частью ОС Windows NT Server, данное программное обеспечение можно бесплатно получить с Web-сайта Microsoft. Подключение осуществляется с помощью панели управления и редактора реестра. Данная реализация PPTP широко используется в коммерческих применениях VPN, например Aventail и Freegate именно потому, что входит в состав ОС Microsoft.

Сервер Microsoft PPTP может существовать только для Windows NT, хотя клиентское программное обеспечение существует для Windows NT, некоторых версий Windows и Windows 98.

Реализация Microsoft поддерживает три варианта аутентификации:

1. Текстовый пароль: Клиент передает серверу пароль в открытом виде.
2. Хэшированный пароль: Клиент передает серверу хэш пароля (см. параграф 3).
3. Вызов/Отклик: Аутентификация сервера и клиента с использованием протокола MS-CHAP (вызов/отклик), что описано в параграфе 4.

Третий вариант называется в документации для пользователей "Аутентификации Microsoft", для шифрования пакетов PPTP его надо разрешить. При выборе любого из двух других вариантов шифрование неосуществимо. Кроме того, возможность шифрования (40- или 128-разрядное) гарантируется только в том случае, если клиент использует Windows NT. Некоторые клиенты Windows 95 не могут поддерживать зашифрованные сеансы.

§3. Криптоанализ функций хэширования паролей Windows NT

В ОС Microsoft Windows NT для защиты паролей используются две однонаправленные хэш-функции: хэш Lan Manager и хэш Windows NT. Функция хэша Lan Manager была разработана Microsoft для операционной системы IBM OS/2, она была интегрирована в Windows for Workgroups и частично в Windows 3.1. Данная функция используется в некоторых протоколах аутентификации перед Windows NT.

Хэш Windows NT был разработан специально для ОС Microsoft Windows NT.

-
- Функция хэша Lan Manager основана на алгоритме DES;
- Функция хэша Windows NT основана на односторонней хэш-функции MD4.

Обе эти функции используются во многих протоколах аутентификации Windows NT, а не только в PPTP.

Функция хэша Lan Manager вычисляется следующим образом:

1. Превращение пароля в 14-символьную строку путем либо отсечки более длинных

паролей, либо дополнения коротких паролей нулевыми элементами.

2. Замена всех символов нижнего регистра на символы верхнего регистра.
3. Цифры и специальные символы остаются без изменений.
4. Разбиение 14-байтовой строки на две семибайтовых половины.
5. Использование каждой половины строки в роли ключа DES, шифрование фиксированной константы с помощью каждого ключа, получение двух 8-байтовых строк.
6. Слияние двух строк для создания одного 16-разрядного значения хэш-функции.

Словарные атаки на функцию хэша Lan Manager легко достигают успеха по следующим причинам:

-
- Большинство людей выбирают легко угадываемые пароли.
- Все символы преобразуются в верхний регистр, что ограничивает и без того небольшое число возможных паролей.
- Нет индивидуальной привязки (salt); два пользователя с одинаковыми паролями всегда будут иметь одинаковые значения хэш-функции.
- Таким образом, можно заранее составить словарь хэшированных паролей и осуществлять поиск неизвестного пароля в нем. При таком подходе с точки зрения отношения время/память тестирование пароля может выполняться со скоростью дискового ввода/вывода.
- Две семибайтовых "половины" пароля хэшируются независимо друг от друга.
- Таким образом, две половины могут подбираться методом грубого подбора независимо друг от друга, и сложность атаки не превышает сложности атаки против семибайтового пароля.
- Пароли, длина которых превышает семь символов, не сильнее, чем пароли с длиной семь символов. Кроме того, те пароли, длина которых не превышает семь символов очень просто распознать, поскольку вторая половина хэша будет одной и той же фиксированной константой: шифрование фиксированной константы с помощью ключа из семи нулей.

Функция хэша Windows NT вычисляется следующим образом:

1. Преобразование пароля, длиной до 14 символов, с различием регистров в Unicode.
2. Хэширование пароля с помощью MD4, получение 16-символьного значения хэш-функции.

Хэш Windows NT обладает преимуществом по сравнению с функцией хэша Lan Manager - различаются регистры, пароли могут быть длиннее 14 символов, хэширование пароля в целом вместо разбиения его на маленькие части - хотя по-прежнему отсутствует индивидуальность.

Таким образом, люди, имеющие одинаковые пароли, всегда будут иметь одинаковые хэшированные пароли Windows NT. Сравнение файла хэшированных паролей с заранее рассчитанным словарем хэшированных паролей может быть весьма эффективной атакой.

Кроме того, более серьезная проблема реализации существенно облегчает раскрытие паролей. Даже хотя хэш Lan Manager был включен по соображениям совместимости с предыдущими версиями, и не требуется в сетях Windows NT, оба значения хэш-функций всегда передаются вместе. Следовательно, можно выполнить грубый подбор пароля с помощью более слабой хэш-функции Lan Manager и затем выполнить тестирование с учетом регистра для подбора значения хэш-функции Windows NT.

§4. Криптоанализ MS-CHAP

PPP содержит различные способы обработки аутентификации. Одним из способов является протокол аутентификации вызов-рукопожатие (CHAP). Реализация PPP CHAP компанией Microsoft (MS-CHAP) почти совпадает с методом аутентификации, используемым для аутентификации клиентов в Windows-сетях.

MS-CHAP функционирует следующим образом:

1. Клиент запрашивает вызов сетевого имени.
2. Сервер возвращает восьмибайтовый случайный вызов.
3. Клиент вычисляет хэш-функцию Lan Manager, добавляет пять нулей для создания 21-байтовой строки и делит строку на три семибайтовых ключа. Каждый ключ используется для шифрования вызова, что приводит к появлению 24-разрядного зашифрованного значения. Оно возвращается серверу как отклик.
4. Клиент выполняет то же самое с хэш-функцией Windows NT.
5. Сервер ищет значение хэш-функции в своей базе данных, шифрует запрос с помощью хэш-функции и сравнивает его с полученными зашифрованными значениями.

Если они совпадают, аутентификация заканчивается. Сервер может выполнять сравнение по хэш-функции Windows NT или по хэш-функции Lan Manager; результаты должны совпадать.

6. Хэш, используемый сервером, зависит от конкретного флага в пакете. Если флаг установлен, то сервер выполняет тестирование с помощью хэш-функции Windows NT; в противном случае тестирование выполняется с помощью хэш-функции Lan Manager.

Протокол вызова/отклика является стандартным; использование случайного вызова имени делает невозможными словарные атаки на MS-CHAP и файл записанных хэш-функций от паролей. В то же время, поскольку даже в Windows NT-сетях используются оба значения хэш-функции, можно в каждом случае атаковать более слабую хэш-функцию Lan Manager. Поскольку ответ клиента разбит на три части, и каждая часть шифруется независимо от других, можно атаковать сам протокол MS-CHAP.

Последние восемь байт хэш-функции Lan Manager представляют собой константу в том случае, если длина пароля не превышает семи символов. Это верно, несмотря на случайный вызов. Следовательно, последние восемь байт отклика клиента будут представлять собой вызов, зашифрованный с помощью данной константы. Легко проверить, не превышает ли длина пароля семи символов. После того, как атакующий находит значение хэш-функции Lan Manager, он может использовать эту информацию для восстановления хэш-функции Windows NT.

Атака может быть существенно ускорена за счет активного использования предварительных вычислений и тщательного исследования слабостей хэш-функции Lan Manager и протокола MS-CHAP.

Далее приводятся подробности оптимизированной атаки:

-
- P0-P13 - байты пароля.
- H0-H15 - байты хэш-функции Lan Manager, которая преобразуется в 21-байтовый ключ K0-K20.
- S- фиксированная константа, используемая в хэш-функции Lan Manager.
- Вызов C и 24-байтовый отклик R0-R23. Злоумышленник может знать C и R и хочет найти P.

1. Попробуйте все возможные комбинации K14, K15. Правильное значение выделяется, когда C превращается в R16, ..., R23 с ключом K14, K15, 0,0,0,0,0. На это уходит примерно 215 операций.
2. Попробуйте вероятные значения P7,...,P13. Неверные значения можно быстро отбросить путем шифрования S и проверки совпадения последних двух байт полученного значения с K14 и K15. (Так остается только один вариант из каждых 216).
3. Каждый оставшийся вариант P7,...,P13 предоставляет значение-кандидат для K8,...,K13. Чтобы проверить значение-кандидат, проверьте все возможные значения K7, чтобы увидеть, есть ли такое, при котором C шифруется в R8,...,R15 при значении-кандидате K8,...,K15.
4. Если есть такое K7, то догадка для P7,...,P13 почти наверняка верна. Если нет, то надо выбрать другое значение для P7,...,P13. Если существуют N вероятных вариантов P7,...,P13, то подбор верного значения можно провести за N тестовых шифрований.
5. Обратите внимание, что поскольку в протоколе нет индивидуальной настройки, эта атака может быть существенно ускорена с помощью замены время/память.
6. Если есть N заранее вычисленных тестовых шифрований, то восстановление верного значения P7,...,P13 потребует N/216 операций. После нахождения P7,...,P13, восстановление P0,...,P6 требует M попыток, где M - число вероятных значений P0,...,P6. Опять же, поскольку нет индивидуальной настройки, атака может быть выполнена за N/28 попыток при M предварительно вычисленных значениях.

Кроме того, данный протокол позволяет выполнить аутентификацию только клиента. Атакующий, выполняющий подмену соединения, может тривиально замаскироваться под сервер. Если шифрование разрешено, атакующий не сможет посылать и принимать сообщения (пока не взломает шифр), однако используя старое значение вызова он сможет получить две сессии текста, зашифрованные одним ключом (см. атаки далее).

§5. Криптоанализ MPPE

§5.1. Описание MPPE

Протокол шифрования в одноранговых сетях (MPPE) обеспечивает методологию для шифрования пакетов PPTP. Он предполагает существование секретного ключа, известного обоим участникам соединения, и использует поточный шифр RC4 с 40- либо 128-разрядным ключом. Такой метод установки использования MPPE является одной из функций протокола управления сжатием PPP (CCP) и описан в приложении C. После установки режима работы начинается сеанс PPP по передаче пакетов зашифрованных данных. Важно отметить, что шифруются только те пакеты PPP, номера протоколов

которых лежат в диапазоне 0x0021-0x00fa. Все остальные пакеты передаются без шифрования, даже если шифрование разрешено. Типы пакетов, шифрование которых осуществляется/не осуществляется, регламентируются документом RFC 1700. Для любых пакетов не обеспечивается аутентификация.

В MPPE 40-битовый ключ RC4 определяется следующим образом:

-
- Генерация определяющего 64-битового ключа из хэш-функции Lan Manager пароля пользователя (известного пользователю и серверу) с помощью SHA.
- Установка старших 24 бит ключа в значение 0xD1269E.

128-битовый ключ RC4 определяется следующим образом:

-
- Объединение хэша Windows NT и 64-битового случайного значения, выданного сервером при работе по протоколу MS-CHAP.
- Данное число посылается клиенту по протоколу обмена, потому что оно известно и клиенту, и серверу.
- Генерация определяющего 128-битового ключа из результатов предыдущего этапа с помощью SHA.

Результирующий ключ используется для инициализации RC4 обычным способом, а затем для шифрования байт данных. После каждых 256 пакетов - MPPE поддерживает счетчик, в котором фиксируется число пакетов - генерируется новый ключ RC4 по следующим правилам:

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

Длина типичного пакета PPTP составляет 200 байт, включая заголовок.

При потере синхронизации происходит реинициализация RC4 с использованием текущего ключа. Существует также возможность обновления ключа RC4 после каждого пакета; эта возможность снижает эффективность шифрования примерно наполовину, поскольку на выполнение плановых изменений ключа RC4 требуется время.

§5.2. Восстановление ключа

В MPPE степень защиты ключа не превышает степень защиты пароля. Большая часть паролей имеет существенно меньше 40 бит безопасности и раскрываются с помощью словарных атак. Хэш-функция Lan Manager еще более уязвима: с учетом максимальной длины порции, ограниченного алфавита и отсутствия символов нижнего регистра, невозможно сгенерировать 128-битовый ключ, даже если пользователь хочет это сделать. В документации по MPPE описывается флаг для вычисления 40-битового ключа RC4 на основании хэш-функции Windows NT, а не Lan Manager, но эта функция еще не реализована. Нет способов вычисления 128-битового ключа RC4 на основании хэш-функции Windows NT, хотя такой вариант был бы более безопасным (хотя существенно менее безопасным, чем 128-битовый случайный ключ.)

В любом случае, общая степень защиты составляет не 40 или 128 бит, а количество бит энтропии пароля. На основании экспериментальных данных получено, что английскому языку свойственна энтропия 1,3 бита на символ. Изменения регистра, цифры и специальные символы существенно повышают это значение. Любая атака, которая использует словарь слабых паролей, может быть способна прочитать зашифрованный MPPE трафик. Кроме того, стилизованные заголовки в пакете PPP облегчают сбор известных текстов и базы для проверки угаданного ключа.

40-битовый алгоритм RC4 подвержен более серьезным уязвимостям. Поскольку не предусмотрена индивидуальная настройка, атакующий может подготовить словарь зашифрованных заголовков PPP, а затем быстро найти данный зашифрованный текст в словаре. При поиске мест в пакетах MPPE, где может содержаться незашифрованный текст, атакующий может воспользоваться множеством связей по SMB и NetBIOS, которые происходят при стандартных соединениях Microsoft.

Более того, тот же 40-битовый ключ RC4 генерируется всякий раз, когда пользователь инициализирует протокол PPTP. Поскольку RC4 представляет собой способ шифрования с обратной связью по выходу, то просто взломать шифр за два сеанса. Серьезная уязвимость отмечается в большей части свежих спецификаций MPPE, хотя она исчезла из предыдущей версии. Ни в одной версии документации Microsoft не указано, что один и тот же ключ используется как в прямом, так и в обратном направлении, что гарантирует, что для шифрования двух разных текстов используется один и тот же поток ключей.

128-битовый RC4 использует в процессе генерации ключей 64-битовую случайную величину. Такой подход делает непрактичной словарную атаку. По-прежнему, метод грубого подбора пароля более эффективен, чем метод грубого подбора пространства ключей. Случайное число также означает, что для двух сессий с одним паролем будут использованы разные 128-битовые ключи RC4, хотя для шифрования текста в обоих направлениях будет использован один и тот же ключ.

§5.3. Атаки переворота битов

RC4 - способ поточного шифрования с обратной связью по выходу, при этом не обеспечивается аутентификация потока зашифрованного текста. Поскольку в MPPE не предусмотрено другого способа аутентификации, атакующий может незаметно менять значения бит в шифре. Если протокол нижнего уровня чувствителен к изменению значения конкретных бит - разрешение/запрещение каких-либо функций, выбор вариантов, сброс параметров - эта атака может быть достаточно эффективна. Обратите внимание, для проведения этой атаки атакующему не надо знать ключ шифрования или пароль клиента. Конечно, такие атаки могут обнаруживаться или предотвращаться протоколами верхнего уровня.

§5.4. Атака путем ресинхронизации

Если в процессе передачи теряется пакет, либо приходит пакет с неверным номером в заголовке MPPE, то происходит ресинхронизация ключа. Сторона, принявшая неверный пакет, посылает отправителю запрос на ресинхронизацию. По принятию данного запроса, отправитель реинициализирует таблицы RC4 и устанавливает бит "сброшен" (flushed) в заголовке MPPE. Если система обнаруживает в пакете установленный бит "сброшен", она реинициализирует свои таблицы RC4 и устанавливает счетчик пакетов в соответствии с полученным значением.

Так создается проблема, когда атакующий может либо подавать запросы на ресинхронизацию, либо вбрасывать пакеты MPPE с неверными значениями счетчика пакетов. Если выполнять это постоянно перед обменом 256-м пакетом, когда происходит смена сеансового ключа, то атакующий может добиться успеха - сеансовый ключ не будет изменен.

§6. Другие атаки на MS-PPTP

Несмотря на то, что атаки на протоколы MS-CHAP и MPPE приводят к полному отрицанию полезности и безопасности MS PPTP, необходимо упомянуть о нескольких интересных атаках.

§6.1. Пассивный мониторинг

Потрясающее количество информации можно получить, если просто наблюдать за трафиком сеанса PPTP, передаваемым по сети. Такая информация бесценна для анализа трафика, ее следует защищать. Тем не менее, сервер выдает всем желающим такие сведения, как максимальное количество доступных каналов. Эту информацию можно использовать для установки соответствующего размера сервера PPTP и контроля его нагрузки. Если атакующий регулярно передает пакеты PPTP_START_SESSION_REQUEST, то он может наблюдать создание новых соединений и закрытие существующих соединений. Таким способом атакующий может собрать информацию о системе и шаблонах ее использования, при этом ему не нужно быть рядом.

Путем установки стандартных средств просмотра и расшифровки общественных линий связи от серверов Microsoft PPTP была получена следующая информация:

-
- IP-адрес клиента
- IP-адрес сервера
- Количество доступных на сервере виртуальных каналов PPTP
- Версия RAS клиента
- Имя клиента NetBIOS
- Идентификация производителя клиента
- Идентификация производителя сервера
- IP-адрес клиента во внутреннем виртуальном туннеле
- Внутренние DNS-сервера, обслуживающие клиента
- Имя пользователя на клиенте
- Достаточно информации для получения значений хэш-функций паролей

пользователей

- Достаточно информации для получения начального значения MPPE
- Текущее значение шифрованного пакета для клиента перед реинициализацией

RC4

- Текущее значение шифрованного пакета для сервера перед реинициализацией
- RC4

В любом случае, когда канал связи шифруется и пользователь предполагает некоторый уровень конфиденциальности, перечисленная выше информация не должна быть доступна так легко. Для Microsoft PPTP нет легкого способа зашифровать эту информацию, поскольку утечки происходят вне канала, контролируемого MPPE. В некоторых случаях, эти пакеты представляют собой конфигурационные и установочные пакеты для шифрования в рамках MPPE, и они должны передаваться до начала шифрования. Единственным решением является шифрование канала управления или резкое уменьшение количества передаваемой по нему информации.

§6.2. Перехват переговоров PPP

Пакеты переговоров PPP передаются до начала шифрования и после его окончания. Поскольку метод ресинхронизации ключей осуществляется с использованием пакетов PPP CCP, эти каналы связи не могут шифроваться таким же образом. Добавим, что реальная аутентификация данных пакетов не выполняется. Этап конфигурации полностью открыт для атаки.

Подмена конфигурационного пакета, описывающего DNS-сервер, позволяет направить всю систему распознавания имен на ложный сервер имен.

Точно так же, подмена пакета, содержащего внутренний туннельный IP-адрес, позволяет обойти файрволы, осуществляющие фильтрацию пакетов по правилам, поскольку клиент будет подключаться к внешним машинам из внутренней защищенной сети.

§6.3. Канал управления и отказ в обслуживании на сервере

В данной статье каналу управления PPTP посвящена не слишком большая часть.

Частично потому, что непонятно, зачем этот канал существует. Все, что реализовано с помощью этого дополнительного канала, можно осуществить по каналам PPP или задействовать неиспользуемые фрагменты заголовка GRE.

Другой причиной была реализация Microsoft канала управления. Мы быстро обнаружили, что просто нарушить работоспособность машины Windows NT с сервером PPTP, иногда это приводило к появлению "голубого экрана". На самом деле, трудно провести тестирование канала управления и не нарушить работу сервера PPTP. Настолько трудно, что большая часть атак, предпринимавшихся для изучения теоретических проблем безопасности канала управления, приводила к нарушению работы сервера раньше, чем атаки могли сработать.

Далее описана малая часть тестов, приводивших к нарушению работы Windows NT Server с установленным Service Pack 3:

-
- Цикл по пакетам PPTP_CLEAR_CALL_REQUEST с тем, чтобы пройти 16-разрядное пространство идентификаторов вызова.
- Перебор всех возможных и невозможных значений, которые могут содержаться в поле Тип пакета заголовка пакета PPTP.
- Передача недопустимых значений в заголовке пакета управления PPTP.

Все вышеуказанные пакеты могут отправляться на сервер PPTP из-за файрвола, без всякой аутентификации. Предполагается, что нет конфигурации файрвола, позволяющей передавать PPTP на сервер PPTP с определенных IP-адресов или сетей. Однако, если у пользователей есть возможность обращаться к серверу PPTP из любой точки мира, то атакующий тоже должен иметь возможность послать запрос из любой точки мира.

§6.4. Потенциальные утечки информации на клиенте

Клиент Windows 95 не выполняет требуемую очистку буферов, и потому допускается утечка информации в сообщениях протокола. Хотя в документации PPTP сказано, что в пакете PPTP_START_SESSION_REQUEST символы после имени компьютера и производителя должны быть сброшены в 0x00, Windows 95 этого не делает.

Криптоанализ известного протокола RPTP от Microsoft

Автор: Алексей Пешков - Обновлено 27.07.2013 03:00

080: 0000 6c6f 6361 6c00 0000 3e1e 02c1 0000 ..local...>.....

096: 0000 85c4 03c1 acd9 3fc1 121e 02c1 2e00?.....

112: 0000 2e00 0000 9c1b 02c1 0000 0000 0000

128: 0000 88ed 3ac1 2026 02c1 1049 05c1 0b00: &...l....

144: 0000 3978 00c0 280e 3dc1 9c1b 02c1 041e ..9x..(.=.....

160: 02c1 0e00 0000 121e 02c1 2e00 0000 2e00

176: 0000 3dad 06c1 74ed 3ac1 1c53 05c1 9c1b ..=...t:..S....

192: 02c1 041e 02c1 0e00 0000 121e 02c1 2e00

208: 0000 ..

Выше показаны символы, содержащиеся после имени компьютера и строки производителя. В байтах 82-86 содержится имя компьютера, которое для клиента Windows 95 всегда равняется "local". Байт 113 - то место, где должна содержаться строка производителя. При просмотре аналогичного пакета Windows NT обнаружено, что все символы "мусора" сброшены в 0x00.

Существует очевидная возможность утечки информации в зависимости от того, как и где используются и размещаются структуры данных и что происходит на клиентской системе. Для оценки данной утечки информации необходимо провести дальнейший анализ кода Windows 95.

§7. Выводы

Реализация PPTP от Microsoft уязвима с точки зрения реализации, и обладает серьезными недостатками с точки зрения протокола. Протокол аутентификации имеет известные уязвимости, на которые указывалось не только здесь, но и в группах, например, L0pht. Шифрование выполнено неверно, в данной реализации используется поточный шифр с обратной связью по выходу, хотя более уместен был бы блочный шифр "шифр-блок-цепочка" (CBC). Чтобы связать слабую аутентификацию с плохим шифрованием Microsoft задал ключ шифрования как функцию от пароля пользователя вместо использования сильного алгоритма обмена ключами типа Диффи-Хеллмана или ЕКЕ. Наконец, канал управления не аутентифицируется и не сильно защищен.

Мы не потратили много времени на изучение механизмов обеспечения локальных IP-адресов клиентов и того, как Microsoft пытался и смог ли он учесть уязвимость представления клиента с двумя адресами. Тем не менее, мы обнаружили проблемы с нестандартными масками подсети и внутренним трафиком туннеля, отправленного от PPTP сервера. Разработчики, будьте внимательны!

Наконец, хочется подчеркнуть, что криптоанализ не подвергал сомнению протокол PPTP (?), но лишь реализацию протокола от Microsoft. Хотя Microsoft использует свои собственные расширения (MS-CHAP, MPPE, MPPE) в PPP секции PPTP, стандарт PPTP не требует этого. Производители могут включить расширения Microsoft в свои продукты по соображениям совместимости, но они не обязаны ограничиваться их использованием и, наверное, реализуют более безопасные решения. Конечно, новые расширения для корректной работы должны поддерживаться как клиентом, так и сервером.

1 - В ходе экспериментов выяснилось, что некоторые клиенты Windows 95

поддерживают аутентификацию Microsoft, а некоторые - нет. Мы не смогли оценить различия или определить способы, позволяющие понять, поддерживает ли данная система Windows 95 аутентификацию Microsoft. Если протокол не поддерживается, то пункт в диалоговом окне недоступен. Это ограничение соответствует заявлению Microsoft, что Windows 95 не обеспечивает безопасность, и что те пользователи, которым она нужна, должны перейти на NT. Тем не менее, Microsoft заявлял, что Windows 95 не обрабатывает хэш Windows NT, а использует хэш Lan Manager. Однако клиенты Windows 95 передают обе хэш-функции. Из нашего анализа кода Windows 95 неясно, почему шифрование нельзя реализовать в клиентах Windows 95.

2 - В документации Microsoft сказано, что длина паролей Windows NT может достигать 128 символов, и хэш-функция Windows NT принимает пароли такой длины. Однако, диспетчер пользователей ограничивает длину паролей до 14 символов. В документации MS-CHAP также упоминается это ограничение, которое подтвердилось в ходе экспериментов.

3 - Известное средство хакеров, L0phtcrack, автоматизирует процесс подбора пароля по его хэш-значению. На Pentium Pro 200, L0phtcrack 2.0 может проверить файл с 200 паролями за минуту с использованием 8 мегабайтного словаря паролей.

4 - Мы не исследовали ни сам генератор псевдослучайных чисел, ни его криптографическую стойкость.

§8. Благодарности

Мы хотели бы поблагодарить Mark Chen, Chris Hall, Brad Kemp, Paul Jones, Ben McCann, Mark Seiden, Inderpreet Singh, David Wagner и Wray West за их ценные замечания.

§9. Литература

[Ave98] Aventail Corp., 1998. <http://www.aventail.com>.

[BV98] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," Network Working Group, RFC 2284, Mar 1998. <ftp://ftp.isi.edu/in-notes/rfc2284.txt>.

[CK78] T.M. Cover and R.C. King, "A Convergent Gambling Estimate of Entropy," IEEE Transactions on Information Theory, v. IT-24, n. 4, Jul 1978, pp. 413--421.

[Fre98] FreeGate Corp., 1998. <http://www.freegate.com>.

[HLFT94] S. Hanks, T. Li, D. Farinacci, and P. Traina, "Generic Routing Encapsulation (GRE)," Network Working Group, RFC 1701, Oct. 1994. <ftp://ftp.isi.edu/in-notes/rfc1701.txt>.

[Hob97] Hobbit, "CIFS: Common Insecurities Fail Scrutiny," Avian Research, Jan 1997.

[HPV+97] K. Hamzeh, G.S. Pall, W. Verthein, J. Taarud, and W.A. Little, "Point-to-Point Tunneling Protocol," Internet Draft, IETF, Jul 1997.

[KSWH98] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators," Fast Software Encryption: 5th International Workshop, Springer-Verlag, 1998, pp. 168-188

[Kle90] D.V. Klein, "Foiling the Cracker: A Security of, and Implications to, Password Security," Proceedings of the USENIX UNIX Security Workshop, Aug 1990, pp. 5--14.

[Kli98] S. Klinger, "Microsoft PPTP and RRAS for Windows NT Server 4.0," LAN Times, Feb ??, 1998.

[L97a] L0pht Heavy Industries Inc, L0phtcrack, 1997. [L97b] L0pht Heavy Industries Inc, "A L0phtCrack Technical Rant," Jul 1997. <http://www.l0pht.com/l0phtcrack/rant.php>.

[LS92] B. Lloyd and W. Simpson, "PPP Authentication Protocols," Network Working Group, RFC 1334, Oct 1992. <ftp://ftp.isi.edu/in-notes/rfc1334.txt>.

[Mey96] G. Meyer, "The PPP Encryption Control Protocol (ECP)," Network Working Group, RFC 1968, Jun 1996. <ftp://ftp.isi.edu/in-notes/rfc1968.txt>.

[Mic96a] Microsoft Corporation, Advanced Windows NT Concepts, New Riders Publishing, 1996. Relevant chapter at <http://www.microsoft.com/communications/nrpptp.html>.

[Mic96b] Microsoft Corporation, "Pont-to-Point Tunneling Protocol (PPTP) Frequently Asked Questions," Jul 1996. [Mic97] Microsoft Corporation, "Response to Security Issues Raised by the L0phtcrack Tool," Apr 1997.

[Mic98] Microsoft Corporation, "Clarification on the L0phtcrack 2.0 Tool." Mar 1998.

[MB97] P. Mudge and Y. Benjamin, "Deja Vu All Over Again," Byte, Nov 1997. <http://www.byte.com/art/9711/sec6/art3.html>.

[NBS77] National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard," National Bureau of Standards, U.S. Department of Commerce, Jan 1977.

[NIST93] National Institute of Standards and Technology, "Secure Hash Standard," U.S. Department of Commerce, May 93.

[Pal96a] G.S. Pall, "Microsoft Point-to-Point Compression (MPPC) Protocol," Network Working Group Internet Draft, Jul 1996.

[Pal96b] G.S. Pall, "Microsoft Point-to-Point Encryption (MPPE) Protocol," Network Working

Group Internet Draft, Jul 1996.

[PZ98] G.S. Pall and G. Zorn, "Microsoft Point-to-Point Encryption (MPPE) Protocol," Network Working Group, Internet Draft, IETF, Mar 1998.

[Ran96] D. Rand, "The PPP Compression Control Protocol (CCP)," Network Working Group, RFC 1962, Jun 1996. <ftp://ftp.isi.edu/in-notes/rfc1962.txt>.

[RP94] J. Reynolds and J. Postel, "Assigned Numbers," Networking Group, Std 2, RFC 1700, Oct 1994. <ftp://ftp.isi.edu/in-notes/rfc1700.txt>.

[Riv91] R.L. Rivest, "The MD4 Message Digest Algorithm," Advances in Cryptology --- CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 303--311. [Sch96] B. Schneier Applied Cryptography, 2nd Edition, John Wiley & Sons, 1996.

[Sim94] W. Simpson, "The Point-to-Point Protocol (PPP)," Network Working Group, STD 51, RFC 1661, Jul 1994. <ftp://ftp.isi.edu/in-notes/rfc1661.txt>.

[Sim96] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)" Network Working Group, RFC 1334, Aug 1996. <ftp://ftp.isi.edu/in-notes/rfc1994.txt>.

[ZC98] G. Zorn and S. Cobb, "Microsoft PPP CHAP Extensions," Network Working Group Internet Draft, Mar 1998.