УДК 004.7(075)

ИССЛЕДОВАНИЕ СПОСОБОВ ЗАЩИТЫ VPN СОЕДИНЕНИЯ НА ПРИМЕРЕ ПРОТОКОЛА IPSEC.

Волошенко А.Н., Кратинов А.Г., Маркин Н.А.
Восточноукраинский национальный университет имени Владимира Даля
кафедра автоматизации и компьютерно-интегрированных технологий
E-mail: kratinov@bigmir.net

Аннотация

Волошенко А.Н., Кратинов А.Г., Маркин Н.А. Исследование способов защиты VPN соединения на примере протокола IPsec. *Рассмотрена архитектура безопасности для протокола сетевого уровня internet (IPsec), проанализирована её эффективность.*

Общая постановка проблемы. В последнее время в мире телекоммуникаций наблюдается повышенный интерес к так называемым Виртуальным Частным Сетям (Virtual Private Network – VPN). Это обусловлено необходимостью снижения расходов на содержание корпоративных сетей за счет более дешевого подключения удаленных офисов и удаленных пользователей через сеть Internet. Однако, необходимо отметить, что при объединении сетей через Internet, возникает вопрос о безопасности передачи данных, поэтому актуальной задачей является разработка и использование механизмов, позволяющих обеспечить конфиденциальность и целостность передаваемой информации.

Анализ последних исследований и публикаций. Существует множество протоколов для построения виртуальных частных сетей, самые популярные самые популярные из них - протоколы PPTP, L2TP [1,2]. При анализе безопасности этих протоколов обнаружены различные серьёзные уязвимости [3]. По этой причине рекомендуется применять дополнительные меры [4]. В то же время, некоторые теоретические и практические аспекты применения механизмов повышения информационной безопасности в виртуальных сетях освещены еще недостаточно.

Цель – анализ защиты VPN соединения на примере протокола IPsec.

Изложение основного материала исследований. Особенности архитектуры безопасности для протокола сетевого уровня internet (IPsec) объяснены в стандарте RFC-2401.

Основные компонентов архитектуры безопасности IPsec, рассматриваемые с точки зрения их функциональности и структуры:

- протоколы безопасности — “Заголовок аутентификации” (AH) и “Функция “повторного обрамления” защищаемой информации” (ESP);
- защищенный сеанс информационного обмена (защищенное виртуальное соединение) — что это такое, как это функционирует, как этим управлять, обработка информации для управления соединением;
- управление процедурами обмена и распределения ключевой информации — “вручную” и автоматически (IKE);
- алгоритмы аутентификации и шифрования.

IPsec использует два протокола для защиты трафика — протокол формирования “Заголовка аутентификации” (AH) и протокол, реализующий “Функцию “повторного обрамления” защищаемой информации” (ESP):

- AH обеспечивает целостность виртуального соединения (передаваемых данных), аутентификацию источника информации и дополнительную функцию по предотвращению повторной передачи пакетов;

- ESP может обеспечить конфиденциальность (шифрование) передаваемой информации, ограничение потока конфиденциального трафика. Кроме этого, он может обеспечить целостность виртуального соединения (передаваемых данных), аутентификацию источника информации и дополнительную функцию по предотвращению повторной передачи пакетов (Всякий раз, когда применяется ESP, в обязательном порядке должен использоваться тот или иной набор данных услуг по обеспечению безопасности.);
- AH и ESP являются специализированными средствами для контроля доступа, основанного на процедурах распределения криптографических ключей и управления потоками трафика, который формируется в связи с применением этих протоколов безопасности.

Эти протоколы могут использоваться каждый индивидуально или комбинации друг с другом с целью обеспечения выбранного набора услуг по обеспечению безопасности для IPv4 и IPv6. Каждый протокол может использоваться в двух режимах: транспортном режиме и режиме туннелирования. В транспортном режиме как правило обеспечивается защита протоколов верхних уровней архитектуры INTERNET; в режиме туннелирования обеспечивается туннелирование IP-пакетов (IPsec-туннель).

IPsec предоставляет пользователю (или системному администратору) возможность управления количеством формируемых IPsec-туннелей в соответствии с выбранной процедурой обеспечения безопасности. Например, он может сформировать только один криптографический туннель для транслирования всего трафика между двумя шлюзами безопасности или несколько отдельных криптографических туннелей для каждого TCP-соединения (сеанса связи) между каждой парой IP-узлов, соединенных через эти шлюзы безопасности.

Концепция “Защищенного виртуального соединения” (“Security Association” — SA) является фундаментальной в IPsec-архитектуре.

SA представляет собой симплексное соединение, которое формируется процедурами обеспечения безопасности для транспортирования по нему соответствующего трафика. При реализации услуг безопасности формируется SA на основе использования протоколов AH и ESP (либо обоих одновременно). Последние могут формировать два и более SA для защиты трафика. Как правило, при организации дуплексного виртуального соединения (если оно востребовано) между двумя IP-узлами или двумя шлюзами безопасности фомируются два SA (каждое для одного направления).

SA имеет уникальный маркер, состоящий из трех элементов:

- индекса параметра безопасности;
- IP-адреса назначения (доставки информации);
- идентификатора протокола безопасности (AH или ESP).

В принципе, IP-адрес назначения может быть индивидуальным (unicast address, то есть IP-узел ⇨ IP-узел), либо широковещательным (broadcast ad-dress, то есть IP-узел ⇨ IP-узлы), либо групповым (multicast group address, то есть IP-узлы ⇨ IP-узлы). Однако в IPsec-архитектуре рассматриваются только индивидуальные IP-адреса. SA определен в соответствии с концепцией межтерминального (сквозного) соединения (“point-to-point”).

Набор услуг по обеспечению безопасности, предлагаемый SA зависит от выбранного протокола безопасности, режима функционирования SA, конечных терминалов SA и выбора дополнительных функций в рамках протокола безопасности. Например, протокол AH обеспечивает аутентификацию источника информации и целостность последней для IP-пакетов.

Протокол AH также обеспечивает процедуру блокирования повторной передачи IP-пакетов (как часть процедуры обеспечения целостности информации) “по усмотрению” приемного терминала (это помогает противодействовать атакам типа “отказ в обслуживании”). Этот протокол наиболее приемлем, когда не требуется процедура

обеспечения конфиденциальности (или когда нет разрешения, например, вследствие правительственных ограничений на применение шифрования). Кроме этого, AH способен “аутентифицировать” выбранные поля заголовка IP-пакета, содержание которых может понадобиться для нормального функционирования сетевых компонентов. Например, AH может обеспечить целостность поля “Услуги” (при использовании IPv4) или дополнительных полей (при использовании IPv6) заголовка IP-пакета, если необходимо защитить маршрутную информацию от возможной ее модификации, обеспечив тем самым корректный маршрут доставки данных (за исключением, пожалуй, непредсказуемых изменений отдельных частей заголовка IP-пакета).

Протокол ESP дополнительно обеспечивает процедуру шифрования трафика. (Надежность данной процедуры зависит, в частности, от используемого алгоритма шифрования.) Кроме этого, ESP обеспечивает процедуру аутентификации. Если последняя востребована в рамках SA протокола ESP, то приемный терминал может “усилить” эту процедуру путем выбора дополнительной функции блокирования повторной передачи IP-пакетов с такими же параметрами, как и при использовании протокола AH. Однако, процедура аутентификации, предлагаемая протоколом ESP, немного “заужена” по сравнению с аналогичной, предлагаемой протоколом AH (то есть “внешний” ESP-заголовок в рамках IP-заголовка не защищается). Если протоколы верхних уровней нуждаются в процедуре аутентификации, то в этом случае последняя, предлагаемая протоколом ESP, является более предпочтительной, так как более эффективно использует поля заголовка IP-пакета по сравнению с протоколом AH совместно с ESP в режиме туннелированния.

Атаки на AH, ESP. Все виды атак на компоненты IPSec можно разделить на следующие группы: атаки, эксплуатирующие конечность ресурсов системы (типичный пример - атака "Отказ в обслуживании", Denial-of-service или DOS-атака), атаки, использующие особенности и ошибки конкретной реализации IPSec и, наконец, атаки, основанные на слабостях самих протоколов AH и ESP. Чисто криптографические атаки можно не рассматривать - оба протокола определяют понятие "трансформ", куда скрывают всю криптографию. Если используемый криптоалгоритм стоек, а определенный с ним трансформ не вносит дополнительных слабостей (это не всегда так, поэтому правильнее рассматривать стойкость всей системы - Протокол-Трансформ-Алгоритм), то с этой стороны все нормально.

Replay Attack - нивелируется за счет использования Sequence Number (в одном единственном случае это не работает - при использовании ESP без аутентификации и без AH). Далее, порядок выполнения действий (сначала шифрация, потом аутентификация) гарантирует быструю отбраковку "плохих" пакетов (более того, согласно последним исследованиям в мире криптографии, именно такой порядок действий наиболее безопасен, обратный порядок в некоторых, правда очень частных случаях, может привести к потенциальным дырам в безопасности; к счастью, ни SSL, ни IKE, ни другие распространенные протоколы с порядком действий "сначала аутентифицировать, потом зашифровать", к этим частным случаям не относятся, и, стало быть, этих дыр не имеют). Остается Denial-Of-Service атака. Как известно, это атака, от которой не существует полной защиты. Тем не менее, быстрая отбраковка плохих пакетов и отсутствие какой-либо внешней реакции на них (согласно RFC) позволяют более-менее хорошо справляться с этой атакой. В принципе, большинству (если не всем) известным сетевым атакам (sniffing, spoofing, hijacking и т.п.) AH и ESP при правильном их применении успешно противостоят.

С криптографией несколько сложнее, - она не вынесена, как в AH и ESP, отдельно, а реализована в самом протоколе. Тем не менее, при использовании стойких алгоритмов и примитивов (PRF), проблем быть не должно. В какой-то степени можно рассматривать как слабость IPsec то, что в качестве единственного обязательного к реализации криптоалгоритма в нынешних спецификациях указывается DES (это справедливо и для ESP),

56 бит ключа которого уже не считаются достаточными. Тем не менее, это чисто формальная слабость - сами спецификации являются алгоритмо-независимыми, и практически все известные вендоры давно реализовали 3DES (а некоторые уже и AES).Таким образом, при правильной реализации, наиболее "опасной" атакой остается Denial-Of-Service.

Выводы. Подводя итог необходимо раскрыть также все отрицательные стороны применения протокола. Несмотря на бесспорные плюсы использования данной технологии, негативные элементы могут нивелировать пользу. И как следствие ставить под вопрос эффективность использования IPsec-протоколов.

Применение IPsec-протоколов требует дополнительных вычислительных затрат от IP-узлов и шлюзов безопасности, которые имеют программные IPsec-модули в составе своих программных комплексов. Эти вычислительные затраты связаны, в первую очередь, с необходимостью выделения ресурсов памяти для хранения машинного IPsec-кода и информационных структур (например, баз данных для SA), вычисления контрольных сумм для обеспечения целостности данных, шифрования и расшифрования и дополнительной обработки каждого IP-пакета. Вычислительные затраты на обработку каждого IP-пакета могут быть вызваны увеличением времени задержки и, возможно, всеобщим замедлением процесса. Применение SA и протоколов управления распределением ключевой информацией, особенно это касается криптографии с открытыми ключами, также требует дополнительных вычислительных затрат при использовании IPsec-протоколов. Эти затраты будут вызваны увеличением времени задержки, вызванной формированием защищенного виртуального соединения. Для большинства IP-узлов, это означает, программные криптомодули не будут существенно снижать производительность системы, однако для шлюзов безопасности и отдельных IP-узлов могут потребоваться аппаратно-программные комплексы (так как они представляют собой крупные комплексы технических средств).

Применение IPsec-протоколов также приводит к увеличению нагрузки на сеть (приемопередающие, коммутационные и маршрутизационные компоненты инфраструктуры Internet). Это связано с ростом трафика и повышением необходимой пропускной способности для его транспортировки. Это является очевидным следствием увеличения размеров IP-пакетов, связанного с добавлением AH- и/или ESP-заголовков при транслировании трафика и вторых IP-заголовков (AH- и ESP-протоколы) при туннелировании трафика, и появления дополнительного трафика, связанного с функционированием протоколов управления распределением ключевой информацией.

Это означает, что в большинстве компонентов такое увеличение необходимой пропускной способности для доставки возросшего трафика не приведет к каким-либо негативным последствиям для Internet-инфраструктуры. Однако, для некоторых компонентов негативные последствия будут весьма существенны, например, для коммутируемых телефонных линий доступа в сеть. В последнем случае, время передачи шифрованного (ESP-протокол) трафика резко возрастет, если не принять дополнительных мер по компрессии (сжатию) данных может возникнуть задержка. Такая задержка может негативно повлиять на протокол транспортного уровня и прикладной процесс.