ОСОБЕННОСТИ ТЕСТИРОВАНИЯ СЕРВИСОВ БЕЗОПАСНОСТИ СЕТЕВОГО УРОВНЯ IPSEC ВТОРОЙ ВЕРСИИ

В.З. Шнитман, А.В. Никешин, Н.В. Пакулин

Семейство протоколов безопасности Интернет (IPsec) разрабатывается с целью предоставления сервисов безопасности на сетевом уровне стека протоколов TCP/IP. Предлагаемый набор сервисов безопасности включает контроль доступа, целостность дейтаграмм, аутентификацию источника данных, обнаружение и отклонение повторно воспроизводимых сообщений, конфиденциальность трафика. Эти сервисы предлагают стандартный метод защиты для всех протоколов, которые могут работать на сетевом уровне стека TCP/IP/IPv6 и выше (включая сами IPv4 и IPv6, TCP, UDP).

Большинство сервисов безопасности предоставляются двумя протоколами, протоколом аутентифицирующего заголовка (AH) и протоколом инкапсулирующей защиты блока данных (ESP), а также протоколами управления криптографическими ключами.

После публикации в 1998 году спецификаций IPsec они были подвергнуты всестороннему анализу. Выявленные в процессе критического анализа недостатки способствовали лучшему пониманию их особенностей и послужили причиной продолжения исследований в этой области. В результате в 2005 году была опубликована новая версия спецификаций (RFC 4301-4309). Архитектура IPsec (RFC 4301) [1] сохранила основные черты первой версии, однако был внесен ряд существенных изменений:

- Переопределены элементы политик безопасности: каждая политика теперь может задаваться несколькими несвязанными наборами селекторов, по которым определяется применимость политики к конкретному проходящему трафику.
- Функция пересылки (маршрутизации) отделена от политик безопасности. Больше не требуется поддержка вложенных контекстов безопасности («связок SA»).
- Специфицирован единый алгоритм отображения входных IPsec-дейтаграмм на контексты безопасности (SA).
- Протокол AH (цифровая подпись сообщений) больше не является обязательным, так как аналогичную функциональность предоставляет протокол шифрования данных ESP.
- Добавлены несколько подходов к обработке фрагментов открытого текста на защищенной стороне границы IPsec.
- Реализации IPsec теперь позволено фрагментировать IPv4 пакеты до применения IPsec.
- На маршрутизаторах с поддержкой защиты IPsec (защитных шлюзах) разрешена поддержка нескольких контекстов IPsec для разных абонентов.
- По умолчанию автоматическим протоколом управления ключами выбран IKEv2. IKEv2 представляет собой новый протокол, созданный на основе IKEv1 (RFC 2407, 2408, 2409), с целью его упрощения и оптимизации.

Спецификация протоколов AH и ESP (RFC 4302, 4303), незначительно отличается от предыдущей версии (RFC 2402, 2406):

- Улучшена конфиденциальность потоков трафика, добавлена возможность использовать фиктивные пакеты (Next Header = 59).
- Добавлены алгоритмы режима комбинированной конфиденциальности. Список обязательных для реализации алгоритмов перенесен в отдельный документ. Благодаря этому, эти алгоритмы могут обновляться или заменяться, не оказывая влияния на процесс стандартизации остального набора документов IPsec.
- Добавлена новая опция 64-битового порядкового номера (Extended Sequence Number) для высокоскоростных соединений.

С 2004-го года ИСП РАН ведет работы по созданию формальных спецификаций и тестового набора [3] для проверки соответствия реализаций IPsec первой версии стандарту протокола (RFC 2401[2], 2402, 2406). В настоящее время осуществляется перенос и дополнение разработанного тестового набора до второй версии IPsec. Ниже мы кратко представляем основные изменения, внесенные в тестовый набор и формальные спецификации IPsec v1 для поддержки обновленной спецификации безопасности сетевого уровня IPsec v2.

Для тестирования реализации семейства протоколов IPsec на соответствие новой спецификации, была разработана тестовая модель. В отличие от ранее разработанной нашей группой тестовой модели для предыдущего поколения протоколов IPsec, в ней учтены вышеперечисленные изменения и другие требования, в том числе:

- Реализована новая структура управляющих баз данных (SPD, SAD), а также добавлена новая база данных авторизации партнеров (PAD)
- Изменены алгоритмы поиска политик и контекстов безопасности.
- Изменены алгоритмы построения IPsec заголовков.
- Добавлена возможность использовать фиктивные пакеты (Next Header = 59)

Необходимо отметить, что архитектура тестового набора, выбранная при разработке тестового набора для первой версии протоколов безопасности IPsec v2, не претерпела изменений. Изменения коснулись только семантики спецификации и генераторов тестовых воздействий, которые были обновлены для поддержки новых функциональных требований и форматов сообщений.

Разработаны тесты для проверки функционирования реализации IPsec в соответствии со спецификацией. Поскольку независимой реализации IPsec нами не обнаружено, то для тестирования были выбраны ОС FreeBsd 6.2 и OpenBsd 4.2, использующие реализацию IPsec KAME Project.

Проект выполняется при поддержке РФФИ, грант № 070700243 «Верификация функций безопасности протокола нового поколения IPsec v2.».

ЛИТЕРАТУРА:

1. IETF RFC 4301. S. Kent, K. Seo. Security Architecture for the Internet Protocol. December 2005. 101 c. (http://www.ietf.org/rfc/rfc4301.txt)
2. IETF RFC 2401. S. Kent, R. Atkinson. Security Architecture for the Internet Protocol. November 1998. 66 c. (http://www.ietf.org/rfc/rfc2401.txt)
3. Ключников Г.В., Пакулин Н.В., Шнитман В.З. Автоматизированное тестирование сетевых сервисов Интернет-протокола. // Научный сервис в сети ИНТЕРНЕТ. Труды Всероссийской научной конференции, М.: Изд-во МГУ, 2005. С. 168-170