IPsec в пост-квантовую эру

История создания, текущее состояние и дальнейшее развитие протокола IPsec в пост-квантовую эру.

Валерий Смыслов, архитектор системы, АО "ЭЛВИС-ПЛЮС".

Введение

В мире существует ряд протоколов, позволяющих обращаться к устройствам хранения данных через TCP/IP, например, iSCSI – Internet Small Computer System Interface или iFCP – Internet Fibre Channel Protocol. При этом критически важной становится задача защиты передаваемой информации, и для ее решения в этих случаях предполагается использовать протокол, называемый IPsec (или IP Security).

История создания IPsec

Протокол IPsec, а точнее, целое семейство протоколов, начал разрабатываться в IETF (Internet Engineering Task Force) еще в 1992 году. В то время активно продвигался протокол IPv6, и идея заложить в него возможность криптографической защиты данных на сетевом уровне казалась весьма привлекательной. В результате в 1995 году появились два протокола – AH (Authentication Header) и ESP (Encapsulating Security Payload). Первый обеспечивал аутентификацию и целостность IP-пакета, второй – его конфиденциальность; предполагалось, что они будут использоваться совместно. Через три года эти протоколы были обновлены, при этом в ESP также появилась возможность обеспечивать аутентификацию и целостность IP-пакета в дополнение к его конфиденциальности, что позволило в большинстве случаев обходиться без AH. В дальнейшем в ESP была добавлена опция инкапсуляции в UDP для совместимости с существующими трансляторами сетевых адресов (NAT, Network Address Translator), что со временем привело практически к полному исчезновению AH из реальной жизни. Последняя, во многом косметическая, ревизия AH и ESP была сделана в 2005 году, и с тех пор эти протоколы остаются неизменными, а их основа сохраняется с 1998 года.

Столь длительный срок их активного использования, в первую очередь, объясняется простотой этих протоколов – уже в самом начале было решено отделить протокол управления ключами от непосредственно протоколов защиты данных, при этом последние получились простыми и фактически определяют только формат инкапсуляции IP-пакета. Совсем другая история имела место с протоколом управления ключами. Именно он по замыслу разработчиков должен был обеспечить AH и ESP ключевой информацией, согласовать криптографические алгоритмы, обеспечить взаимную аутентификацию партнеров и т.д. Работа над таким протоколом началась в IETF практически одновременно с работой над ESP и AH, но задача была существенно сложней и заняла больше времени. Только в 1998 году появился протокол с претенциозным названием IKE – Internet Key Exchange. Надо сказать, что, в отличие от многих протоколов (например, SSL – Secure Socket Layer), IKE с самого начала разрабатывался с участием представителей академических кругов и имел надежную криптографическую основу. В частности, он одним из первых базировался на протоколе аутентифицированного обмена ключами SIGMA Хьюго Кравчика, на котором сегодня строится большинство протоколов управления ключами и который до сих пор считается наиболее передовым в этой области. Тем не менее, в процессе разработки первой версии IKE было допущено много инженерных просчетов: протокол получился чрезмерно усложненным, медленным, недостаточно устойчивым к DoS-атакам (Denial of Service) и плохо расширяемым.

Как следствие, вскоре после появления на свет IKE версии 1 в IETF осознали необходимость его замены, и в этот раз постарались учесть допущенные ошибки. В результате в 2005 году появился IKE версии 2, который стал основным протоколом управления ключами в IPsec. В 2010 и в 2016 годах IKEv2 прошел во многом косметические ревизии, не затронувшие ядро протокола. Что касается IKE первой версии, то из-за наличия многочисленных проблем он получил статус «не рекомендованный к использованию», однако этот протокол до сих пор продолжает применяться в некоторых IPsec-продуктах, в частности, в России.

IKEv2 в двух словах

Задача IKEv2 – провести аутентифицированный обмен ключами между двумя партнерами, в результате которого должно создаться защищенное соединение, по которому партнеры смогут обмениваться данными. В IPsec защищенное соединение принято называть SA (Security Association), и оно включает в себя, помимо общего ключа, также такую информацию, как криптографические алгоритмы, которые будут использоваться для защиты данных; режимы их использования; характеристики IP-трафика, подлежащего защите и т.п. Каждое защищенное соединение характеризуется уникальным идентификатором, называемым SPI (Security Parameter Index), что позволяет иметь несколько одновременно существующих SA между двумя партнерами. Таким образом, задача IKEv2 состоит в создании, обновлении и удалении защищенных соединений ESP (рис. 1).

Предполагается, что каждый из партнеров имеет политику безопасности, которая определяет, какие именно криптографические алгоритмы могут быть использованы для защиты данных, какой вид IP-трафика должен защищаться, какие дополнительные параметры должно иметь защищенное соединение, с кем именно оно должно создаваться и т.д. Кроме того, каждая из сторон владеет некоторой секретной информацией, позволяющей партнерам аутентифицировать друг друга. Протокол IKEv2 допускает использование различных методов аутентификации, поэтому эта информация может быть, например, в виде предварительно распределенного симметричного ключа (PSK, PreShared Key) или в виде закрытого ключа подписи.

Заметим, что, как и у своего предшественника, криптографической основой IKEv2 является протокол SIGMA, который предполагает, что секретная информация, которой обладают партнеры, ни-

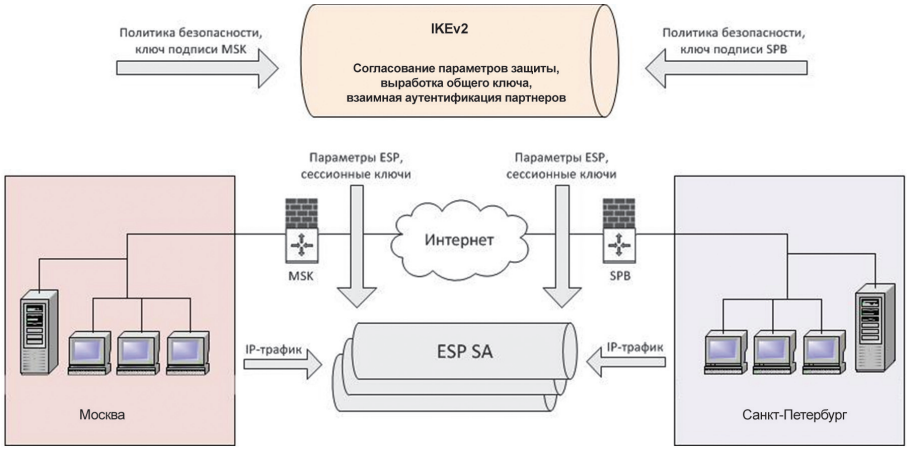

Рис. 1. Архитектура IPsec.

когда не используется для вычисления сеансовых ключей, применяемых для защиты данных; она используется только для аутентификации партнеров. Это крайне важно с точки зрения криптографии, т.к. обеспечивает наличие у протокола свойства, называемого «совершенная прямая секретность» (PFS – Perfect Forward Secrecy), заключающегося в том, что при компрометации любого ключа в системе (включая долговременные ключи) противник получает доступ только к ограниченному объему защищаемой информации. Свойство PFS считается крайне важным с точки зрения современной криптографии, и IKEv2 обладает этим свойством во всех режимах его использования (например, широко используемый протокол TLS (Transport Layer Security) вплоть до версии 1.3, принятой в 2018 году, обеспечивал PFS далеко не во всех режимах).

Протокол IKEv2 использует UDP в качестве транспорта и, как правило, создает ESP SA за два обмена сообщениями между партнерами. В первом обмене, называемом IKE_SA_INIT, стороны проводят согласование криптографических алгоритмов, которые будут использоваться для защиты самого IKE, обмениваются нонсами и открытыми ключами Диффи-Хеллмана, а также могут согласовывать использование различных расширений протокола. Протокол IKEv2 предполагает, что партнеры используют эфемерные ключи Диффи-Хеллмана, то есть для каждого нового соединения закрытые ключи вырабатываются случайным образом, что позволяет обеспечить свойство PFS. Кроме того, IKEv2 не накладывает ограничений на механизм выработки разделяемого секрета, то есть это может быть классический протокол Диффи-Хеллмана на основе дискретных логарифмов или более современный его вариант, базирующийся на свойствах эллиптических кривых.

Если все прошло успешно, то после завершения обмена IKE_SA_INIT обе стороны имеют согласованный набор алгоритмов для защиты IKE, разделяемый секрет и понимание того, какие расширения протокола могут быть использованы. Возможны две ситуации, при которых потребуется выполнить обмен IKE_SA_INIT еще раз. Первая ситуация – когда инициирующая сторона отослала открытый ключ, соответствующий алгоритму, по какой-то причине неприемлемому для отвечающей стороны (например, неподдерживаемая эллиптическая кривая). В этом случае инициатор должен выработать новый ключ для одного из взаимопреемлемых алгоритмов и заново послать IKE_SA_INIT. Вторая ситуация возможна, когда отвечающая сторона получает слишком много сообщений IKE_SA_INIT, на которые она исправно отвечает (что требует выполнения достаточно ресурсоемких действий и сохранения состояния), но дальнейшего продолжения со стороны инициатора не следует. Это ведет к исчерпанию ресурсов отвечающей стороны и воспринимается как DoS-атака. Для отсечения запросов, направленных с «фейковых» IP-адресов, используется механизм, называемый куки (cookie). Суть его заключается в том, что отвечающая сторона не сохраняет состояние до подтверждения того, что запрос пришел с реального IP-адреса. Для этого инициатору в ответ отсылается блок данных, называемый куки, а инициатор должен повторить свой запрос, включив в него полученный куки. При этом куки вычисляется таким образом, что отвечающая сторона может проверить его корректность, не сохраняя при этом никакой информации о самом запросе. Если присланный куки является правильным, то это означает, что по крайней мере инициатор является «живым» субъектом, и запрос пришел с реального IP-адреса.

За обменом IKE_SA_INIT следует второй обмен, называемый IKE_AUTH. К этому моменту стороны уже вычислили разделяемый секрет, и все сообщения IKE, начиная с IKE_AUTH, посылаются в зашифрованном виде. Однако партнеры еще не аутентифицировали друг друга, то есть не исключена ситуация наличия человека-в-середине (Man-in-the-Middle). Основная задача обмена IKE_AUTH – провести такую аутентификацию, тем самым завершив создание защищенного соединения. В соответствии с протоколом SIGMA, каждая из сторон вычисляет цифровую подпись (или MAC, Message Authentication Code, в случае, если аутентификация проводится на симметричных ключах) блока данных, включающего в себя сообщение IKE_SA_INIT, нонс партнера и значение MAC от собственного имени, вычисленное на разделяемом секрете. Такая конструкция позволяет связать воедино все компоненты протокола и средствами криптографии удостоверяет, что данная сессия, в которой был вычислен данный разделяемый секрет, была создана именно этими партнерами, и никто другой в этом не участвовал.

Помимо аутентификации в IKE_AUTH, стороны согласуют алгоритмы, которые будут использоваться в ESP (алгоритмы, которые использует сам IKE, согласовываются на предыдущем этапе), обмениваются информацией о параметрах защищаемого IP-трафика (рис. 2), а также могут проводиться дополнительные действия по конфигурированию ESP SA (например, назначение адреса из внутренней подсети).

Таким образом, после завершения двух обменов IKE_SA_INIT и IKE_AUTH стороны получают ESP SA. Дополнительные защищенные соединения ESP могут создаваться упрощенным способом, за один обмен, т.к. партнеры уже аутентифицировали друг друга. Для этой цели служит обмен CREATE_CHILD_SA, он же используется для обновления сеансовых ключей. Кроме того, в IKEv2 есть еще один обмен – INFORMATIONAL, используемый для самых разнообразных целей: удаления SA, отсылки сообщений об ошибках, проверки жизнеспособности партнера и т.п.

Что дальше?

С момента принятия IKEv2 прошло уже 14 лет. В отличие от своего предшественника, протокол оказался удачным и, что важно, позволяющим достаточно легко добавлять в себя новую функциональность. За эти годы было разработано порядка десятка различных расширений протокола, и этот процесс продолжается. В короткой статье невозможно рассказать обо всех, поэтому остановимся на самом, с нашей точки зрения, интересном – на работе по адаптации IKEv2 к функционированию в условиях существования квантовых компьютеров.

Квантовые компьютеры существуют пока только в «игрушечном» виде, и до сих пор непонятно, можно ли вообще создать полномасштабный квантовый компьютер с числом кубитов (квантовый аналог бита) порядка, скажем, нескольких тысяч. Но, несмотря на то, что их нет, алгоритмы для них уже есть, и эти алгоритмы являются кошмарным сном для криптографов всего мира. В частности, алгоритм Гровера фактически уменьшает эффективную длину ключа любого симметричного алгоритма в два раза. Иными словами, при использовании ключей размером в 256 бит их стойкость будет соответствовать ключам размером в 128 бит. Это неприятно, но не смертельно, т.к. 128 бит – почти такая же «бесконечная» величина для полного перебора, как и 256. Гораздо страшнее алгоритм Шора – он позволяет квантовым компьютерам соответствующего размера «взламывать» любой алгоритм с открытым ключом (например, вычисление разделяемого секрета по Диффи-Хеллману или цифровую подпись) за полиномиальное время. Фактически это означает, что все протоколы, использующие криптографию с открытым ключом, а таковых сейчас подавляющее большинство, окажутся в одночасье уязвимыми, как только инженеры смогут создать полноразмерный квантовый компьютер. А это может случиться (если вообще случится)

Рис. 2. Создание защищенного соединения в IKEv2.

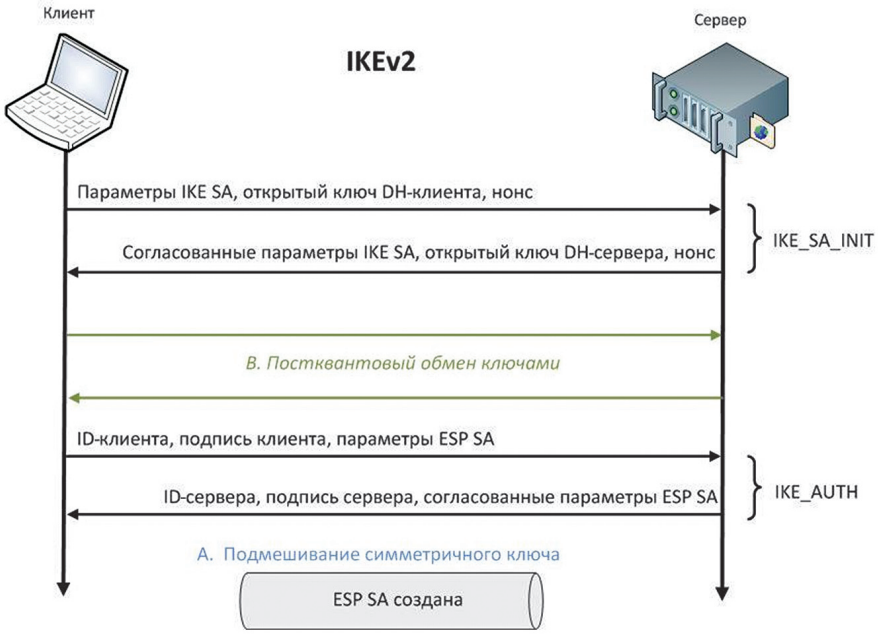

Рис. 3. Варианты противодействия квантовым компьютерам в IKEv2.

достаточно скоро, по некоторым прогнозам в пределах 20 лет (такая оценка, например, дается в меморандуме NIST (National Institute of Standards and Technology), опубликованном в апреле 2016 года).

Так или иначе, но угроза (реальная или мнимая) появления полноразмерных квантовых компьютеров привела к тому, что в последнее время в существующие протоколы стали добавлять механизмы, позволяющие каким-то образом ей противодействовать. Этот процесс только начался, и протокол IKEv2 в настоящее время является одним из наиболее передовых в этом направлении.

Какие же контрмеры предполагается использовать? Сегодняшняя наука видит два основных пути противодействия квантовым компьютерам.

Первый путь предполагает частичный отказ от криптографии с открытым ключом в пользу симметричной криптографии. Как уже было сказано выше, квантовые алгоритмы не приведут к катастрофическим последствиям для симметричной криптографии, а снижение эффективной длины ключа вдвое не является критическим при правильном ее выборе. В частности, использование ключей длиной 256 бит считается безопасным даже с учетом появления квантовых компьютеров. Однако полный отказ от криптографии с открытым ключом нежелателен, так как неизбежно приведет к проблемам с масштабируемостью, неотказуемостью аутентификации, отсутствием PFS и т.д. Поэтому разрабатываются комбинированные схемы, когда симметричные ключи используются совместно с открытыми ключами. Такое решение не является оптимальным и рассматривается как временное, его основная задача – защитить от квантовых компьютеров сегодняшние коммуникации: предполагается, что противник может записывать зашифрованный трафик много лет, не имея возможности его расшифровать, а с появлением квантовых компьютеров такая возможность у него появится. Комбинированная схема с добавлением симметричного ключа позволяет это предотвратить. Такая комбинированная схема уже разработана для IKEv2 и находится в стадии стандартизации.

Второй – «правильный» путь заключается в использовании так называемой «постквантовой» криптографии, которая предполагает замену уязвимых примитивов с открытым ключом на аналогичные по функциональности, но стойкие к квантовым компьютерам. Замечание: не надо путать «пост-квантовую» криптографию с «квантовой» криптографией, под которой сейчас подразумевается так называемое «Квантовое Распределение Ключей» (QKD – Quantum Key Distribution), то есть передача ключей по оптическим каналам связи с использованием квантовых эффектов таким образом, что ключ не может быть считан по дороге, не будучи при этом изменен. Квантовое распределение ключей бурно развивается в последнее время, но имеет ряд непреодолимых на сегодняшний день проблем: ограниченная дальность передачи (десятки-сотни километров), малая скорость, необходимость аутентифицировать переданные ключи посредством других ключей и т.п.

Возвращаясь к пост-квантовой криптографии: в настоящее время американский институт по стандартизации NIST проводит второй этап конкурса по выбору постквантовых примитивов. Достаточно сказать, что во втором этапе участвуют 17 кандидатов по шифрованию с открытым ключом и обмену ключами и 9 по цифровой подписи, причем участвуют алгоритмы, построенные на самых разных математических принципах: решетки, коды исправления ошибок, изогении эллиптических кривых. Такое разнообразие свидетельствует о том, что у ученых пока нет полной уверенности в стойкости новых механизмов, и не все используемые принципы достаточно глубоко изучены. Такая ситуация толкает разработчиков протоколов на создание гибридных схем обмена ключами, когда несколько алгоритмов различных типов используются последовательно. Такая схема в настоящее время разрабатывается и для IKEv2. Заметим, что дополнительной проблемой является то, что практически все пост-квантовые примитивы имеют существенно больший размер открытых ключей (до десятков и даже сотен килобайт). Это приводит к дополнительным сложностям для IKEv2, т.к. он базируется на протоколе UDP, имеющем ограничения по размеру передаваемых данных и проблемы с прохождением фрагментированных IP-пакетов через NAT. Тем не менее, в процессе разработки механизма гибридного пост-квантового обмена ключами для IKEv2 все эти проблемы удалось успешно преодолеть, что еще раз подтверждает высокие функциональные качества протокола (рис. 3).

Заключение

Протокол продолжает развиваться, отвечая новым вызовам, и свой вклад в его развитие вносит и наша страна. В частности, представители компании ЭЛВИС-ПЛЮС активно участвуют в разработке расширений IKEv2 в IETF, в том числе и в работах по его адаптации к пост-квантовой эре.

Валерий Смыслов,
АО "ЭЛВИС-ПЛЮС".

Никто не защищен от кибератак

Август 2019 г. — Компания Check Point® Software Technologies Ltd. выпустила отчет Cyber Attack Trends: 2019 Mid-Year Report, в котором выявили ключевые тренды киберугроз в первом полугодии 2019**:**

- *мобильный банкинг*: количество атак возросло вдвое по сравнению с 2018 г.;
- *атака на цепь поставок*: киберпреступники могут расширить свое влияние, использовав атаку на цепочку поставок компании. При таком типе кибератаки хакеры внедряют вредоносный код непосредственно в программное обеспечение компании-жертвы. После выполнения этого вредоносного кода преступники могут получить доступ к приватной информации компании;
- *электронная почта*: злоумышленники используют различные методы для обхода решений безопасности и спам-фильтров. Например, они рассылают сложные закодированные электронные письма, а также сложный базовый код, который смешивает обычные текстовые буквы с символами HTML;
- *облачные хранилища*: растущая популярность общедоступных облачных сред привела к увеличению числа кибератак, нацеленных на огромные объемы конфиденциальных данных, находящихся на этих платформах. Самые серьезные угрозы для безопасности облаков в 2019 году – неправильная конфигурация и плохое управление облачными ресурсами.

«Ни облачные хранилища, ни наши смартфоны и электронная почта — ни одна среда не застрахована от кибератак. Такие угрозы, как персонализированные атаки вымогателей, DNS-атаки и криптомайнеры, будут по-прежнему актуальны в 2019 году», — отмечает Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ.