В. И. НОВИКОВ[1]
К. Г. КАЛЕНИК[1]

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКИХ СТАНДАРТОВ

[1]*Учреждение образования «Высший государственный колледж связи», Республика Беларусь*

Введение

Протоколы безопасности – это алгоритмы, использующие криптографию для достижения определённых целей безопасности. На практике эти протоколы регулируют, как вычислительные устройства осуществляют критические по отношению к безопасности задачи. Однако, в то время как органы по стандартизации делают свою работу превосходно, безопасность существующих протоколов значительно варьируется.

Поскольку стандарты тщательно разрабатываются экспертами, можно было бы надеяться на прочную гарантию безопасности. Однако эта надежда не всегда оправдывается. В то время как стандарты часто содержат детализированные функциональные описания, во многих из них отсутствует информация по безопасности. Вместо однозначных свойств безопасности и четких моделей угроз, многие стандарты криптографических протоколов, в лучшем случае, определяют высокоуровневые свойства безопасности и горстка сценариев угроз. Это отсутствие четких моделей угроз и детально описанных свойств лишает возможности дать объективную оценку качества протокола: без них нет ничего, что можно было бы объективно проверить.

В течении последних нескольких десятилетий для анализа малых протоколов с чётко определёнными моделями угроз и чёткими целями информационной безопасности успешно использовались формальные методы оценки. Для этих методов разрабатываются тестовые модели угроз и свойств безопасности, относительно которых будет осуществляться анализа стандарта.

В дальнейшем мы разберём виды проблем, которые возникают, когда в стандартах пренебрегают моделями угроз и свойствами безопасности, и продемонстрируем, насколько могут отличаться формальные методы. Также мы посмотрим, как формальные методы и связанные с ними инструменты могут быть улучшены. Для этого будем использовать три протокола WiMAX, EAP, и ISO/IEC 9798.

Стандарт WiMAX

Для начала рассмотрим стандарт беспроводной связи IEEE 802.16, также известный как WiMAX, который направлен на обеспечение "последней мили" беспроводного широкополосного доступа. WiMAX включает несколько механизмов, которые работают с ключами или используют криптографические операции. Основа механизма – этап авторизации, во время которого устанавливается открытый ключ, на котором базируется вся последующая безопасность. Эта авторизация может быть выполнена с использованием протокола EAP, или PKM, если таковые описаны.

Стандарт WiMAX впервые был предложен в 2001 году и с тех пор несколько раз обновлен. В первую версию был включён только протокол PKMv1-RSA. Этот протокол выполняется между абонентской станцией (SS) и базовой станцией провайдера (BS). Абонентская станция инициирует связь с базовой, отправляя свой сертификат, список поддерживаемых алгоритмов, а также уникальный идентификатор соединения (CID). Базовая станция генерирует ключ авторизации (AK) и отсылает его назад, зашифровав с открытым ключом абонентской станции. Также передаётся порядковый номер и срок жизни ключа, идентификатор ассоциации по безопасности, который мы назовём SAID. Эти обмены сообщениями могут быть представлены следующим образом:

(PKMv1-RSA)

SS → BS: SS_Certificate, SS_Algo_Suites, CID
BS → SS: $Enc_{PK(SS)}$(AK), SAID

В 2004 году Джонстон и Уокер [9] определили ряд недостатков первоначальной версии стандарта. В частности они утверждали, что PKMv1-RSA по существу не обеспечивает гарантии безопасности, поскольку, в контексте беспроводной передачи данных, следует предполагать, что атакующие могут подделывать (то есть отправить сообщения, выдавая себя за другую сторону) произвольные сообщения. Поэтому абонентская станция не имеет ни малейшего понятия, кто зашифровал или, даже, сгенерировал ключ.

Джонстон и Уокер утверждали, что протокол должен, по крайней мере, обеспечить взаимную аутентификацию, исходя из предположения, что атакующие могут подслушать и внедрять свои потоки данных. Их аргументы конечно были неформальными, так как стандарт не определял ни модели угрозы, ни какие-либо другие подробности о свойствах безопасности, которых она стремится достигать.

В 2005 году была выпущена новая версия стандарта – протокол PKMv2-RSA, с тремя обращениями, использующими цифровую подпись. Абонентская станция инициирует связь с базовой станцией, отправляя случайное число (SS_Random), его сертификат, и уникальный идентификатор соединения. Сообщение подписывается с использованием закрытого ключа RSA абонентской станции (SigSS). Базовая станция генерирует ключ (per-PAK), объединяет его с MAC-адресом абонента (SS_MAC), и шифрует результат открытым ключом. Результат отсылается обратно к абоненту вместе со случайным числом SS_Random, случайным числом базовой станции BS_Random, и сертификатом. Сообщение подписывается закрытым ключом базовой станции (SigBS). В третьем сообщении абонент подтверждает получение предыдущего сообщения, отсылая случайное число базовой станции назад и подписывая сообщение (SigSS').

(PKMv2-RSA)

SS → BS: SS_Random, SS_Certificate, CID, SigSS
BS → SS: SS_Random, $Enc_{PK(SS)}$(per-PAK||SS_MAC), BS_Random, SAID, BS_Certificate, SigSS
SS → BS: BS_Random, SigSS'

Кажется, что новый протокол был предназначен для устранения недостатков PKMv2-RSA. Но опять же, ни модель угрозы, ни свойства безопасности не были определены. Следовательно, хоть стандарт PKMv2-RSA и дополняет предыдущую версию новыми характеристиками, он их не обосновывает.

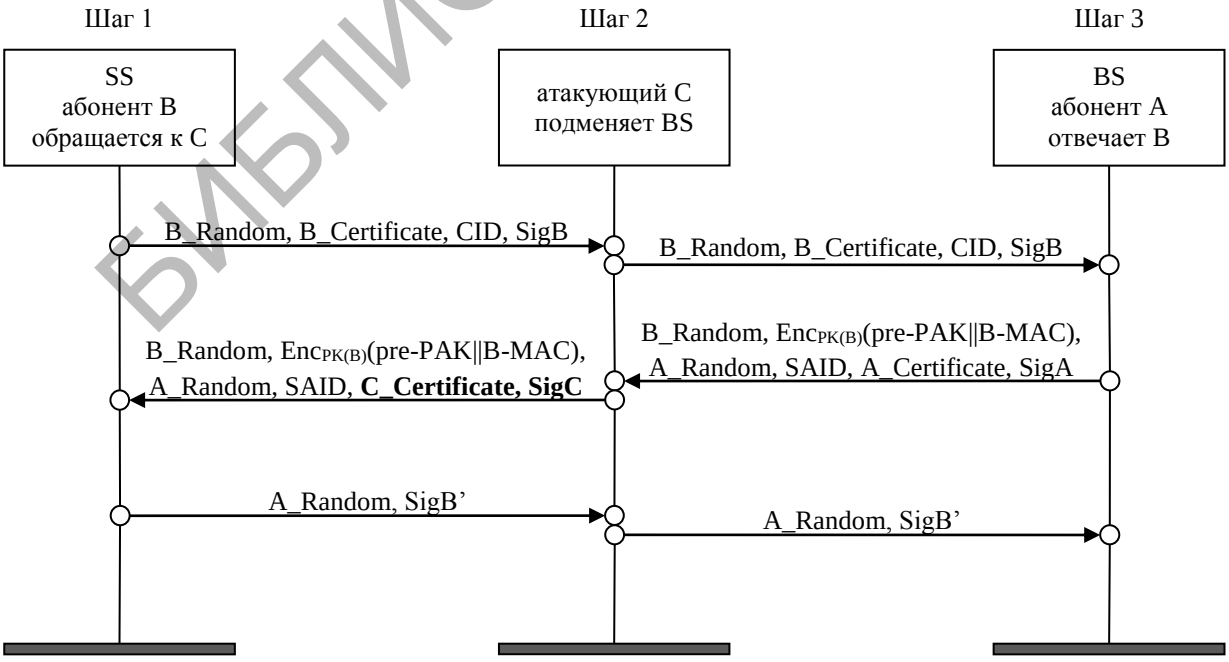

Рисунок 1: Атака "человек посередине" PKMv2-ЮАР. Абонент A считает, что B разговаривает с ним. На самом деле абонент B говорит с атакующим C.

На рисунке 1 приведена атака, при которой не удаётся выполнить однозначную аутентификацию пользователей. Причина этой проблемы заключается в том, что первое и третье сообщения не включают информации о легитимных абонентах. Атака может быть предотвращена путём простого добавления идентификационных данных базовой станции в третье сообщение.

Интересно, что, несмотря на эту атаку, злоумышленник не может ни подслушать последующие сообщения абонента B, ни отправить сообщения от его имени. Причин здесь две. Во-первых, посылая сообщение абоненту B, злоумышленник не может дешифровать ключ абонента A. Во-вторых, протокол сразу криптографически связывает коммуникационные идентификационные данные партнеров со всеми сообщениями. Таким образом, злоумышленник не может продолжать свою атаку. Эта "атака" – действительно является угрозой нарушения безопасности? Мы не можем ответить наверняка, т.к. стандарт не описывает ни свойства безопасности, ни модель угрозы. Если мы не рискуем предполагать, что PKMv2-RSA не обеспечивает надёжную безопасность, то криптографические операции, выполняемые в PKMv2-RSA и последующих версиях стандарта, являются избыточными. Фактически, мы могли бы отбросить третье сообщение PKMv2-RSA, не жертвуя безопасностью. Мы могли бы упростить протокол и уменьшить его коммуникационную сложность. Либо, мы могли бы поверить, что для PKMv2-RSA необходимо выполнять три аутентификации сообщений и игнорировать проблему "человек посредине". Однако, это может привести к серьёзным проблемам.

К сожалению, такое отсутствие описания модели угроз и свойств безопасности не единичный случай.

Стандарт EAP

Второй стандарт, который мы будем рассматривать, Extensible Authentication Protocol (EAP) разработанный инженерной группой по развитию интернета (IETF).

EAP – основа для аутентификации доступа к сети. Он поддерживает несколько протоколов аутентификации. Модель угрозы определяется предположением, что атакующий может скомпрометировать соглашения, по которым передаются пакеты EAP, используя одну из десяти упомянутых в протоколе атак. Несомненно, это источник неоднозначности: любая неописанная атака может рассматриваться из контекста модели угрозы.

Один из способов получения более точной модели угроз основывается на том, что мы рассматриваем существенные возможности атакующего. Из первых описанных атак следует: атакующий может подслушать, имитировать и модифицировать пакеты EAP. Далее в протоколе описаны определенные сценарии атак, которые являются следствиями этих трех возможностей: первый касается атак "отказ в обслуживании", а три других – определенных атак "человек посередине". Последний пункт списка рассматривает определенный сценарий, где атакующий может имитировать сообщения протокола нижнего уровня. Способность атакующего в этом случае не определяется только конкретным сценарием, но и предположением того, что сообщения нижнего уровня также находятся под контролем атакующего. Т.е. мы предполагаем, что атакующий в состоянии подслушать, имитировать, и модифицировать EAP и все пакеты нижнего уровня. Оставшиеся пункты утверждают, что атакующий может выполнить онлайн вычисления, такие как атаки с подбором по словарю паролей и атаки на слабые криптографические схемы.

Обратимся к свойствам безопасности. Метод аутентификации EAP должен указывать, какие свойства безопасности он утверждает. Ниже приведены важные для принятия точных решений свойства.

Защита целостности. Относится к аутентификации источника данных и защите от несанкционированного изменения информации для пакетов EAP (включая запросы EAP и ответы). Спецификация метода должна описывать пакеты EAP и поля, которые нужно защищать.

Повтор защиты. Относится к защите от повторения метода EAP или его сообщений, включая сообщения о состоянии.

Независимость сессии. Демонстрация того, что пассивные атаки (такие как получение разговора EAP), или активные атаки (включая взлом основных сеансовых ключей) не допускают компромисс последующих или предшествующих ключей.

Стандарт ISO/IEC 9798

Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) совместно разрабатывают стандарты для информационных технологий. В 1991 они опубликовали первую часть стандарта 9798, который определяет семейство протоколов аутентификации объекта.

1. A → B: $TN_A \,||\, Text_2 \,||\, f_{Kab}(TN_A \,||\, I_B \,||\, Text_1)$
2. B → A: $TN_B \,||\, Text_4 \,||\, f_{Kab}(TN_B \,||\, I_A \,||\, Text_3)$

Рисунок 2: версия 2009 года ISO/IEC 9798 протокол взаимной аутентификации с двумя передачами, использующий криптографическую функцию проверки.

Начиная с 1991 года, части стандарта были пересмотрены несколько раз, чтобы выделить недостатки и неоднозначности. Однако, не совсем ясно, какие свойства безопасности обеспечиваются протоколами стандарта. Стандарт вводит формулировки "аутентификацию объекта" и "аутентификация идентификационных данных истца". Есть несколько возможных истолкований этих понятий, что делает чрезвычайно усложняет проверку надёжности аутентификации. Точно так же, как распространено во многих стандартах, модель угрозы только определяется с точки зрения неформальных типов атаки, таких как "атака ролевой путаницы".

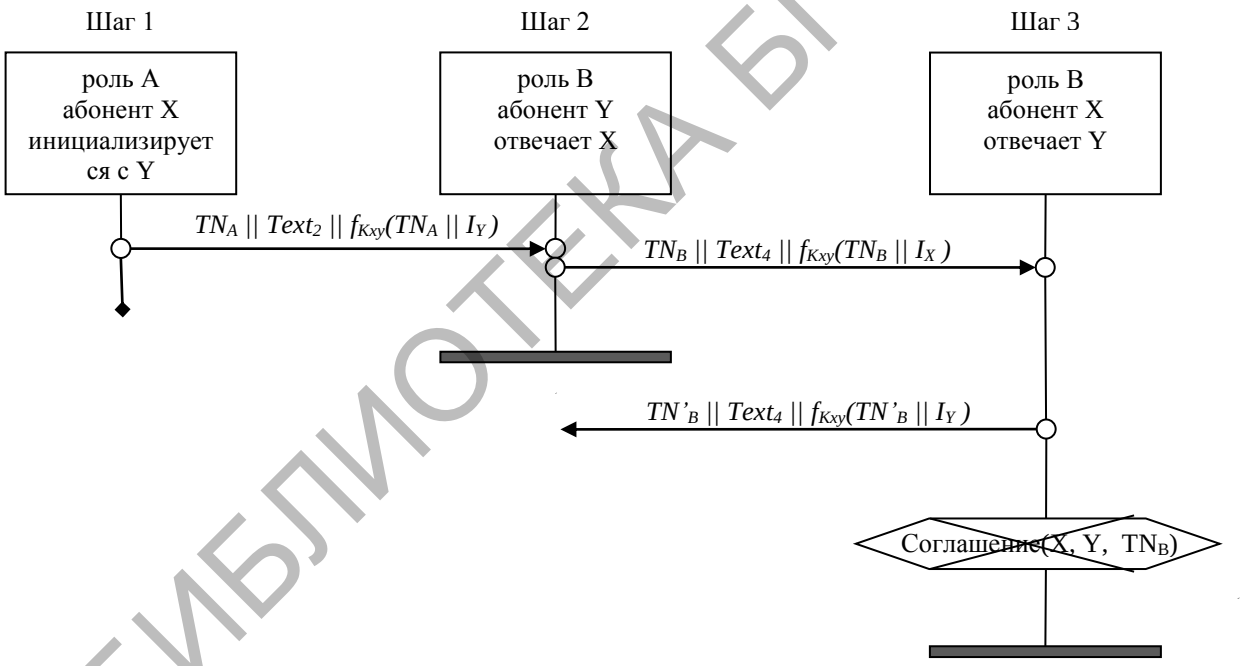

Рисунок 3: “атака ролевой путаницы” для протокола версии 2009 года совместной аутентификации с двумя проходами, при использовании криптографической функции проверки.

На рисунке 3 показан пример атаки ролевой путаницы по протоколу из рисунка 2. Агенты выполняют движения, такие как отправка и получение сообщений (представлено горизонтальными стрелками). Действия выполняются в пределах потоков, представленных вертикальными стрелками. Свойство безопасности, отмеченное шестиугольником, нарушается.

В этой атаке злоумышленник использует сообщение от абонента Yв роли B (шаг 2) чтобы обмануть абонента X в роли B (шаг 3), который считает, что инициализация сеанса происходит от Y. Однако, Y (шаг 2) отвечают на сообщение от X в роли A (шаг 1). Таким образом, злоумышленник обманывает абонента X, заставляя его считать, что Y находится в определённом состоянии.

Заключение

Исследование WiMAX обеспечивает поучительную историю о том, что происходит, когда модели угрозы и цели безопасности не включены в стандарт. В этом случае, отсутствие этих моделей создало ситуацию, когда некоторые протоколы не могут быть объявлены небезопасными. Анализ EAP показывает, что протоколы системы защиты все чаще рассматриваются в рамках модели угроз и предназначены для удовлетворения специфических требования безопасности.

Тем не менее, модели угроз и требования безопасности должны быть указаны неофициально, что затрудняет сравнение предложений протокола и принятие решения о соответствии протокола поставленной цели. Исследование ISO/IEC 9798 демонстрирует возможность точного описания модели угроз и свойств безопасности, а также, возможность выполнения формальной верификации. Формальные методы медленно начинают оказывать влияние на органы по стандартизации.

Как только в стандарты к их функциональным спецификациям будут добавлены однозначные свойства безопасности и модели угроз, у нас появятся основания для их оценки, а впоследствии и для сравнения различных стандартов.

Литература

1. Basin, D., Cremers, C., Miyazaki, K., Radomirovic, S., Watanabe, D.: Improving the security of cryptographic protocol standards. IEEE Security & Privacy, P.24-31, 2014