Международный союз электросвязи

МСЭ-Т X.1362

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(03/2017)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги – Безопасность интернета вещей (IoT)

Простая процедура шифрования для среды интернета вещей (IoT)

Рекомендация МСЭ-Т X.1362

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
Безопасность интернета вещей (IoT)	**X.1360–X.1369**
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1362

Простая процедура шифрования для среды интернета вещей (IoT)

Резюме

Интернет вещей (IoT) рассматривается как одна из важнейших областей будущей стандартизации. IoT, с позиции МСЭ-Т, определяется как глобальная инфраструктура для информационного общества, которая делает возможным предоставление перспективных услуг путем присоединения (физического и виртуального) вещей.

В определенной среде IoT, в особенности это касается устройств IoT, применяется требование обработки в режиме реального времени, когда задачи должны выполняться в течение определенного периода времени. Одна из основных мер обеспечения защиты целостности и конфиденциальности данных заключается в применении алгоритмов шифрования/аутентификации данных. Однако проблема заключается в том, что стандартные приложения алгоритмов шифрования/аутентификации данных не могут выполнить это требование.

В Рекомендации МСЭ-Т X.1362 определен алгоритм шифрования с присоединенными данными для маскирования (EAMD) для устройств интернета вещей (IoT). Приведено описание EAMD и порядка предоставления набора услуг безопасности для трафика, в котором используется EAMD.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1362	30.03.2017 г.	17-я	11.1002/1000/13196

Ключевые слова

Применение алгоритмов шифрования/аутентификации данных, шифрование с присоединенными данными для маскирования (EAMD), устройства IoT, среда IoT, требование обработки в режиме реального времени.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Интернет вещей (IoT) рассматривается как одна из важнейших областей будущей стандартизации. IoT, с позиции МСЭ-Т, определяется как глобальная инфраструктура для информационного общества, которая делает возможным предоставление перспективных услуг путем присоединения (физического и виртуального) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий [b-ITU-T Y.2060].

Повсеместно распространенные сенсорные сети (ПРСС) представляются одной из важнейших областей IoT. Это сети интеллектуальных сенсорных узлов, которые можно развернуть "в любом месте, в любое время, любыми силами и с помощью любых средств". Мы считаем эффективным применение в IoT методов обеспечения безопасности, разработанных для повсеместно распространенных сенсорных сетей, в силу того, что ПРСС имеют много общего с IoT, работая с такими устройствами, как датчики-измерители и исполнительные механизмы. Что касается безопасности ПРСС, то уже опубликованы такие Рекомендации, как основы безопасности [b-ITU-T X.1311], "Руководящие указания по обеспечению безопасности промежуточного программного обеспечения" [b-ITU-T X.1312] и "Требования обеспечения безопасности при маршрутизации в беспроводных сенсорных сетях" [b-ITU-T X.1313]. Однако исследования для разработки Рекомендаций по методам защиты конфиденциальности и целостности данных, которые обеспечивают безопасность на уровне устройств в ПРСС, не проводились. Таким образом безопасность на уровне устройств остается неисследованной областью в ПРСС, так же, как и в IoT, и, поэтому следует изучить и обсудить данную проблематику для будущей стандартизации.

С другой стороны, в определенной среде IoT, в особенности это касается таких устройств IoT, как датчики-измерители и исполнительные механизмы, которые можно использовать в промышленных системах управления (ICS), применяется требование обработки в режиме реального времени, когда задачи должны выполняться в течение определенного периода времени. Одна из основных мер обеспечения защиты целостности и конфиденциальности данных заключается в применении алгоритмов шифрования/аутентификации данных. Однако проблема заключается в том, что стандартные приложения алгоритмов шифрования/аутентификации данных не могут выполнить это требование. Другая проблема – объединение разных уровней безопасности, а именно: данные, размещенные в разных позициях в пределах пакета связи, требуют разных уровней важных последующих мер безопасности. Таким образом шифрование данных в позиции, указывающей низкий уровень безопасности, представляется излишней затратой ресурсов на обработку.

Как упоминалось выше, для обеспечения безопасности среды IoT, в особенности устройств IoT, требуется новое приложение для алгоритмов шифрования/аутентификации данных, которое отвечает требованиям обработки в режиме реального времени и объединяет разные уровни безопасности.

Следовательно, требуется шифрование с присоединенными данными для маскирования, когда выполняется шифрование только тех данных в пакете связи, для которых требуется высокий уровень безопасности. Присоединенные данные для маскирования используются для указания уровней безопасности данных в каждой позиции в пределах пакета.

Рекомендация МСЭ-Т X.1362

Простая процедура шифрования для среды интернета вещей (IoT)

1 Сфера применения

В настоящей Рекомендации представлена процедура шифрования для обеспечения безопасности устройств интернета вещей (IoT). Эта процедура предназначена для применения в среде IoT, особенно в устройствах IoT, которые имеют обязательные средства связи и дополнительные измерительные и/или исполнительные средства, а также средства хранения и обработки данных. В настоящей Рекомендации определяется шифрование с присоединенными данными для маскирования (EAMD) для среды IoT. Приведено описание EAMD и порядка предоставления набора услуг безопасности для трафика, в котором используется EAMD. В Приложении A приведены также примеры конкретных применений.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP).*

[IETF RFC 7296] IETF RFC 7296 (2014), *Internet Key Exchange Protocol Version 2 (IKEv2).*

[IETF RFC 7321] IETF RFC 7321 (2014), *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[ISO/IEC 10116] ISO/IEC 10116:2006, *Information technology – Security techniques –Modes of operation for an n-bit block cipher*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 исполнительный механизм (actuator) [b-ITU-T Y.4109]: Устройство, которое инициирует физическое действие после возбуждения входным сигналом.

ПРИМЕЧАНИЕ. − Исполнительный механизм может воздействовать, например, на поток газа или жидкости, на распределение электроэнергии или выполнять механическую операцию. Примерами исполнительных механизмов служат реостаты и реле. Решение о включении исполнительного механизма может поступать от приложения МОС, от человека или от устройств и шлюзов МОС.

3.1.2 инкапсуляция полезной нагрузки безопасности (encapsulating security payload (ESP)) [IETF RFC 4303]: Протокол IPsec, который используется для обеспечения конфиденциальности, аутентификации источника данных, обеспечения целостности данных в режиме без установления соединения, услуги антиповтора (форма целостности дробной последовательности) и конфиденциальности (ограниченного) потока трафика. Набор предоставляемых услуг зависит от параметров, выбранных в процессе создания ассоциации безопасности (SA) и от места реализации в топологии сети.

3.1.3 индекс параметров безопасности (security parameters index (SPI)) [b-IETF RFC 4301]: Произвольное 32-битовое значение, используемое приемником для идентификации SA, с которой следует связать входящий пакет.

3.1.4 измеренные данные (sensed data) [b-ITU-T F.4104]: Данные, полученные датчиком, который подсоединен к конкретному сенсорному узлу.

3.1.5 датчик (sensor) [b-ITU-T Y.4105]: Электронное устройство, которое измеряет физическое состояние или химический состав и доставляет электронный сигнал, соответствующий наблюдаемой характеристике.

3.1.6 порядковый номер (sequence number) [IETF RFC 4303]: 32-битовое поле без знака, содержащее значение счетчика, которое увеличивается на единицу при передаче каждого пакета, то есть порядковый номер пакета в SA.

3.2 Термины определенные в настоящей Рекомендации

В настоящей Рекомендации используются следующие термины.

3.2.1 программируемый контроллер (programmable controller): Электронное устройство для управления исполнительными механизмами на основе измеренных данных, получаемых от датчиков.

3.2.2 ассоциация безопасности с маскированием (security association with mask (SAM)): Набор параметров, зависящий от протокола безопасности. SAM определяет услуги и механизмы, необходимые для защиты трафика путем шифрования с присоединенными данными для маскирования (EAMD). SAM определяется связанным с ней протоколом в зависимости от уровней протокола, например транспортного уровня или уровня протокола Интернет (IP). В этих параметрах могут быть указаны идентификаторы алгоритмов, режимы, идентификаторы уровней, на которых применяется EAMD, и криптографические ключи.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AES	Advanced Encryption Standard	Расширенный стандарт шифрования
CBC	Cipher Block Chaining	Сцепление блоков шифротекста
CMAC	Cipher-based Message Authentication Code	Код аутентификации сообщения на основе шифра
EAMD	Encryption with Associated Mask Data	Шифрование с присоединенными данными для маскирования
EAMDSP	EAMD Security Payload	Полезная нагрузка безопасности EAMD
ESP	Encapsulating Security Payload	Инкапсуляция полезной нагрузки безопасности
ICS	Industrial Control System	Промышленная система управления
IP	Internet Protocol	Протокол Интернет
IPSec	IP Security	Безопасность IP
IoT	Internet of Things	Интернет вещей
IV	Initialization Vector	Вектор инициализации
MAC	Message Authentication Code	Код аутентификации сообщения
SA	Security Association	Ассоциация безопасности
SAM	Security Association with Mask	Ассоциация безопасности с маскированием
SAMD	SAM Database	База данных SAM
SPI	Security Parameters Index	Индекс параметров безопасности
TCP	Transmission Control Protocol	Протокол управления передачей
UDP	User Datagram Protocol	Протокол дейтаграмм пользователя
USN	Ubiquitous Sensor Networks	ПРСС Повсеместно распространенные сенсорные сети
XOR	Exclusive OR	Исключающее ИЛИ

5 Условные обозначения

Отсутствуют.

6 Введение в шифрование с присоединенными данными для маскирования (EAMD)

6.1 Спецификация процедуры EAMD

В среде IoT существует широкий спектр угроз безопасности [b-ZT]. В настоящей Рекомендации рассматриваются следующие виды угроз:

1) атаки путем подмены участника, когда подлинные данные перехватываются или подделываются, что приводит к раскрытию или фальсификации информации;

2) атаки путем подслушивания, когда в сети перехватываются пакеты, переданные другими компьютерами, и данные прочитываются в поисках конфиденциальной информации любого вида;

3) атаки путем имитации, когда подлинный компонент подменяется в целях получения данных или фальсификации информации.

Для смягчения последствий этих угроз в среде IoT, особенно для устройств IoT, в настоящей Рекомендации представлен метод шифрования с присоединенными данными для маскирования (EAMD), при котором с открытыми пакетами связи, передаваемыми между некоторыми устройствами, выборочно производятся криптографические операции. К этим криптографическим операциям относятся шифрование/дешифрование и генерирование/верификация кода аутентификации сообщения (MAC), а также шифрование с аутентификацией. Описание криптографических алгоритмов, используемых в EAMD, не входит в сферу применения настоящей Рекомендации, однако хорошими справочными материалами по алгоритмам шифрования, алгоритмам MAC и алгоритмам шифрования с аутентификацией служат [b-ISO/IEC 9797], [b-ISO/IEC 18033] и [b-ISO/IEC 19772] соответственно.

Следует отметить, что конструкцию, описанную в этом разделе, можно рассматривать как протокол, использующий шифрование с последующим применением MAC [b-ASIACRYPT] и [b-EUROCRYPT].

Блоки данных в составе пакета связи, над которыми выполнены криптографические операции, указываются *маской*.

Предполагается, что отправителю известны алгоритм шифрования, ключ, начальный вектор и маска для связи с EAMD-защитой, а также отправителю и получателю известен идентификатор алгоритма и ключи друг друга. При этих условиях связь с EAMD-защитой осуществляется путем получения информации для шифрования с присоединенными данными для маскирования на стороне отправителя и совместного использования информации шифрования с получателем. Рисунок 1 служит иллюстрацией общего представления шифрования с присоединенными данными для маскирования.

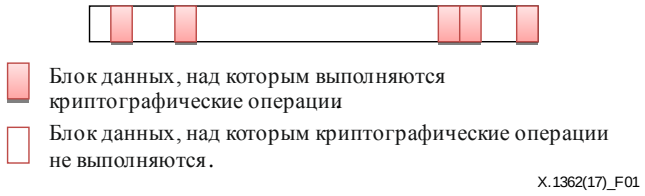

Рисунок 1 − Пакет, передаваемый в сеансе связи с использованием шифрования с присоединенными данными для маскирования

При связи с EAMD-защитой выполняется следующая обработка исходящих пакетов:

1) Добавляется необходимый заполнитель для шифрования.

2) Данные, подлежащие шифрованию, извлекаются с применением маски шифрования и копируются в буфер, который используется для промежуточных вычислений.

3) Результат шифруется в буфере с использованием ключа, алгоритма шифрования и всех необходимых данных.

4) Результат вставляется в пакет с использованием маски.

5) Результат инкапсулируется в поле полезной нагрузки[1].

Если выбрана целостность, то обработка производится следующим образом.

6) Данные для генерирования MAC с использованием маски извлекаются для генерирования MAC и копируются в буфер.

7) Добавляется необходимый заполнитель для генерирования MAC.

8) На основании результатов в буфере генерируется MAC.

9) MAC добавляется в пакет.

Порядок обработки исходящих пакетов показан на рисунке 2.

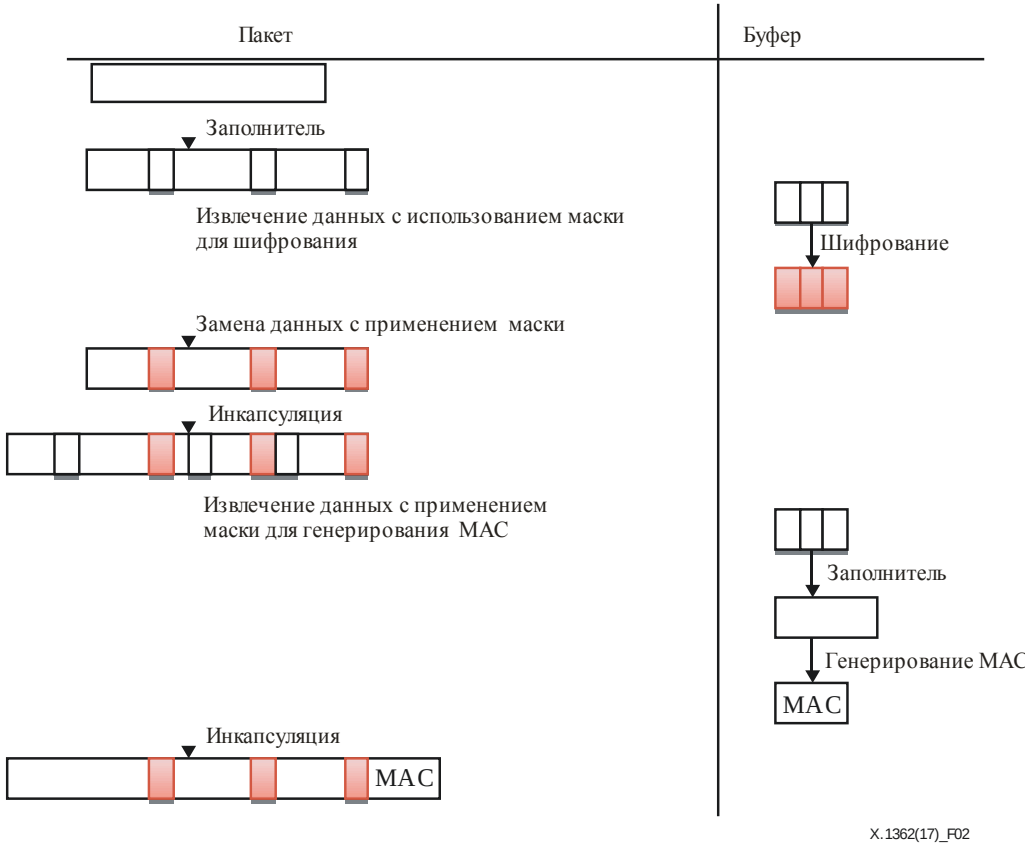

Рисунок 2 − Создание пакета с применением шифрования с присоединенными данными для маскирования при обработке исходящих пакетов

При связи с EAMD-защитой выполняется следующая обработка входящих пакетов:

Если выбрана целостность, то выполняются приведенные ниже шаги 1–3[1]:

1) Данные из пакета за вычетом MAC извлекаются в буфер в соответствии с маской для генерирования MAC.

2) Добавляется необходимый заполнитель для генерирования MAC.

3) По данным заполнителя вычисляется MAC с использованием определенного алгоритма целостности и выполняется проверка, чтобы убедиться, что этот MAC совпадает с MAC, полученным в пакете. Если вычисленное и принятое значения MAC совпадают, то пакет считается действительным и принимается. Если тест не пройден, то получатель должен отбросить полученный пакет как недействительный.

---

[1] Для использования привязки шифрования с присоединенными данными для маскирования к протоколу IPsec следует обеспечить конфиденциальность и аутентификацию.

4) Из пакета удаляется заголовок.

5) Данные результата извлекаются в буфер в соответствии с маской для дешифрования.

6) Результат, извлеченный в буфер, дешифруется.

7) Результат из буфера вставляется в пакет с применением маски для дешифрования.

8) Заполнитель для шифрования удаляется из пакета.

Порядок обработки входящих пакетов показан на рисунке 3.

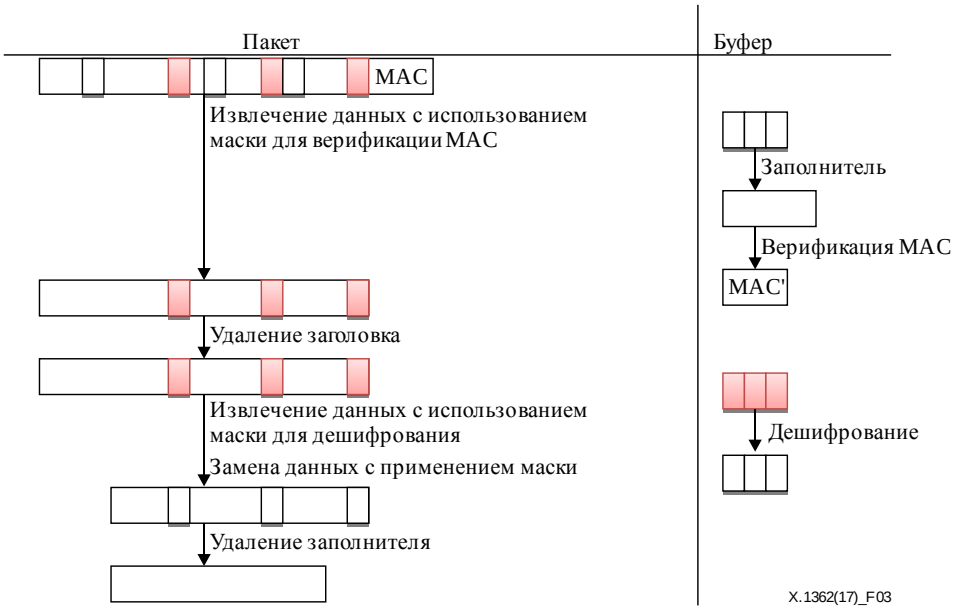

Рисунок 3 − Создание пакета с применением шифрования с присоединенными данными для маскирования при обработке входящих пакетов

6.2 Маска для извлечения целевых данных для шифрования с присоединенными данными для маскирования

В операциях шифрования с присоединенными данными для маскирования целевые данные блоков, обрабатываемых соответствующим алгоритмом, извлекаются путем разбиения пакета на блоки подходящего для этого алгоритма шифрования размера в соответствии с параметром маски.

7 Шифрование с присоединенными данными для маскирования

В этом разделе представлено описание набора услуг безопасности для трафика на каждом уровне. В настоящей Рекомендации описана безопасная связь с использованием шифрования с присоединенными данными для маскирования на основе полезной нагрузки безопасности EAMD (EAMDSP). Обзор такой связи приведен на рисунке 4. Ниже подробно описаны потоки связи с EAMD-защитой.

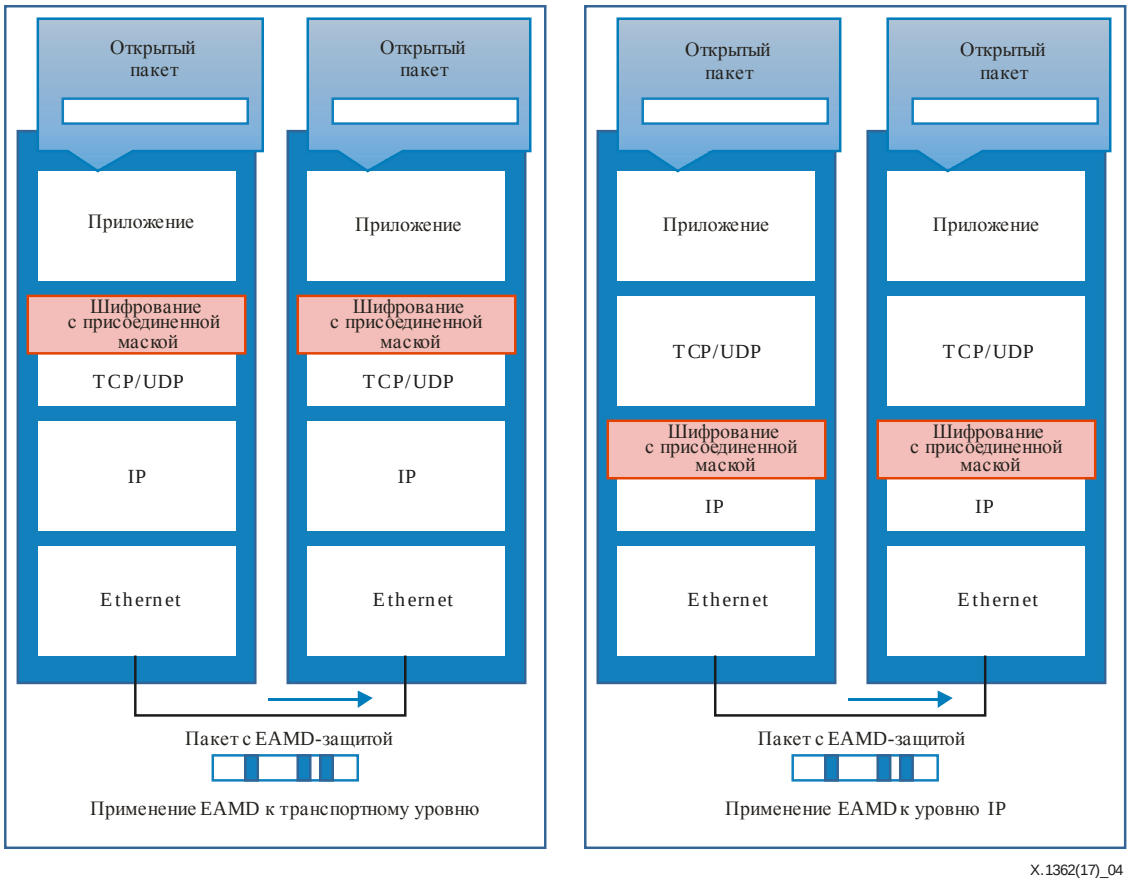

Рисунок 4 − Обзор связи с использованием шифрования с присоединенными данными для маскирования (EAMD)

7.1 Ассоциация безопасности с маскированием (SAM)

Ассоциация безопасности с маскированием (SAM) определяется как набор параметров, зависящих от протокола безопасности. SAM определяет услуги и механизмы, необходимые для защиты трафика путем применения EAMD. SAM определяется связанным с ней протоколом в зависимости от уровней протокола, например транспортного уровня или уровня протокола Интернет (IP). В этих параметрах могут быть указаны идентификаторы алгоритмов, режимы, идентификаторы уровней, на которых применяется EAMD, зависящие от уровня параметры, такие как IP-адрес и порт, и криптографические ключи. SAM содержит CryptCtx – набор криптографических параметров. Данные о состоянии, связанные с SAM, представлены в базе данных SAM (SAMD).

Все обязательные параметры этого формата указаны в таблице 1.

Таблица 1 − Обязательные параметры CryptCtx в ассоциации безопасности (SA)

№ п/п	Параметр	Значение
1	encAlg	Идентификатор алгоритма шифрования
2	encKey	Ключ шифрования
3	encMask	Область шифрования

Все необязательные параметры указаны в таблице 2.

Таблица 2 − Необязательные параметры CryptCtx в SA

№ п/п	Параметр	Значение
1	encRoundKey	Итерационный ключ шифрования
2	decRoundKey	Итерационный ключ дешифрования
3	encIV	Начальный вектор (IV) шифрования
4	macRoundKey	Итерационный ключ MAC
5	macK1	Подключ CMAC K1
6	macK2	Подключ CMAC K2
7	KeyStream	Предварительно сгенерированные случайные числа
8	KeyStreamHead	Указатель начала списка неиспользуемых случайных чисел
9	KeyStreamTail	Указатель конца списка неиспользуемых случайных чисел
10	EncIVTail	Начальный вектор для генерирования случайных чисел
11	macAlg	Идентификатор алгоритма MAC
12	macKey	Ключ MAC
13	macMask	Область, используемая для создания MAC с помощью указанного алгоритма

7.2 Формат пакета полезной нагрузки безопасности EAMD (EAMDSP)

На рисунке 5 показан формат пакета полезной нагрузки безопасности EAMD (EAMDSP). Пакет начинается с заголовка EAMDSP переменной длины. За этим полем следуют данные полезной нагрузки, подструктура которых зависит от выбора алгоритма и режима шифрования. За данными полезной нагрузки следуют поля заполнителя и длины заполнителя и поле следующего заголовка. Пакет завершается необязательным полем кода аутентификации сообщения (MAC). Концевая часть EAMDSP состоит из полей заполнителя, длины заполнителя и следующего заголовка.

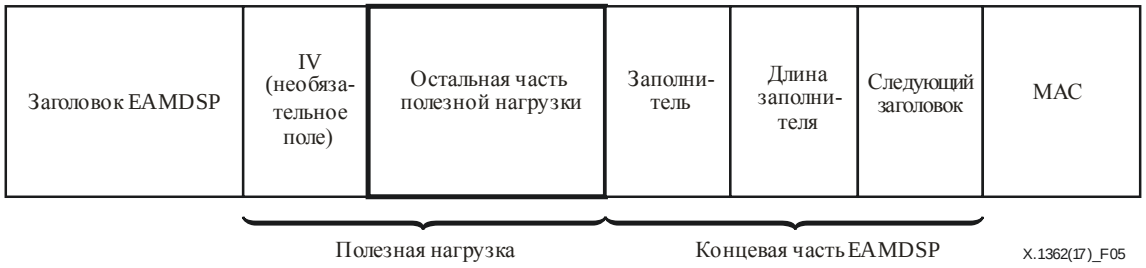

Рисунок 5 − Формат пакета EAMDSP

Концевая часть EAMDSP (передаваемая) состоит из полей заполнителя, длины заполнителя и следующего заголовка. В вычислении целостности также участвуют дополнительные неявные данные концевой части EAMDSP (которые не передаются).

Если выбрана услуга целостности, то вычисление целостности охватывает заголовок EAMDSP, данные полезной нагрузки и концевую часть EAMDSP. Если выбрана услуга конфиденциальности, то шифротекст состоит из данных полезной нагрузки (за исключением любых данных криптографической синхронизации, которые могут включаться) и концевой части EAMDSP.

В следующих далее пунктах приводится описание полей в формате заголовка. Необязательное поле означает, что поле опускается, если параметр не выбран, то есть оно не присутствует ни в передаваемом пакете, ни в пакете, отформатированном для вычисления MAC. Выбран параметр или нет, указывается при создании SAM. Таким образом формат пакетов EAMDSP для данной SAM на время действия этой SAM является фиксированным. Обязательные поля, напротив, всегда присутствуют в формате пакетов EAMDSP для всех SAM.

7.2.1 Данные полезной нагрузки

Данные полезной нагрузки – это поле переменной длины, содержащее данные (из исходного пакета), описываемые в поле следующего заголовка. Поле данных полезной нагрузки является обязательным полем, и его длина кратна байту. Если для алгоритма, используемого для шифрования полезной нагрузки, требуется криптографическая синхронизация данных, например вектор инициализации (IV), то эти данные явно передаются в поле полезной нагрузки, но в EAMDSP они не обозначаются как отдельное поле, то есть для EAMDSP передача явного IV остается невидимой.

7.2.2 Заполнитель (для шифрования)

Если применяется алгоритм шифрования, требующий, чтобы длина открытого текста была кратной некоторому числу байтов, например размеру блока блочного шифротекста, то используется поле заполнителя для дополнения открытого текста (состоящего из полей данных полезной нагрузки, заполнителя, длины заполнителя и следующего заголовка) до размера, предписываемого алгоритмом.

7.2.3 Длина заполнителя

В поле длины заполнителя указывается число байтов заполнителя в предшествующем поле заполнителя. Поле длины заполнителя является обязательным.

7.2.4 Следующий заголовок

Следующий заголовок является обязательным полем. Оно определяет тип данных, содержащихся в поле полезной нагрузки, например заголовок и данные следующего уровня.

7.2.5 Код аутентификации сообщения (MAC)

Код аутентификации сообщения представляет собой поле переменной длины, вычисляемое по указанным маской данным для защиты целостности данных. В вычислении MAC участвуют поля неявных данных концевой части EAMDSP, такие как заполнитель для создания MAC. MAC является необязательным полем. Оно присутствует, только если выбрана услуга целостности, и обеспечивается либо посредством отдельного алгоритма целостности, либо посредством алгоритма комбинированного режима, использующего MAC. Длина поля определяется выбранным алгоритмом целостности и связана с SAM. Спецификация алгоритма целостности должна определять длину MAC, правила сравнения и шаги обработки данных в целях валидации.

7.3 Обработка пакетов

7.3.1 Обработка исходящих пакетов

Обработка исходящих пакетов с использованием шифрования с присоединенными данными для маскирования осуществляется следующим образом:

1) Поиск SAM:

   Прежде чем применять EAMDSP к исходящему пакету, определяется соответствующая SAM, которая обусловливает EAMDSP, по такой информации, как идентификатор уровня и зависящий от уровня параметр, например IP-адрес или номер порта в пакете. SAM указывает ключ и маски для шифрования и генерирования MAC.

2) Преобразование данных с помощью EAMD описано в пункте 6.1.

3) Передача пакета:

   К преобразованному путем EAMD пакету добавляется исходный заголовок, и полученный в результате пакет передается по сети.

7.3.2 Обработка входящих пакетов

Обработка входящих пакетов с использованием шифрования с присоединенными данными для маскирования осуществляется следующим образом:

1) Поиск SAM:

   Получив пакет, содержащий заголовок EAMDSP, приемник определяет соответствующую SAM путем поиска в SAMD. В записи SAMD для SAM также указывается, EAMD какого уровня применяется при обработке исходящего пакета и зависящий от уровня параметр,

например IP-адрес или номер порта в пакете, а также должно ли присутствовать поле MAC. Кроме того, в записи SAMD указаны алгоритмы и ключи, используемые для дешифрования и верификации MAC (в соответствующих случаях).

2) Верификация данных заголовка EAMDSP:

Проверка данных заголовка EAMDSP может производиться с использованием определенных значений в заголовке EAMDSP и выполняется перед проверкой целостности и дешифрованием. Если эта проверка не пройдена, пакет отбрасывается.

Преобразование данных с помощью EAMD описано в пункте 6.1.

8 EAMD с использованием алгоритма шифрования с аутентификацией

8.1 Ассоциация безопасности с маскированием (SAM)

В случае, если EAMD использует алгоритм шифрования с аутентификацией, определение SAM соответствует определению, приведенному в пункте 7.1.

Все обязательные параметры этого формата представлены в таблице 3.

Таблица 3 − Обязательные параметры CryptCtx в SA

№ п/п	Параметр	Значение
1	auencAlg	Идентификатор алгоритма шифрования с аутентификацией
2	auencKey	Ключ шифрования с аутентификацией
3	encMask	Область шифрования

Все необязательные параметры представлены в таблице 4.

Таблица 4 − Необязательные параметры CryptCtx в SA

№ п/п	Параметр	Значение
1	auencRoundKey	Итерационный ключ шифрования с аутентификацией
2	audecRoundKey	Итерационный ключ дешифрования
3	IV	Начальный вектор шифрования с аутентификацией
4	Nonce	Итерационный ключ шифрования с аутентификацией

8.2 Формат пакета полезной нагрузки безопасности EAMD (EAMDSP)

На рисунке 6 показан формат пакета EAMDSP (полезная нагрузка безопасности EAMD). Пакет начинается с заголовка EAMDSP переменной длины. За этим полем следуют данные полезной нагрузки, подструктура которых зависит от выбора алгоритма и режима шифрования. За данными полезной нагрузки следуют поля заполнителя и длины заполнителя и поле следующего заголовка. Концевая часть EAMDSP состоит из полей заполнителя, длины заполнителя и следующего заголовка.

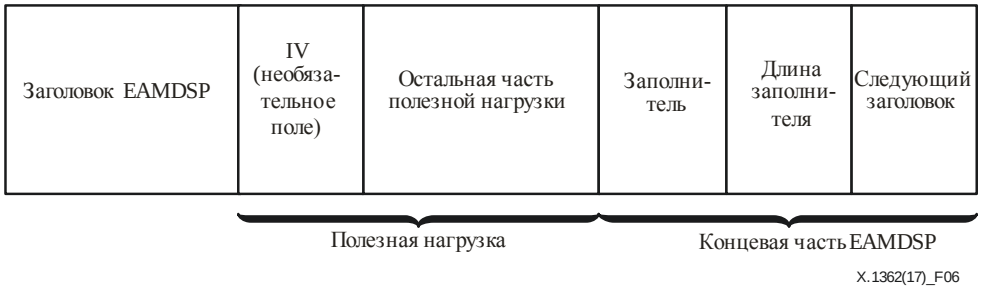

Рисунок 6 − Формат пакета EAMDSP (для шифрования с аутентификацией) без MAC

Концевая часть EAMDSP (передаваемая) состоит из полей заполнителя, длины заполнителя и следующего заголовка. В вычислении целостности также участвуют дополнительные неявные данные концевой части EAMDSP (которые не передаются).

Если выбрана услуга целостности, то вычисление целостности охватывает заголовок EAMDSP, данные полезной нагрузки и концевую часть EAMDSP. Если выбрана услуга конфиденциальности, то шифротекст состоит из данных полезной нагрузки (за исключением любых данных криптографической синхронизации, которые могут включаться) и концевой части EAMDSP.

В следующих далее пунктах приводится описание полей в формате заголовка. Необязательное поле означает, что поле опускается, если параметр не выбран, то есть оно не присутствует ни в передаваемом пакете, ни в пакете, отформатированном для вычисления MAC. Выбран параметр или нет, указывается при создании SAM. Таким образом формат пакетов EAMDSP для данной SAM на время действия этой SAM является фиксированным. Обязательные поля, напротив, всегда присутствуют в формате пакетов EAMDSP для всех SAM.

8.2.1 Данные полезной нагрузки

Данные полезной нагрузки – это поле переменной длины, содержащее данные (из исходного пакета), описываемые в поле следующего заголовка. Поле данных полезной нагрузки является обязательным полем, и его длина кратна байту.

Формат пакета инкапсуляции полезной нагрузки безопасности (ESP) можно описать выражением ESP = SPI || Порядковый номер || IV || C, где C – шифротекст, создаваемый алгоритмом шифрования с аутентификацией. В данном случае C содержит признак аутентификации.

8.2.2 Заполнитель (для шифрования с аутентификацией)

Если применяется алгоритм шифрования с аутентификаций, требующий, чтобы длина открытого текста была кратной некоторому числу байтов, например размеру блока блочного шифротекста, то используется поле заполнителя для дополнения открытого текста (состоящего из полей данных полезной нагрузки, заполнителя, длины заполнителя и следующего заголовка) до размера, предписываемого алгоритмом.

8.2.3 Длина заполнителя

В поле длины заполнителя указывается число байтов заполнителя в предшествующем поле заполнителя. Поле длины заполнителя является обязательным.

8.2.4 Следующий заголовок

Следующий заголовок является обязательным полем. Оно определяет тип данных, содержащихся в поле полезной нагрузки, например заголовок и данные следующего уровня.

8.3 Обработка пакетов

8.3.1 Обработка исходящих пакетов

Обработка исходящих пакетов с использованием шифрования с присоединенными данными для маскирования осуществляется следующим образом:

1) Поиск SAM:

   Прежде чем применять EAMDSP к исходящему пакету, определяется соответствующая SAM, которая обусловливает EAMDSP, по такой информации, как идентификатор уровня и зависящий от уровня параметр, например адрес протокола Интернет (IP) или номер порта в пакете. SAM указывает ключ и маски для шифрования с аутентификацией.

2) Преобразование данных в режиме шифрования EAMD с аутентификацией:

   1) Добавляется необходимый заполнитель для шифрования.

   2) Данные, подлежащие шифрованию, извлекаются с применением маски шифрования и копируются в буфер, который используется для промежуточных вычислений.

   3) Результат шифруется в буфере с использованием ключа, алгоритма шифрования и всех необходимых данных.

4) Шифротекст вставляется в пакет с применением маски.

5) В пакет добавляется признак аутентификации в качестве MAC.

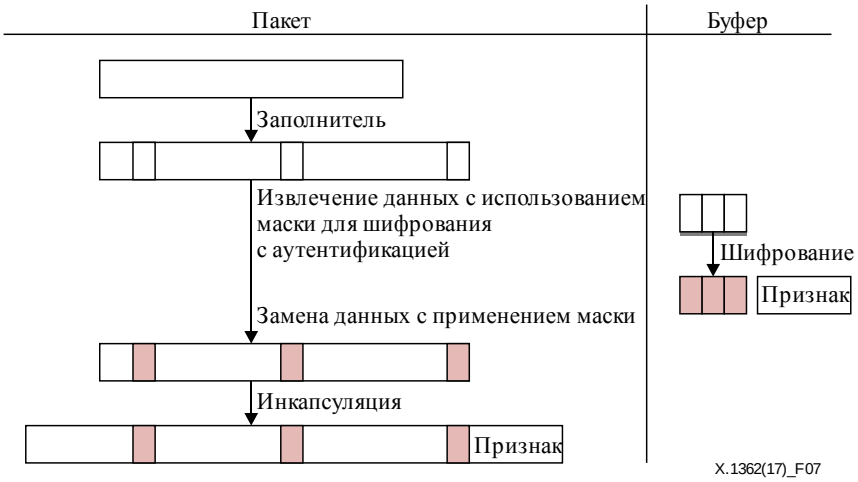

Рисунок 7 − Обработка исходящих пакетов в режиме шифрования с аутентификацией

3) Передача пакета:

К преобразованному путем EAMD пакету добавляется исходный заголовок, и полученный в результате пакет передается по сети.

8.3.2 Обработка входящих пакетов

Обработка входящих пакетов с использованием шифрования с присоединенными данными для маскирования осуществляется следующим образом:

1) Поиск SAM:

Получив пакет, содержащий заголовок EAMDSP, приемник определяет соответствующую SAM путем поиска в SAMD. В записи SAMD системы SAM также указывается, EAMD какого уровня применялась при обработке исходящего пакета и зависящий от уровня параметр, например IP-адрес или номер порта в пакете. Кроме того, в записи SAMD указаны алгоритмы и ключи, используемые для дешифрования и верификации признака.

2) Верификация данных заголовка EAMDSP:

Проверка данных заголовка EAMDSP может производиться с использованием определенных значений в заголовке EAMDSP и выполняется перед проверкой целостности и дешифрованием. Если эта проверка не пройдена, пакет отбрасывается.

3) Преобразование данных в режиме дешифрования с аутентификацией EAMD:

   1) Из пакета удаляется заголовок.
   2) Данные, подлежащие дешифрованию, извлекаются с применением маски шифрования и копируются в буфер, который используется для промежуточных вычислений.
   3) Признак аутентификации отделяется от пакета и копируется в буфер.
   4) Результат дешифруется в буфере с использованием ключа, алгоритма шифрования и всех необходимых данных.
   5) Если дешифрование завершено успешно, результат дешифрования вставляется в пакет с применением маски.

4) Заполнитель для шифрования удаляется из пакета.

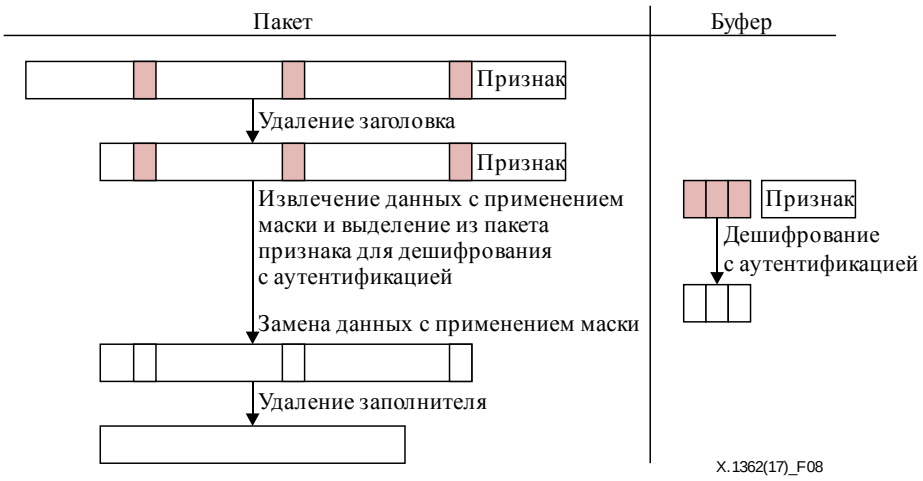

Рисунок 8 − Обработка входящих пакетов в режиме шифрования с аутентификацией

9 Руководящие указания и ограничения

9.1 Руководство по созданию SAM

В отношении метода маскирования при шифровании EAMD следует отметить, что если злоумышленнику удастся изменить маску, то он получит возможность установить такое значение маски, что никакие данные не будут зашифрованы. После такого изменения маски все данные будут передаваться устройством открыто (то есть незашифрованными). Это создаст значительную уязвимость безопасности.

Для решения этой проблемы необходимо рассмотреть следующие вопросы:

1) Безопасность передачи маски

Для инициализации и обновления ключевого материала, такого как криптографические ключи, начальные векторы и другие параметры безопасности, существует ряд протоколов создания ключей, например протокол обмена ключами в интернете версии 2 (IKEv2) [IETF RFC 7296], соглашение о ключах и транспортировка ключей.

Необходимо гарантировать, чтобы маска инициализировалась и обновлялась в увязке с инициализацией и обновлением ключевого материала в процессе сеанса связи между взаимосвязанными объектами с использованием этих протоколов. Например, в процессе сеанса связи для создания ключей вышеупомянутый ключевой материал должен также содержать маску, с тем чтобы обеспечить целостность и конфиденциальность маски с помощью алгоритмов шифрования и алгоритмов MAC, используемых в этих протоколах.

2) Безопасность хранения маски

Необходимо гарантировать, что когда маска находится в устройстве, другое устройство не сможет прочесть ее с помощью какого бы то ни было протокола.

Для этой цели можно предложить следующие методы.

Первый метод – система защиты, которая назначает компоненты системы таким образом, что устройства, в которых применяется EAMD, не взаимодействуют с внешними по отношению к системе объектами напрямую, взаимодействие с такими объектами происходит только через безопасный компонент шлюза с высокой вычислительной мощностью.

Второй метод – защита устройства с помощью устойчивой к взлому аппаратуры или программного метода запутывания, который создает трудный для понимания человеком запутывающий код.

9.2 Руководство по надлежащему использованию векторов инициализации и одноразовых кодов (nonce)

В данном пункте приведено руководство по надлежащему использованию векторов инициализации (и дополнительных режимов блочного шифрования и заполнителей). Неправильное использование векторов инициализации или заполнителей является типичной ошибкой, создающей возможности для атак на протоколы. Параметр IV или одноразовый код обычно играют решающую роль для безопасности протокола.

Для того чтобы использовать режим сцепления блоков шифротекста (CBC) [ISO/IEC 10116] для шифрования, при котором блоки открытого текста комбинируются с предшествующими блоками шифротекста, необходимо выполнить изложенные ниже условия.

При использовании режима CBC в качестве режима работы с блочными шифрами следует рассмотреть вопрос защиты от атак типа Padding Oracle, описанных в [b-CBCPADD]. Для режима CBC требуется объединить IV с первым блоком открытого текста. Параметр IV не обязательно засекречивать, но он должен быть непредсказуемым.

Для того чтобы надежно использовать алгоритм шифрования с аутентификацией, необходимо выполнить изложенные ниже условия.

Если приложение не отвечает требованию уникальности при генерировании одноразового кода (nonce), оно должно использовать одноразовый код нулевой длины. Для таких приложений подходят рандомизированные алгоритмы и алгоритмы с отслеживанием состояния [b-IETF RFC 5116]. В ином случае в приложении следует использовать одноразовые коды длиной 12 октетов.

В случае если одноразовые коды или IV повторяются, многие программы становятся уязвимыми к атакам, при которых вскрывают, например, комбинацию "исключающее ИЛИ" (XOR) двух пакетов. Настоятельно рекомендуется поэтому гарантировать уникальность IV и одноразовых кодов.

9.3 Ограничение использования EAMD

Использование EAMD ограничено требованиями к производительности системы в режиме реального времени.

EAMD обеспечивает оптимальные преимущества в системах, где отправители и получатели обладают определенным уровнем вычислительной мощности, например ЦП с 16-разрядной или 32-разрядной архитектурой, достаточной тактовой частотой (сотни мегагерц) и памятью.

Следует отметить, что EAMD, возможно, не является хорошим решением для систем с требованиями ограничения мощности, поскольку потребление мощности для процесса буферизации EAMD может привести к значительным затратам ресурсов.

Следует также отметить, что маска, как указано выше, требует такой же защиты, что и ключ шифрования, поэтому EAMD можно применять лишь при условии безопасного управления маской и ее надежной защиты.

Приложение A

Привязки к существующим протоколам

(Это Приложение является неотъемлемой частью настоящей Рекомендации.)

Для безопасной связи на основе шифрования с присоединенными данными для маскирования уровень, на котором применяется это шифрование, должен быть фиксированным. Существует несколько вариантов таких уровней, на которых это возможно осуществить, например транспортный уровень, IP-уровень и т. п. В настоящем Приложении описан способ привязки шифрования с присоединенными данными для маскирования к существующим протоколам. Использование привязки шифрования с присоединенными данными для маскирования к протоколу IPsec требует конфиденциальности и аутентификации. Следует обеспечить конфиденциальность и аутентификацию [IETF RFC 7321].

A.1 Привязка к протоколу ESP IP security (IPSec) IETF RFC 4303

A.1.1 Формат SAM

SAM определяет услуги и механизмы, необходимые для защиты трафика путем применения EAMD. На рисунке A.1 описан формат ассоциации защиты с маскированием (SAM) для случая, когда EAMD применяется к сетевому уровню.

```
SecurityAssertion ::= SEQUENCE {
  layerIdentifier OCTET STRING (SIZE(1)),
  SPI             OCTET STRING (SIZE (4)),
  ipAddr          OCTET STRING (SIZE (4)),
  cryptCtx        CryptCtx
}
CryptCtx ::= SEQUENCE {
  encAlg    OCTET STRING (SIZE (4))
  encKey    OCTET STRING (SIZE (keySizeMax)),
  encMask   OCTET STRING (SIZE (maskLength))
}
keySizeMax INTEGER ::= 64
maskLength INTEGER ::= 16
```

Рисунок A.1 − Формат SAM для сетевого уровня

A.1.2 Формат пакетов

На рисунке A.2 приведен пример формата пакетов полезной нагрузки безопасности EAMD (EAMDSP). Пакет начинается с заголовка EAMDSP переменной длины. За этим полем следуют данные полезной нагрузки, подструктура которых зависит от выбора алгоритма и режима шифрования. За данными полезной нагрузки следуют поля заполнителя и длины заполнителя и поле следующего заголовка. Пакет завершается необязательным полем кода аутентификации сообщения (MAC). Концевая часть EAMDSP состоит из полей заполнителя, длины заполнителя и следующего заголовка. Учитывая объем трафика, обусловливаемого вычислениями MAC EAMD и шифрованием EAMD, можно привести другой пример формата, где длина порядкового номера может составлять 8 байтов, а поле следующего заголовка размещается в заголовке EAMDSP.

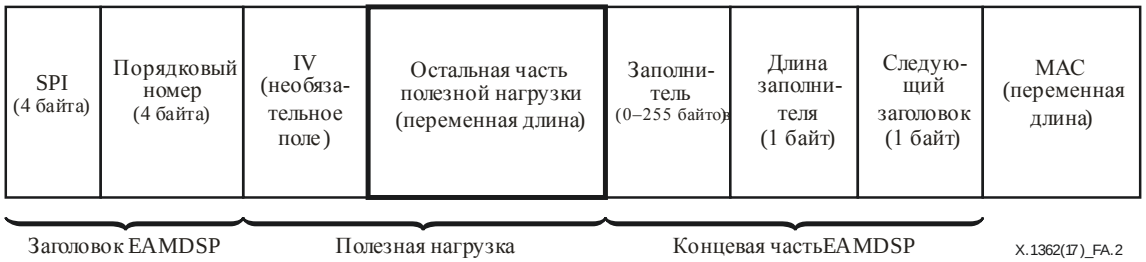

Рисунок A.2 − Пример формата пакета EAMDSP для привязки к протоколу ESP IPSec

1) Индекс параметров безопасности (SPI):

SPI – это произвольное 32-битовое значение, используемое приемником для идентификации SAM, с которой следует связать входящий пакет. Поле SPI является обязательным полем. SPI передается по протоколу, который позволяет принимающей системе выбрать SAM, в которой будет обрабатываться полученный пакет.

2) Порядковый номер:

Это 32-битовое или 64-битовое поле без знака содержит значение счетчика, которое увеличивается на единицу при передаче каждого пакета, то есть порядковый номер пакета в SAM или, иначе, значение, генерируемое в соответствии с однозначно понимаемым правилом.

3) Данные полезной нагрузки:

Данные полезной нагрузки – это поле переменной длины, содержащее данные (из исходного пакета), описываемые в поле следующего заголовка. Поле данных полезной нагрузки является обязательным полем, и его длина кратна байту. Если для алгоритма, используемого для шифрования полезной нагрузки, требуется криптографическая синхронизация данных, например вектор инициализации (IV), то эти данные явно передаются в поле полезной нагрузки, но в EAMDSP они не обозначаются как отдельное поле, то есть для EAMDSP передача явного IV остается невидимой.

4) Заполнитель (для шифрования):

Заполнитель может потребоваться также, вне зависимости от требований алгоритма шифрования, для гарантии того, что результирующий шифротекст заканчивается на границе 4 байтов. В частности поля длины заполнителя и следующего заголовка должны быть выровнены по правому краю в пределах 4-байтового слова, как показано выше на иллюстрациях формата пакета EAMDSP, для того чтобы гарантировать, что поле MAC (если оно присутствует) выровнено по границе четырех байтов.

5) Длина заполнителя:

В поле длины заполнителя указывается число байтов заполнителя в предшествующем поле заполнителя. Диапазон допустимых значений от 0 до 255, где нулевое значение указывает, что байты заполнителя отсутствуют. Поле длины заполнителя является обязательным полем.

6) Следующий заголовок:

Поле следующего заголовка является обязательным 8-битовым полем, которое определяет тип данных, содержащихся в поле данных полезной нагрузки, например следующий заголовок уровня и данные.

7) Код аутентификации сообщения (MAC):

Код аутентификации сообщения представляет собой поле переменной длины, вычисляемое по указанным маской данным для защиты целостности данных. В вычислении MAC участвуют поля неявной концевой части EAMDSP, такие как заполнитель для создания MAC. MAC является необязательным полем.

A.1.3 Обработка пакетов

Обработка исходящих пакетов с использованием шифрования с присоединенными данными для маскирования осуществляется следующим образом:

1) Поиск SAM:

   Определяется соответствующая SAM, которая обусловливает обработку EAMDSP, по такой информации, как идентификатор уровня и зависящий от уровня параметр, например IP-адрес или номер порта в пакете.

2) Преобразование данных с помощью EAMD:

   Шифрование и генерирование MAC выполняются с использованием EAMD в соответствии с процессом, описанным в пункте 6.1.

3) Передача пакета:

   К преобразованному путем EAMD пакету добавляется исходный заголовок, и полученный в результате пакет передается по сети.

Обработка входящих пакетов с использованием шифрования с присоединенными данными для маскирования осуществляется следующим образом:

1) Поиск SAM:

   Определяется соответствующая SAM, которая обусловливает обработку EAMDSP, по такой информации, как идентификатор уровня, который указывает транспортный уровень и IP-адрес, а также номер порта в пакете.

2) Верификация порядкового номера:

   Проверка порядкового номера осуществляется с помощью числового значения порядкового номера в заголовке EAMDSP и выполняется перед проверкой целостности и дешифрованием. Если эта проверка не пройдена, пакет отбрасывается.

3) Преобразование данных с помощью EAMD:

   Верификация MAC и дешифрование выполняются с использованием EAMD в соответствии с процессом, описанным в пункте 6.1.

A.1.4 Маска для извлечения целевых данных в процессе шифрования с присоединенными данными для маскирования

В операциях шифрования с присоединенными данными для маскирования целевые данные блоков, обрабатываемых соответствующим алгоритмом, извлекаются путем разбиения пакета на блоки подходящего для используемого алгоритма шифрования размера в соответствии с параметром маски. Например, в случае шифрования с присоединенными данными для маскирования с применением усовершенствованного стандарта шифрования (AES) полезная нагрузка разделяется через каждые 128 битов, потому что длина блока AES составляет 128 битов. Целевые данные дешифруемого блока извлекаются путем поиска блока по маске. После этого генерируются целевые данные для операции путем конкатенации целевых данных дешифруемого блока. Формат маски описан на рисунках A.3 и A.4. Этот параметр показывает, какой блок следует шифровать или дешифровать в случае разбиения полезной нагрузки на блоки размером, подходящим для используемого алгоритма шифрования.

```
MaskFormat ::= SEQUENCE {
  encryptionArea OCTET STRING (SIZE (12))
  reserved OCTET STRING (SIZE (4))
}
```

Рисунок A.3 − Формат маски

Рисунок A.4 − Детальный формат параметра маски

В данном случае параметр маски означает, что шифруется только первый блок, потому что первый бит параметра маски имеет значение "истинный". Для шифрования некоторых областей требуется изменить значение некоторых битов параметра маски с "ложного" на "истинный".

A.1.5 Алгоритм заполнения

Алгоритм заполнения можно описать следующим образом:

− добавить 0 x 80 в конце полезной нагрузки;

− если длина полезной нагрузки кратна длине блока алгоритма шифрования, то заполнение завершено.

Если длина полезной нагрузки НЕ кратна длине блока алгоритма шифрования, добавлять 0 x 00 в конце полезной нагрузки до тех пор, пока длина полезной нагрузки не станет кратной длине блока.

Библиография

[b-ITU-T Y.4104] Recommendation ITU-T Y.4104/F.744 (2009), *Service description and requirements for ubiquitous sensor network middleware.*

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2012, *Information technology – Security framework for ubiquitous sensor networks*.

[b-ITU-T X.1312] Recommendation ITU-T X.1312 (2011), *Ubiquitous sensor network middleware security guidelines.*

[b-ITU-T X.1313] Recommendation ITU-T X.1313 (2012), *Security requirements for wireless sensor network routing*.

[b-ITU-T Y.4000] Рекомендация МСЭ-Т Y.4000/Y.2060 (2012 г.), *Обзор интернета вещей*.

[b-ITU-T Y.4105] Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.*

[b-ITU-T Y.4109] Рекомендация МСЭ-Т Y.4109/Y.2061 (2012 г.), *Требования к поддержке приложений машинно-ориентированной связи в среде сетей последующих поколений*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-IETF RFC 5116] IETF RFC 5116 (2008), *An Interface and Algorithms for Authenticated Encryption.*

[b-ISO/IEC 9797] ISO/IEC 9797-1:2011, *Information technology – Security techniques –Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*.

[b-ISO/IEC 18033] ISO/IEC 18033-3:2010, *Information technology – Security techniques –Encryption algorithms – Part 3: Block ciphers.*

[b-ISO/IEC 19772] ISO/IEC 19772:2009, *Information technology – Security techniques – Authenticated encryption.*

[b-ASIACRYPT] Bellare, M., and Namprempre, C. (2000), *Authenticated encryption:* Relations *among notions and analysis of the generic composition paradigm*, in Tatsuaki Okamoto, editor, ASIACRYPT 2000, Vol. 1976 of LNCS, Springer, December, pp. 531-545.

[b-CBCPADD] Vaudenay, S. (2002), *Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS*, EUROCRYPT 2002.

[b-EUROCRYPT] Namprempre, C., Rogaway, P., and Shrimpton, T. (2014), *Reconsidering generic composition*, in Phong Q. Nguyen and Elisabeth Oswald, editors, EUROCRYPT 2014, Vol. 8441 of LNCS, Springer, May, pp. 257-274.

[b-ZT] Li, Zhang, and Xin, Tong (2013), *Threat Modeling and Countermeasures Study for the Internet of Things*, Journal of Convergence Information Technology (JCIT), Vol. 8, No. 5, March.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2018 г.