РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 623 197**(13) **C2**

(51) МПК
H04L 29/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ФОРМУЛА ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21)(22) Заявка: **2014106831, 24.07.2012**

(24) Дата начала отсчета срока действия патента:
24.07.2012

Дата регистрации:
27.06.2017

Приоритет(ы):
(30) Конвенционный приоритет:
25.07.2011 US 61/511,166;
19.04.2012 US 61/635,490

(43) Дата публикации заявки: **27.08.2015** Бюл. № **24**

(45) Опубликовано: **27.06.2017** Бюл. № **18**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **25.02.2014**

(86) Заявка PCT:
IB 2012/053759 (24.07.2012)

(87) Публикация заявки PCT:
WO 2013/014609 (31.01.2013)

Адрес для переписки:
129090, Москва, ул. Б. Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
КЕОХ Сие Лоонг (NL),
ГАРСИЯ МОРЧОН Оскар (NL),
КУМАР Сандип Шанкаран (NL),
БРАХМАНН Мартина (NL),
ЭРДМАНН Божена (NL)

(73) Патентообладатель(и):
ФИЛИПС ЛАЙТИНГ ХОЛДИНГ Б.В. (NL)

(56) Список документов, цитированных в отчете о поиске: **EA 005473 B1, 24.02.2005. RU 2313912 C2, 27.12.2007. EA 008652 B1, 29.06.2007. EA 005914 B1, 30.06.2005.**

(54) СПОСОБЫ, УСТРОЙСТВА И СИСТЕМЫ ДЛЯ СОЗДАНИЯ СКВОЗНЫХ БЕЗОПАСНЫХ СОЕДИНЕНИЙ И ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ПАКЕТОВ ДАННЫХ

(57) Формула изобретения

1. Система (100) связи для безопасной передачи пакетов данных между первым устройством и вторым устройством, при этом система (100) связи, содержащая:

- первую сеть (120), основанную на первом протоколе транспортного уровня,

- первое устройство (124, 136), выполненное с возможностью осуществления связи через первую сеть (120) с другими устройствами, причем первое устройство (124, 136) выполнено с возможностью применения первого протокола безопасности транспортного уровня поверх первого протокола транспортного уровня,

- вторую сеть (108), основанную на втором протоколе транспортного уровня,

- второе устройство (102), выполненное с возможностью осуществления связи через вторую сеть (108) с другими устройствами, причем второе устройство (102) выполнено с возможностью применения второго протокола безопасности транспортного уровня

RU 2623197 C2

RU 2623197 C2

поверх второго протокола транспортного уровня,

- промежуточное устройство (110), выполненное с возможностью осуществления связи через первую сеть (120) с первым устройством (124, 136) и выполненное с возможностью осуществления связи через вторую сеть (108) со вторым устройством (102), и выполненное с возможностью модификации пакетов данных, принимаемых через первую сеть (120), которые сформированы в соответствии с первым протоколом безопасности транспортного уровня, в пакеты данных для осуществления связи через вторую сеть (108) в соответствии со вторым протоколом безопасности транспортного уровня, и наоборот, при этом

- первый протокол транспортного уровня или второй протокол транспортного уровня является сетевым протоколом, основанным на дейтаграмме, а другой из первого протокола транспортного уровня или второго протокола транспортного уровня является протоколом транспортного уровня, ориентированным на надежное соединение,

- первое устройство (124, 136) выполнено с возможностью восстановления заголовка первого пакета данных, принимаемого от промежуточного устройства (110), таким образом, что заголовок соответствует заголовку второго пакета, который был передан вторым устройством (102) промежуточному устройству (110) и был модифицирован промежуточным устройством (110) в первый пакет данных,

- первое устройство (124) выполнено с возможностью проверки поля проверки безопасности принимаемого пакета данных на основании восстановленного заголовка первого пакета данных, причем поле проверки формируется вторым устройством в соответствии со вторым протоколом безопасности транспортного уровня.

2. Система (100) связи по п. 1, в которой первый протокол безопасности транспортного уровня и второй протокол безопасности транспортного уровня инициируют сеанс безопасной связи с протоколом подтверждения установления связи и принимаемый пакет данных является пакетом данных протокола подтверждения установления связи.

3. Система (100) связи по п. 1, в которой принимаемый пакет данных содержит код аутентификации сообщения (MAC) в качестве поля проверки безопасности для аутентификации аутентичности принимаемого пакета данных.

4. Система (100) связи по п. 1, в которой первое устройство (124, 136) выполнено с возможностью сначала проверять код проверки безопасности в соответствии с первым протоколом безопасности транспортного уровня и, если эта проверка неудачна, то восстанавливается заголовок первого пакета данных и поле проверки безопасности проверяется на основании восстановленного заголовка первого пакета данных в соответствии со вторым протоколом безопасности транспортного уровня.

5. Система (100) связи для безопасной передачи пакетов данных между первым устройством (124, 136) и вторым устройством (102), при этом система (100) связи, содержащая:

- первую сеть (120), основанную на первом протоколе транспортного уровня,

- первое устройство (124, 136), выполненное с возможностью осуществления связи через первую сеть (120) с другими устройствами, причем первое устройство (124, 136) выполнено с возможностью применения первого протокола безопасности транспортного уровня поверх первого протокола транспортного уровня,

- вторую сеть (108), основанную на втором протоколе транспортного уровня,

- второе устройство (102), выполненное с возможностью осуществления связи через вторую сеть (108) с другими устройствами, причем второе устройство (102) выполнено с возможностью применения второго протокола безопасности транспортного уровня поверх второго протокола транспортного уровня,

- промежуточное устройство (110), выполненное с возможностью осуществления

RU 2623197 C2

RU 2623197 C2

связи через первую сеть (120) с первым устройством (124, 136) и осуществления связи через вторую сеть (108) со вторым устройством (102), и выполненное с возможностью модификации пакетов данных, принимаемых через первую сеть (120), которые формируются в соответствии с первым протоколом безопасности транспортного уровня, в пакеты данных для осуществления связи через вторую сеть (108) в соответствии со вторым протоколом безопасности транспортного уровня, и наоборот,

при этом

- первый протокол транспортного уровня или второй протокол транспортного уровня является сетевым протоколом, основанным на дейтаграмме, а другой из первого протокола транспортного уровня или второго протокола транспортного уровня является протоколом транспортного уровня, ориентированным на надежное соединение,

- первое устройство (124, 136) выполнено с возможностью восстановления заголовка первого пакета данных, принимаемого от промежуточного устройства (110), таким образом, что заголовок соответствует заголовку второго пакета, который был передан вторым устройством (102) промежуточному устройству (110) и был модифицирован промежуточным устройством (110) в первый пакет данных,

- первое устройство (136) выполнено с возможностью формирования поля проверки безопасности для третьего пакета данных, который должен быть отправлен, причем поле проверки безопасности формируется на основании восстановленного заголовка первого пакета данных и формируется в соответствии со вторым протоколом безопасности транспортного уровня.

6. Система (100) связи по п. 5, в которой первый протокол безопасности транспортного уровня и второй протокол безопасности транспортного уровня инициируют сеанс безопасной связи с протоколом подтверждения установления связи, и третий пакет данных, который должен быть отправлен, является пакетом данных протокола подтверждения установления связи.

7. Система (100) связи по п. 5, в которой первое устройство (124, 136) выполнено с возможностью отправки четвертого пакета данных, содержащего поле проверки безопасности, сформированное в соответствии с первым протоколом безопасности транспортного уровня, и отправки третьего пакета данных, содержащего поле безопасности, сформированное в соответствии со вторым протоколом безопасности транспортного уровня.

8. Система (100) связи по п. 5, в которой первое устройство (124, 136) выполнено с возможностью обнаружения того, осуществляет ли первое устройство (124, 136) связь с другим устройством, которое применяет второй протокол безопасности транспортного уровня, и при этом первое устройство (124, 136) выполнено с возможностью отправки третьего пакета данных, содержащего поле безопасности, сформированное в соответствии со вторым протоколом безопасности транспортного уровня, если первое устройство (124, 136) обнаружило, что оно осуществляет связь с другим устройством, применяющим второй протокол безопасности транспортного уровня.

9. Система (100) связи по п. 1 или 5, в которой первым сетевым протоколом связи транспортного уровня является Протокол Пользовательских Дейтаграмм, основанный на Интернет Протоколе, вторым сетевым протоколом связи транспортного уровня является Протокол Управления Передачей основанный на Интернет Протоколе, первым протоколом безопасности транспортного уровня является Протокол Дейтаграмм Безопасности Транспортного Уровня, а вторым протоколом безопасности транспортного уровня является Протокол Безопасности Транспортного Уровня.

10. Система (100) связи по п. 1 или 5, в которой первое устройство (124, 136) выполнено с возможностью применения Ограниченного Прикладного Протокола, а второе устройство выполнено с возможностью применения Протокола Передачи

RU 2623197 C2

RU 2623197 C2

Гипертекста.

11. Устройство (124) приема/передачи данных для использования в системе (100) связи по п. 1, при этом устройство (124) приема/передачи данных содержит:

- первый сетевой интерфейс (126), выполненный с возможностью осуществления связи через первую сеть (120) с другими устройствами, причем первая сеть (120) основана на первом протоколе транспортного уровня, причем первый сетевой протокол является сетевым протоколом, основанным на дейтаграмме, или протоколом транспортного уровня, ориентированным на надежное соединение

- первое прикладное средство (128) протокола безопасности, выполненное с возможностью применения первого протокола безопасности транспортного уровня поверх первого протокола транспортного уровня,

при этом

- средство (130) восстановления выполнено с возможностью восстановления заголовка принимаемого первого пакета данных таким образом, что заголовок соответствует заголовку второго пакета, который был принят промежуточным устройством (110) через вторую сеть (108), основанную на втором протоколе транспортного уровня, поверх которого используется второй протокол безопасности транспортного уровня, причем первый пакет данных принимается от промежуточного устройства (110) через первую сеть (120),

- средство (132) проверки выполнено с возможностью проверки поля проверки безопасности принимаемого пакета данных на основании восстановленного заголовка первого пакета данных, причем поле проверки формируется в соответствии со вторым протоколом безопасности транспортного уровня.

12. Устройство (136) приема/передачи данных для использования в системе (100) связи по п. 5, при этом устройство (136) приема/передачи данных содержит:

- первый сетевой интерфейс (126), выполненный с возможностью осуществления связи через первую сеть (120) с другими устройствами, причем первая сеть (120) основана на первом протоколе транспортного уровня, причем первый сетевой протокол является сетевым протоколом, основанным на дейтаграмме, или протоколом транспортного уровня, ориентированным на надежное соединение,

- первое прикладное средство (128) протокола безопасности, выполненное с возможностью применения первого протокола безопасности транспортного уровня поверх первого протокола транспортного уровня,

при этом

- средство (130) восстановления выполнено с возможностью восстановления заголовка принимаемого первого пакета данных таким образом, что заголовок соответствует заголовку второго пакета данных, который был принят промежуточным устройством (110) через вторую сеть (108), основанную на втором протоколе транспортного уровня, поверх которого используется второй протокол безопасности транспортного уровня, причем первый пакет данных принимается от промежуточного устройства (110) через первую сеть,

- средство (134) формирования выполнено с возможностью формирования поля проверки безопасности для третьего пакета данных, который должен быть отправлен, причем поле проверки безопасности формируется на основании восстановленного заголовка первого пакета данных и формируется в соответствии со вторым протоколом безопасности транспортного уровня.

13. Устройство (110) для приема и передачи данных между первой сетью и второй сетью для применения в системе (100) связи по любому из пп. 1 или 5, при этом устройство (110) содержит:

- первый сетевой интерфейс (126), выполненный с возможностью осуществления

RU 2623197 C2

RU 2623197 C2

связи через первую сеть (120) с первым устройством (124, 136), причем первая сеть (120) основана на первом протоколе транспортного уровня,

- второй сетевой интерфейс (106), выполненный с возможностью осуществления связи через вторую сеть (108) со вторым устройством (102), причем вторая сеть (108) основана на втором протоколе транспортного уровня,

- первое прикладное средство (128) безопасности, выполненное с возможностью применения первого протокола безопасности транспортного уровня поверх первого протокола транспортного уровня,

- второе прикладное средство (104) безопасности, выполненное с возможностью применения второго протокола безопасности транспортного уровня поверх второго протокола транспортного уровня, причем первый или второй сетевой протокол является сетевым протоколом, основанным на дейтаграмме, а другой из первого или второго сетевого протокола является протоколом транспортного уровня, ориентированным на надежное соединение, и

- средство (122) модификации, выполненное с возможностью модификации пакетов данных, принимаемых через первую сеть (120), и которые формируются в соответствии с первым протоколом безопасности транспортного уровня, в пакеты данных для осуществления связи через вторую сеть (108) в соответствии со вторым протоколом безопасности транспортного уровня, и наоборот.

14. Способ (800) безопасной передачи пакетов данных между первым устройством и вторым устройством, при этом способ (800) содержит этапы, на которых:

- принимают (802) первый пакет данных через первую сеть, основанную на первом протоколе транспортного уровня, причем первый протокол безопасности транспортного уровня применяется поверх первого протокола транспортного уровня,

- модифицируют (804) первый пакет данных во второй пакет данных, который должен быть отправлен через вторую сеть, основанную на втором протоколе транспортного уровня, причем второй протокол безопасности транспортного уровня применяется поверх второго протокола транспортного уровня, причем первый протокол транспортного уровня или второй протокол транспортного уровня является сетевым протоколом, основанным на дейтаграмме, а другой один из первого протокола транспортного уровня или второго протокола транспортного уровня является протоколом транспортного уровня, ориентированным на надежное соединение,

- отправляют (806) второй пакет данных через вторую сеть,

- принимают (808) второй пакет данных,

- восстанавливают (810) заголовок второго пакета данных, принимаемого от промежуточного устройства, таким образом, что заголовок соответствует заголовку первого пакета,

- проверяют (812) поле проверки безопасности принимаемого пакета данных на основании восстановленного заголовка первого пакета данных, при этом поле проверки формируется в соответствии с первым протоколом безопасности транспортного уровня.

15. Способ (850) безопасной передачи пакетов данных между первым устройством и вторым устройством, при этом способ (850) содержит этапы, на которых:

- принимают (852) первый пакет данных через первую сеть, основанную на первом протоколе транспортного уровня, при этом первый протокол безопасности транспортного уровня применяется поверх первого протокола транспортного уровня,

- модифицируют (854) первый пакет данных во второй пакет данных, который должен быть отправлен через вторую сеть, основанную на втором протоколе транспортного уровня, при этом второй протокол безопасности транспортного уровня применяется поверх второго протокола транспортного уровня, причем первый протокол транспортного уровня или второй протокол транспортного уровня является сетевым

RU 2623197 C2

RU 2623197 C2

протоколом, основанным на дейтаграмме, а другой один из первого протокола транспортного уровня или второго протокола транспортного уровня является протоколом транспортного уровня, ориентированным на надежное соединение,

- отправляют (856) второй пакет данных через вторую сеть,

- принимают (858) второй пакет данных, восстанавливают (860) заголовок второго пакета данных, принимаемого от промежуточного устройства, таким образом, что заголовок соответствует заголовку первого пакета,

- формируют (862) поле проверки безопасности для третьего пакета данных, при этом поле проверки безопасности формируется на основании восстановленного заголовка первого пакета данных и формируется в соответствии с первым протоколом безопасности транспортного уровня,

- отправляют (864) третий пакет данных через вторую сеть.

RU 2623197 C2