INCREASED COMMUNICATION SECURITY

BACKGROUND

The Constrained Application Protocol (CoAP) is a protocol for allowing computer systems or devices to communicate by exchanging messages. The protocol specifies certain parameters related to message format and message exchange rules. Messages sent over CoAP can be relatively small in size, and therefore, CoAP allows communication between computer systems or devices with limited processing resources and/or limited storage resources. These computer systems or devices are sometimes referred to as “constrained nodes” or “constrained devices.”

To address security concerns associated with communication via CoAP messages, it has been suggested that messages sent over CoAP use Datagram Transport Layer Security (DTLS). Although DTLS can increase the security of communications, it does not provide for authentication of the sender of the CoAP message.

SUMMARY

Embodiments disclosed herein are directed to increased security for communication of Constrained Application Protocol (CoAP) messages between computer systems or devices. Authentication data may be generated and included in a CoAP message communicated from a first computer system for delivery to a second computer system. The authentication data may allow the second computer system to perform message validation for verifying the authenticity of the first computer system

and/or the integrity of the CoAP message. And in one embodiment, where the CoAP message includes a nonce, security can be improved by allowing the second computer system to advantageously detect and/or act on a replay attack.

In one embodiment, an apparatus may include a security component configured to generate authentication data. The security component may be further configured to generate a Constrained Application Protocol (CoAP) message including the authentication data. The apparatus may also include a communication interface configured to communicate the CoAP message.

In another embodiment, an apparatus may include a communication interface configured to receive a Constrained Application Protocol (CoAP) message including authentication data. The apparatus may also include a security component configured to perform message validation based on the authentication data. The apparatus may further include an operation component configured to perform, if the CoAP message is valid, at least one operation associated with the CoAP message.

And in one embodiment, a system may include a first computer system and a second computer system. The first computer system may be configured to generate a Constrained Application Protocol (CoAP) message including authentication data. The first computer system may be further configured to communicate the CoAP message for delivery to the second computer system. The second computer system may be

configured to perform message validation, responsive to receiving the CoAP message, based on the authentication data.

CLAIMS

What is claimed is:

1. An apparatus comprising:
a security component configured to generate authentication data based on message data, wherein said message data includes an authentication mechanism identifier, and wherein said security component is further configured to generate said authentication data using an authentication mechanism associated with said authentication mechanism identifier;
a message generation component configured to generate a Constrained Application Protocol (CoAP) message including said authentication data and said message data; and
a communication interface configured to communicate said CoAP message.

2. The apparatus of claim 1, wherein said communication interface is part of a first computer system, wherein said communication interface is configured to communicate said CoAP message from said first computer system for delivery to a second computer system, and wherein said CoAP message includes a unique identifier associated with said first computer system.

3. The apparatus of claim 1, wherein said authentication mechanism is selected from a group consisting of hash-based message authentication code (HMAC) utilizing a MD5 hash function, HMAC utilizing a SHA-1 hash function, HMAC utilizing a SHA256 hash function, HMAC utilizing a SHA512 hash function, OAuth, OAuth 2.0, and OpenID.

4. The apparatus of claim 1, wherein said communication interface and said security component are part of a first computer system, wherein said communication interface is configured to communicate said CoAP message from said first computer system for delivery to a second computer system, and wherein said security component is further configured to:

access a key associated with said first computer system; and
generate said authentication data using said key.

5. The apparatus of claim 1, wherein said communication interface is configured to communicate said CoAP message using Datagram Transport Layer Security (DTLS).

6. The apparatus of claim 1, wherein said message data is selected from a group consisting of data associated with a header, data associated with a token, data associated with at least one option, data associated with a payload marker, and data associated with at least a portion of a payload.

7. An apparatus comprising:
a communication interface configured to receive a Constrained Application Protocol (CoAP) message including authentication data and message data;
a security component configured to perform message validation based on said authentication data, wherein said security component is further configured to perform said message validation by accessing an authentication mechanism identifier from said message data, and wherein said security component is further configured to perform said message validation using an authentication mechanism associated with said authentication mechanism identifier; and
an operation component configured to perform, if said CoAP message is valid, at least one operation associated with said CoAP message.

8. The apparatus of claim 7, wherein said communication interface is configured to receive said CoAP message from a first computer system, wherein said communication interface and said operation component are part of a second computer system, and wherein said at least one operation is selected from a group consisting of: an operation associated with a method code in said CoAP message; an operation associated with an option in said CoAP message; and a communication of a second CoAP message, associated with said CoAP message, from said second computer system to said first computer system.

9. The apparatus of claim 7, wherein said operation component is configured to perform, if said CoAP message is invalid, at least one other operation associated with said CoAP message.

10. The apparatus of claim 9, wherein said communication interface is configured to receive said CoAP message from a first computer system, wherein said communication interface and said operation component are part of a second computer system, and wherein said at least one other operation is selected from a group consisting of: ignoring said CoAP message; and limiting access of said first computer system to said second computer system.

11. The apparatus of claim 7, wherein said security component is further configured to:
generate second authentication data based on at least a portion of said CoAP message; and
compare said second authentication data to said authentication data to determine whether said CoAP message is valid.

12. The apparatus of claim 11, wherein said communication interface is configured to receive said CoAP message from a first computer system, wherein said communication interface and said security component are part of a second computer system, and wherein said security component is further configured to:
access a unique identifier from said CoAP message, wherein said unique identifier is associated with said first computer system;
access a key based on said unique identifier;
generate said second authentication data using said key;
if said second authentication data correlates to said authentication data, determine that said CoAP message is valid; and
if said second authentication data does not correlate to said authentication data, determine that said CoAP message is invalid.

13. The apparatus of claim 11, wherein said security component is further configured to generate said second authentication data using said authentication mechanism.

14. The apparatus of claim 7, wherein said authentication mechanism is selected from a group consisting of hash-based message authentication code (HMAC) utilizing a MD5 hash function, HMAC utilizing a SHA-1 hash function, HMAC utilizing a SHA256 hash function, HMAC utilizing a SHA512 hash function, OAuth, OAuth 2.0, and OpenID.

15. The apparatus of claim 7, wherein said security component is further configured to:
determine a length of said authentication data based on said authentication mechanism identifier;
remove a portion of said CoAP message based on said length, wherein said portion of said CoAP message includes at least a portion of said authentication data; and
if said CoAP message is free of a payload responsive to removal of said portion of said CoAP message, remove a payload marker from said CoAP message.

16. The apparatus of claim 7, wherein said communication interface is configured to receive said CoAP message from a first computer system, wherein said communication interface and said security component are part of a second computer system, wherein said security component is further configured to determine that said CoAP message is invalid if a condition is not met, and wherein said condition is selected from a group consisting of: said CoAP message includes a unique identifier associated with said first computer system; said CoAP message includes a nonce; said nonce is different from another nonce associated with a previously-received message; a payload of said CoAP message is at least a predetermined size; and a key associated with said first computer system is accessed.

17. The apparatus of claim 7, wherein said communication interface is configured to receive said CoAP message using Datagram Transport Layer Security (DTLS).

18. The apparatus of claim 7, wherein said message data is selected from a group

consisting of data associated with a header, data associated with a token, data associated with at least one option, data associated with a payload marker, and data associated with at least a portion of a payload.

19. A system comprising:
a first computer system; and
a second computer system,
wherein said first computer system is configured to generate a Constrained Application Protocol (CoAP) message including authentication data and message data, and
wherein said first computer system is further configured to communicate said CoAP message for delivery to said second computer system, and
wherein said second computer system is configured to perform message validation, responsive to receiving said CoAP message, based on said authentication data,
wherein said second computer system is further configured to perform said message validation by accessing an authentication mechanism identifier from said message data, and wherein said second computer system is further configured to perform said message validation using an authentication mechanism associated with said authentication mechanism identifier.

20. The system of claim 19, wherein said first computer system is further configured to generate said authentication data using said authentication mechanism, and wherein said authentication mechanism is selected from a group consisting of hash-based message authentication code (HMAC) utilizing a MD5 hash function, HMAC utilizing a SHA-1 hash function, HMAC utilizing a SHA256 hash function, HMAC utilizing a SHA512 hash function, OAuth, OAuth 2.0, and OpenID.

21. The system of claim 19, wherein said second computer system is further configured to perform, if said CoAP message is valid, at least one operation associated with said CoAP message.

22. The system of claim 21, wherein said second computer system is configured to

perform, if said CoAP message is invalid, at least one other operation associated with said CoAP message.

23. The system of claim 22, wherein said at least one other operation is selected from a group consisting of: ignoring said CoAP message; and limiting access of said first computer system to said second computer system.

24. The system of claim 19, wherein said second computer system is further configured to:
generate second authentication data based on at least a portion of said CoAP message; and
compare said second authentication data to said authentication data to determine whether said CoAP message is valid.

25. The system of claim 24, wherein said second computer system is further configured to:
access a unique identifier from said CoAP message, wherein said unique identifier is associated with said first computer system;
access a key based on said unique identifier;
generate said second authentication data using said key;
if said second authentication data correlates to said authentication data, determine that said CoAP message is valid; and
if said second authentication data does not correlate to said authentication data, determine that said CoAP message is invalid.

26. The system of claim 24, wherein said second computer system is further configured to generate said second authentication data using said authentication mechanism.

27. The system of claim 19, wherein said message data is selected from a group consisting of data associated with a header, data associated with a token, data associated with at least one option, data associated with a payload marker, and data

associated with at least a portion of a payload.

28. The system of claim 19, wherein said first computer system is further configured to generate said authentication data based on said message data.

29. The system of claim 19, wherein said first computer system is further configured to:
access a key associated with said first computer system; and
generate said authentication data using said key.

30. The system of claim 19, wherein said first computer system is further configured to communicate said CoAP message using Datagram Transport Layer Security (DTLS).

31. The system of claim 21, wherein said at least one operation is selected from a group consisting of: an operation associated with a method code in said CoAP message; an operation associated with an option in said CoAP message; and a communication of a second CoAP message, associated with said CoAP message, from said second computer system to said first computer system.

32. The system of claim 19, wherein said second computer system is further configured to:
determine a length of said authentication data based on said authentication mechanism identifier;
remove a portion of said CoAP message based on said length, wherein said portion of said CoAP message includes at least a portion of said authentication data; and
if said CoAP message is free of a payload responsive to removal of said portion of said CoAP message, remove a payload marker from said CoAP message.

33. The system of claim 19, wherein said second computer system is further configured to determine that said CoAP message is invalid if a condition is not met, and wherein said condition is selected from a group consisting of: said CoAP message includes a unique identifier associated with said first computer system; said CoAP message

includes a nonce; said nonce is different from another nonce associated with a previously-received message; a payload of said CoAP message is at least a predetermined size; and a key associated with said first computer system is accessed.