

CLAIMS

We Claim:

1. A computer-implemented method for managing security of a communication network, comprising:

receiving, from a first computing device of the communication network and by a second computing device of the communication network, a message formatted based on a stateless communication protocol for the communication network;

generating, by the second computing device, based on a hash function stored in a storage device associated with the second computing device, a fingerprint of the message, wherein the fingerprint is generated using the hash function based on at least a portion of a header of the message or a portion of a body of the message;

storing, by the second computing device, the generated fingerprint of the message in the storage device, and

detecting, by the second computing device, whether the generated fingerprint of the message has a duplicated fingerprint already stored in the storage device, wherein the message is a retried message or replayed message of a message having the duplicated fingerprint.

2. The method of claim 1, further comprising:

generating, by the second computing device, a response message to indicate a rejection of a service request contained in the message when the second device detects the duplicated fingerprint already stored in the storage device.

3. The method of claim 1, wherein the hash function includes SHA-256, SHA-224, SHA-384, SHA-512, or a secure hash algorithm.

4. The method of claim 1, wherein the stateless communication protocol includes Hyper Text Transfer Protocol (HTTP), HTTP/1.1, HTTP/2, HTTP/3, HTTPS, Internet Protocol (IP), or a stateless sensor network protocol.

5. The method of claim 1, wherein the communication network includes

Internet, a sensor network, or an electronic payment transaction processing network.

6. The method of claim 1, wherein the message is a request message for GET, HEAD, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, or PATCH in a HTTP related protocol.

7. The method of claim 1, wherein the message includes a general-header, a client request-header, or an entity-header.

8. The method of claim 1, wherein the message includes the header and the body, and the header includes a field for date, a time to live (TTL) field, or a correlation identification field, and the body or the header includes authentication data.

9. The method of claim 8, wherein the fingerprint is generated without using authentication data contained in the message.

10. The method of claim 1, wherein the fingerprint is generated using the hash function on at least all fields of the header of the message.

11. The method of claim 1, wherein the first computing device or the second computing device includes a smart phone, laptop, tablet, a personal computer, a server, a camera, a sensor, a router, a switch, an Internet of Thing (IoT) device, a point of sale (POS) terminal, or a transaction terminal.

12. The method of claim 1, wherein the message is one of a set of multiple messages sharing a same correlation identification.

13. An executable software product stored on a non-transitory computer-readable medium containing program instructions that cause a processor of a computing device, in response to execution of the instructions by the processor, to:

receive a message formatted based on a stateless communication protocol for the communication network;

generate, based on a hash function stored in a storage device coupled to the processor, a fingerprint of the message, wherein the fingerprint is generated using the hash function based on at least a portion of a header of the message or a portion of a body of the message;

store the generated fingerprint of the message in the storage device, and

detect, by the processor, whether the generated fingerprint of the message has a duplicated fingerprint already stored in the storage device, wherein the message is a retried message or replayed message of a message having the duplicated fingerprint.

14. The executable software product of claim 13, wherein the program instructions are to cause the processor to further:

generate, by the processor, a response message to indicate a rejection of a service request contained in the message when the second device detects the duplicated fingerprint already stored in the storage device.

15. The executable software product of claim 13, wherein the hash function includes SHA-256, SHA-224, SHA-384, SHA-512, or a secure hash algorithm.

16. The executable software product of claim 13, wherein the stateless communication protocol includes Hyper Text Transfer Protocol (HTTP), HTTP/1.1, HTTP/2, HTTP/3, HTTPS, Internet Protocol (IP), or a stateless sensor network protocol; and

wherein the message is a request message for GET, HEAD, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, or PATCH in a HTTP related protocol.

17. The executable software product of claim 13, wherein the communication network includes Internet, a sensor network, or an electronic payment transaction processing network.

18. A computing device, comprising:
a storage device to store a hash function;
one or more processors coupled to the storage device, wherein the one or more processors are configured to:
receive, from another computing device coupled to the computing device by a communication network, a message formatted based on a stateless communication protocol for the communication network;
generate a fingerprint of the message using the hash function based on at least a portion of a header of the message or a portion of a body of the message;
store the generated fingerprint of the message in the storage device;
detect whether the generated fingerprint of the message has a duplicated fingerprint already stored in the storage device, wherein the message is a retried message or replayed message of a message having the duplicated fingerprint; and
generate a response message to indicate a rejection of a service request contained in the message when the second device detects the duplicated fingerprint already stored in the storage device.

19. The system of claim 18, wherein the hash function includes SHA-256, SHA-224, SHA-384, SHA-512, or a secure hash algorithm;
the stateless communication protocol includes Hyper Text Transfer Protocol (HTTP), HTTP/1.1, HTTP/2, HTTP/3, HTTPS, Internet Protocol (IP), or a stateless sensor network protocol; and
the message is a request message for GET, HEAD, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, or PATCH in a HTTP related protocol.

20. The system of claim 18, wherein the fingerprint is generated without using authentication data contained in the message.