

CLAIMS

WHAT IS CLAIMED IS:

1. A method for detecting information leakage, comprising:

receiving a request message sent from a channel party;

matching a parameter included in the request message against keywords obtained in advance through machine learning, to determine first matching degrees between the parameter and the keywords, wherein the keywords respectively correspond to meanings of the parameter;

determining a matching degree between the parameter and one of the keywords based on the first matching degrees and a context of the parameter in the request message; and

determining information of the request message is leaked and recording related information of the request message when the matching degree is higher than a preset threshold.

2. The method according to claim 1, wherein, the operation of matching a parameter included in the request message against a keyword obtained in advance through machine learning, and obtaining a matching degree between the parameter and the keyword based on the matching result comprises:

splitting the parameter included in the request message into a first sub-parameter and a second sub-parameter according to keywords obtained in advance through machine learning;

matching the keywords obtained in advance through machine learning against the first sub-parameter and the second sub-parameter respectively to determine a first probability of matching between the first sub-parameter and a first keyword and a second probability of matching between the second sub-parameter and a second keyword; and

determining the matching degree between the parameter and the keyword based on the first probability, the second probability, and a context of the parameter in the request message.

3. The method according to claim 1, wherein, after the operation of receiving a request message sent from a channel party, the method further comprises:

determining whether an identifier of non-sensitive information that is set by the channel party is present in the request message; and

determining the information of the request message is not leaked when the identifier of non-sensitive information set by the channel party is present in the request message.

4. The method according to claim 1, wherein, the method further comprises:

obtaining a response packet that is returned to the channel party in response to the request message;

comparing information contained in the response packet against pre-recorded target parameters in corresponding fields of the request message; and

determining the information contained in the response packet is leaked and recording the related information of the response packet when the response packet contains more information than the pre-recorded target parameters of the corresponding fields.

5. The method according to claim 1, wherein, the method further comprises:

obtaining a response packet that is returned to the channel party in response to the request message;

comparing information contained in the response packet against pre-recorded target parameters of corresponding fields of the request message; and

determining the information contained in the response packet is leaked and recording the related information of the response packet when the response packet contains more information than the pre-recorded target parameters of the corresponding fields.

6. A device for detecting information leakage, the device comprising:

a receiving module, configured to receive a request message sent from a channel party;

a matching module, comprising:

a first determination unit, configured to match a parameter included in the request message against keywords obtained in advance through machine learning, to determine first matching degrees between the parameter and the keywords, wherein the keywords respectively correspond to meanings of the parameter; and

a second determination unit, configured to determine a matching degree between the parameter and one of the keywords based on the first matching degrees and a context of the parameter in the request message; and

a first determination module, configured to determine information of the request message is leaked and record related information of the request message when the matching degree is higher than a preset threshold.

7. The device according to claim 6, wherein, the matching module further comprises:

a splitting unit, configured to split the parameter included in the request message into a first sub-parameter and a second sub-parameter according to keywords obtained in advance through machine learning;

a matching unit, configured to match the keywords obtained in advance through machine learning against the first sub-parameter and the second sub-parameter respectively to determine a first probability of matching between the first sub-parameter and a first keyword and a second probability of matching between the second sub-parameter and a second keyword; and

a third determination unit, configured to determine the matching degree between the parameter and the keyword based on the first probability, the second probability, and a context of the parameter in the request message.

8. The device according to claim 6, wherein, the device further comprises:

a determination module, configured to determine whether an identifier of non-sensitive information that is set by the channel party is present in the request message; and

a second determination module, configured to determine the information of the request message is not leaked when the identifier of non-sensitive information set by the channel party is present in the request message.

9. The device according to claim 6, wherein, the device further comprises:

an acquisition module, configured to obtain a response packet that is returned to the channel party in response to the request message;

a comparison module, configured to compare information contained in the response packet against pre-recorded target parameters in corresponding fields of the request message; and

a third determination module, configured to determine the information contained in the response packet is leaked and record the related information of the response packet when the response packet contains more information than the pre-recorded target parameters of the corresponding fields.

10. The device according to claim 6, wherein, the device further comprises:

an acquisition module, configured to obtain a response packet that is returned to the channel party in response to the request message;

a comparison module, configured to compare information contained in the response packet against pre-recorded target parameters in corresponding fields of the request message; and

a third determination module, configured to determine the information contained in the response packet is leaked and record the related information of the response packet when the response packet contains more information than the pre-recorded parameters of the corresponding fields.

11. A server comprising a memory storing an information leakage detection program and a processor configured to execute the information leakage detection program to perform the following operations:

receiving a request message sent from a channel party;

matching a parameter included in the request message against keywords obtained in advance through machine learning, to determine first matching degrees between the parameter and the keywords, wherein the keywords respectively correspond to meanings of the parameter;

determining a matching degree between the parameter and one of the keywords based on the first matching degrees and a context of the parameter in the request message; and

determining information of the request message is leaked and recording related information of the request message when the matching degree is higher than a preset threshold.

12. The server according to claim 11, wherein, the processor is further configured to execute the information leakage detection program stored in the memory to perform the operations of matching the parameter included in the request message against the keyword obtained in advance through machine learning and obtaining the matching degree between the parameter and the keyword, by:

splitting the parameter included in the request message into a first sub-parameter and a second sub-parameter according to keywords obtained in advance through machine learning;

matching the keywords obtained in advance through machine learning against the first sub-parameter and the second sub-parameter respectively to determine a first probability of matching between the first sub-parameter and a first keyword and a second probability of matching between the second sub-parameter and a second keyword; and

determining the matching degree between the parameter and the keyword based on the first probability, the second probability, and a context of the parameter in the request message.

13. The server according to claim 11, wherein, the processor is further configured to execute the information leakage detection program stored in the

memory to further perform the following operations subsequent to receiving the request message sent from the channel party:

- determining whether an identifier of non-sensitive information that is set by the channel party is present in the request message; and

- determining the information of the request message is not leaked when the identifier of non-sensitive information set by the channel party is present in the request message.

14. The server according to claim 11, wherein, the processor is further configured to execute the information leakage detection program stored in the memory to further perform the following operations:

- obtaining a response packet that is returned to the channel party in response to the request message;

- comparing information contained in the response packet against pre-recorded target parameters in corresponding fields of the request message; and

- determining the information contained in the response packet is leaked and recording the related information of the response packet when the response packet contains more information than the pre-recorded target parameters of the corresponding fields.

15. A computer-readable storage medium storing one or more programs that when executed by one or more processors cause the following operations to be performed:

- receiving a request message sent from a channel party;

- matching a parameter included in the request message against keywords obtained in advance through machine learning, to determine first matching degrees between the parameter and the keywords, wherein the keywords respectively correspond to meanings of the parameter;

- determining a matching degree between the parameter and one of the keywords based on the first matching degrees and a context of the parameter in the request message; and

- determining information of the request message is leaked and recording related information of the request message when the matching degree is higher than a preset threshold.

16. The computer-readable storage medium according to claim 15, wherein, the computer-readable storage medium is further configured to perform the operation of matching a parameter included in the request message against a keyword obtained in advance through machine learning, and obtaining a matching degree between the parameter and the keyword based on the matching result:

splitting the parameter included in the request message into a first sub-parameter and a second sub-parameter according to keywords obtained in advance through machine learning;

matching the keywords obtained in advance through machine learning against the first sub-parameter and the second sub-parameter respectively to determine a first probability of matching between the first sub-parameter and a first keyword and a second probability of matching between the second sub-parameter and a second keyword; and

determining the matching degree between the parameter and the keyword based on the first probability, the second probability, and a context of the parameter in the request message.