CLAIMS

1. A security check method for performing a security check between a terminal and a server, the method performed by the terminal, the method comprising:

replacing an original check mode with an updated check mode for performing security checks between the terminal and the server, when performing a security check of a terminal user, by:

acquiring (301; 401) first original check credential information of the original check mode,

generating (302; 402) substitutive credential information for the updated check mode and storing the substantive credential information at the terminal, and

transmitting (304; 404) the first original check credential information, the substitutive credential information, and user information of the terminal user from the terminal to the server for correlation of the substitutive credential information with the user information; and

subsequently performing a security check between the terminal and the server using the updated check mode by:

performing (201) a local check of the terminal user at the terminal via the updated check mode to acquire a local check result,

encrypting (202) the local check result according to the substitutive credential information stored at the terminal to acquire an encrypted check result, and

sending (203) the encrypted check result, the local check result, and user information of the terminal user from the terminal to the server for verification, wherein the local check result is trustable when the encrypted check result is verifiable according to substitutive credential information corresponding to the user information.

2. The security check method according to claim 1, further comprising:

storing (303; 403) the substitutive credential information in a trusted storage area associated with the terminal user, wherein the trusted storage area comprises a trusted execution environment module or a security environment module.

3. The security check method according to claim 1 or claim 2, wherein:

the substitutive credential information comprises a public key and a private key;

transmitting the substitutive credential information comprises transmitting (304) the public key from the terminal to the server;

encrypting the local check result comprises digitally signing (309) the local check result according to the stored private key to acquire signature information; and

sending the encrypted check result comprises sending (310) the signature information from the terminal to the server, wherein the local check result is deemed trustable the signature information is verifiable according to the public key corresponding to the user information.

4. The security check method according to claim 1 or claim 2, further comprising: pre-negotiating, by the terminal with the server, a message abstract algorithm, wherein:

the substitutive credential information comprises a random string;

transmitting the substitutive credential information comprises transmitting (404) the random string from the terminal to the server for correlation with the user information;

encrypting the local check result comprises encrypting (409) the random string and the local check result using the message abstract algorithm to acquire a first encrypted data result; and

sending the encrypted check result comprises sending (410) the first encrypted data result from the terminal to the server for verification, wherein the local check result is trustable if second encrypted data generated by encrypting the local check result and a random string corresponding to the user information using the message abstract algorithm is consistent with the first encrypted data result.

5. A security check method for performing a security check between a terminal and a server, the method executed by the server, the method comprising:

replacing an original check mode with an updated check mode for performing security checks between the terminal and the server, when performing a security check of a terminal user, by:

receiving, from the terminal, first original check credential information, substitutive credential information, and user information of a terminal user, wherein the first original check credential information is check credential information of the original check mode, and the substitutive credential information are for the updated check mode;

searching (305; 405) for second original check credential information corresponding to the user information;

determining (306; 406) whether the first original check credential information is consistent with the second original check credential information; and

storing (307; 407) correlation between the substitutive credential information and the user information in response to determining that the first original check credential information is consistent with the second original check credential information; and

subsequently performing a security check between the terminal and the server in accordance with the updated check mode by:

receiving (211), from the terminal, an encrypted check result, a local check result, and the user information of the terminal user,

acquiring (212) the substitutive credential information corresponding to the user information by searching for the correlation; and

determining (213) that the local check result is trustable by verifying the encrypted check result according to the substitutive credential information corresponding to the user information.

6. The security check method according to claim 5, wherein:

the substitutive credential information comprises a public key and a private key;

receiving the substitutive credential information comprises receiving the public key from the terminal;

receiving the encrypted check result comprises receiving signature information from the terminal;

acquiring the substitutive credential information comprises acquiring (311) a public key corresponding to the user information by searching for the correlation; and

verifying the encrypted check result comprises verifying (313) the signature information using the public key corresponding to the user information.

7. The security check method according to claim 5, wherein:

the substitutive credential information comprises a random string;

receiving the substitutive credential information comprises receiving the random string from the terminal;

receiving the encrypted check result comprises receiving a first encrypted data result from the terminal;

acquiring the substitutive credential information comprises acquiring (411) a random string corresponding to the user information by searching for the correlation; and

verifying the encrypted check result comprises:

encrypting (412) using the message abstract algorithm the random string corresponding to the user information and the local check result to acquire a second encrypted data result, and

verifying (413) that the second encrypted data result is consistent with the first encrypted data result.

8. A terminal, comprising:

a processor; and

a memory for storing instructions executable by the processor,

wherein the processor is configured to execute the method according to any one of claims 1 to 4.

9. A server, comprising:

a processor; and

a memory for storing instructions executable by the processor,

wherein the processor is configured to execute the method according to any one of claims 5 to 7.

10. A computer-readable medium storing instructions which, when executed by a processor of a terminal, cause the terminal to execute the method according to any one of claims 1 to 4.

11. A computer-readable medium storing instructions which, when executed by a processor of a server, cause the server to execute the method according to any one of claims 5 to 7.