CLAIMS

What is claimed is:

1. A method for application information risk management on a network device side, wherein, the method comprises comprising:

acquiring receiving target application information that a user selects and requests for validation by using user equipment a user device (S31), wherein the target application information comprises an SMS message;

validating the target application information to obtain determine corresponding risk information; and (S32);

returning corresponding transmitting a rogue base station prompt information to the user equipment device based on the corresponding risk information. (S33);

wherein, if the corresponding risk information indicates that the SMS message comprises false information sent by a rogue based station, the method further comprises:

sending the rogue base station prompt information to other user devices near the user device, wherein a distance between each other user device and the user device is less than or equal to a predetermined device distance threshold.

2. The method based on of claim 1, wherein the validating the target application information to obtain corresponding risk information comprises:

performing match querying in a corresponding validation database based on a related attribute information of the target application information; and

determining the corresponding risk information based on a record information that is in the validation database and that matches the related attribute information.

3. The method based on of claim 2, wherein the validation database comprises at least one of a library of message templates and a grade that enables successive validation of the target application information.

4. The method of claim 2, wherein the related attribute information comprises at least one of the following:

a sender information of the target application information;

a content of the target application information; or

a user guide information of the target application information.

~~4.~~

5. The method ~~based on~~of claim ~~3~~4, wherein~~:~~:

the related attribute information comprises the user guide information of the target application information~~;~~, and

~~the~~ validating the target application information to obtain corresponding risk information further comprises~~:~~

~~when~~, if no record information that matches the user guide information is identified in the validation database, simulating an execution of the target application information based on the user guide information to obtain the corresponding risk information.

~~5.~~

6. The method ~~based on~~of claim ~~4~~5, wherein ~~when no record information that matches the user guide information is identified in the validation database, the~~ simulating the execution of the target application information based on the user guide information to obtain the corresponding risk information comprises:

~~when no record information that matches the user guide information is identified in the validation database, simulating~~ simulating acquiring, based on the user guide information, target information that is in the target application information and that the user is guided to acquire; and

validating a correspondence between the target information and the target application information to obtain the corresponding risk information.

~~6.~~

7. The method ~~based on~~of claim ~~5~~6, wherein ~~the~~ validating the correspondence between the target information and the target application information comprises at least one of the following:

checking whether a sender information of the target information is consistent with the sender information of the target application information;

checking whether a content of the target information is associated with the content of the target application information; ~~or~~and

checking whether a sandbox operation information of the target information matches the target application information.

~~7.~~

8. The method ~~based on any one~~ of ~~claims~~claim 1~~ to 6~~, wherein the ~~target application information~~SMS message comprises ~~an SMS message; and~~

~~the method further comprises:~~

~~when the risk information is that the SMS~~a Smishing message~~ is false information, sending rogue base station prompt information to nearby user equipment of the user equipment, wherein a distance between the nearby user equipment and the user equipment is less than or equal to a predetermined device distance threshold~~.

~~8. A method~~

9. An apparatus for application information risk management~~ on a user equipment side, wherein the method comprises:~~

~~acquiring target application information that a user selects and requests for validation by using user equipment;~~

~~sending the target application information to a corresponding network device; and~~

~~acquiring prompt information that is returned by the network device and that is based on risk information of the target application information.~~

~~9. The method based on claim 8, wherein the method further comprises:~~

~~performing a risk pre-analysis on application information received by the user equipment; and~~

~~displaying, in a corresponding application, one or more pieces of risky application information acquired through the risk pre-analysis, wherein~~

~~the acquiring target application information that a user selects and requests for validation by using user equipment comprises:~~

~~acquiring the target application information that the user selects from the one or more pieces of application information and requests for validation by using the user equipment.~~

~~10. A network device for application information risk management, wherein the device comprises:~~

~~a target application information acquiring apparatus, configured to acquire target application information that a user selects and requests for validation by using user equipment;~~

~~a target application information validation~~, the apparatus~~, configured to validate the target application information to obtain corresponding risk information; and~~

~~a prompt information sending apparatus, configured to return corresponding prompt information to the user equipment based on the risk information.~~

~~11. The device based on claim 10, wherein the target application information validation apparatus comprises:~~

~~a match query unit,~~ comprising a plurality of modules configured to perform ~~match querying in a corresponding validation database based on related attribute information~~the method of ~~the target application information; and~~

~~a first risk information determining unit, configured to determine the corresponding risk information based on record information that is in the validation database and that matches the related attribute information.~~

~~12. The device based on claim 11, wherein the related attribute information comprises at least one of the following:~~

~~sender information of the target application information;~~

~~content of the target application information; or~~

~~user guide information of the target application information.~~

~~13. The device based on claim 12, wherein the related attribute information comprises the user guide information of the target application information; and~~

~~the target application information validation apparatus further comprises:~~

~~a second risk information determining unit, configured to: when no record information that matches the user guide information is identified in the validation database, simulate execution of the target application information based on the user guide information to obtain the corresponding risk information.~~

~~14. The device based on claim 13, wherein the second risk information determining unit is configured to:~~

~~when no record information that matches the user guide information is identified in the validation database, simulate acquiring, based on the user guide information, target information that is in the target application information and that the user is guided to acquire; and~~

~~validate correspondence between the target information and the target application information to obtain the corresponding risk information.~~

~~15. The device based on claim 14, wherein the validating correspondence between the target information and the target application information comprises at least one of the following:~~

checking whether sender information of the target information is consistent with the sender information of the target application information;

checking whether content of the target information is associated with the content of the target application information; or

checking whether sandbox operation information of the target information matches the target application information.

16. The device based on any one of claims 10 to 15, wherein the target application information comprises an SMS message; and

the device further comprises:

a rogue base station prompt information sending apparatus, configured to: when the risk information is that the SMS message is false information, send rogue base station prompt information to nearby user equipment of the user equipment, wherein a distance between the nearby user equipment and the user equipment is less than or equal to a predetermined device distance threshold.

17. User equipment for application information risk management, wherein the device comprises:

a user selected target application information acquiring apparatus, configured to acquire target application information that a user selects and requests for validation by using user equipment;

a target application information sending apparatus, configured to send the target application information to a corresponding network device; and

a prompt information receiving apparatus, configured to acquire prompt information that is returned by the network device and that is based on risk information of the target application information.

18. The device based on claim 17, wherein the device further comprises:

a risk pre-analysis apparatus, configured to perform a risk pre-analysis on application information received by the user equipment; and

an application information display apparatus, configured to display, in a corresponding application, one or more pieces of risky application information acquired through the risk pre-analysis, wherein

the user selected target application information acquiring apparatus is configured to:

acquire the target application information that the user selects from the one or more

~~pieces of application information and requests for validation by using the user equipment.~~

~~19. A system for application information risk management, comprising the network device based on any one of claims 10 to 16 and the user equipment based on claim 17 or 18.~~

1 to 8.