CLAIMS

What is claimed is:

1. A user security awareness detection method, wherein the method comprises:

obtaining behavior features of a user in different risk dimensions within a predetermined time period;

calculating, based on predetermined weights of different behavior features, absolute weights of the user that correspond to the different risk dimensions, wherein the predetermined weights of the different behavior features are determined based on existing user samples through supervised learning;

separately mapping, to standard intervals based on a predetermined mapping rule, the absolute weights of the user that correspond to the different risk dimensions, and using mapping results as standard weights of the user that correspond to the different risk dimensions; and

calculating ~~the~~ a geometric mean of the standard weights of the user that correspond to the different risk dimensions, and determining ~~the~~ a calculation result as a security awareness score of the user.

2. The method according to claim 1, after the separately mapping, to standard intervals based on a predetermined mapping rule, the absolute weights of the user that correspond to the different risk dimensions, and using mapping results as standard weights of the user that correspond to the different risk dimensions, further comprising:

establishing an equilateral portrait of security awareness of the user by using the different risk dimensions as vertices based on the standard weights of the user that correspond to the different risk dimensions.

3. The method according to claim 2, wherein establishing an equilateral portrait of security awareness of the user by using the different risk dimensions as vertices based on the standard weights of the user that correspond to the different risk dimensions comprises:

establishing the equilateral portrait of the security awareness of the user by using the different risk dimensions as vertices, and displaying, at corresponding locations of the equilateral portrait of the security awareness, the standard weights of the user that correspond to the different risk dimensions.

4. The method according to claim 1, wherein obtaining behavior features of a user in different risk dimensions within a predetermined time period comprises:

obtaining social data, payment-related data, and security research data of the user within the predetermined time period, and extracting the behavior features of the user in the different risk dimensions from the obtained data.

5. The method according to claim 1, wherein the different risk dimensions comprise at least a transaction disclosure risk dimension, a fake order risk dimension, a ticket-related risk dimension, and a relative or friend impersonation risk dimension.

6. The method according to claim 1, wherein determining the predetermined weights of the different behavior features based on existing user samples through supervised learning comprises:

obtaining samples from historical data, determining a deceived user as a black sample user, and determining an undeceived user as a white sample user; and

training a logistic regression model by using the black sample user and the white sample user, and determining different parameters in the logistic regression model as weights of different behavior features comprised in the black sample user and the white sample user.

7. The method according to claim 1, wherein the predetermined mapping rule comprises:

determining an absolute weight of the user in any risk dimension, and obtaining an overall average weight and standard deviation of all users in the risk dimension, so as to determine a standard normal distribution function of the user in the dimension; and

calculating a standard weight of the user in the risk dimension based on the standard normal distribution function of the user in the dimension.

8. A user security awareness detection apparatus, wherein the apparatus comprises:

a behavior feature determining module, configured to obtain behavior features of a user in different risk dimensions within a predetermined time period;

an absolute weight calculation module, configured to calculate, based on predetermined weights of different behavior features, absolute weights of the user that correspond to the different risk dimensions, wherein the predetermined weights of the different behavior features are determined based on existing user samples through supervised learning;

a standard weight calculation module, configured to separately map, to standard intervals based on a predetermined mapping rule, the absolute weights of the user that

correspond to the different risk dimensions, and use mapping results as standard weights of the user that correspond to the different risk dimensions; and

a security awareness determining module, configured to calculate ~~the~~ a geometric mean of the standard weights of the user that correspond to the different risk dimensions, and determine ~~the~~ a calculation result as a security awareness score of the user.

9. The apparatus according to claim 8, after the separately mapping, to standard intervals based on a predetermined mapping rule, the absolute weights of the user that correspond to the different risk dimensions, and using mapping results as standard weights of the user that correspond to the different risk dimensions, further comprising:

establishing an equilateral portrait of security awareness of the user by using the different risk dimensions as vertices based on the standard weights of the user that correspond to the different risk dimensions.

10. The apparatus according to claim 9, wherein establishing an equilateral portrait of security awareness of the user by using the different risk dimensions as vertices based on the standard weights of the user that correspond to the different risk dimensions comprises:

establishing the equilateral portrait of the security awareness of the user by using the different risk dimensions as vertices, and displaying, at corresponding locations of the equilateral portrait of the security awareness, the standard weights of the user that correspond to the different risk dimensions.

11. The apparatus according to claim 8, wherein obtaining behavior features of a user in different risk dimensions within a predetermined time period comprises:

obtaining social data, payment-related data, and security research data of the user within the predetermined time period, and extracting the behavior features of the user in the different risk dimensions from the obtained data.

12. The apparatus according to claim 8, wherein the different risk dimensions comprise at least a transaction disclosure risk dimension, a fake order risk dimension, a ticket-related risk dimension, and a relative or friend impersonation risk dimension.

13. The apparatus according to claim 8, wherein determining the predetermined weights of the different behavior features based on existing user samples through supervised learning comprises:

obtaining samples from historical data, determining a deceived user as a black sample user, and determining an undeceived user as a white sample user; and

training a logistic regression model by using the black sample user and the white sample user, and determining different parameters in the logistic regression model as weights of different behavior features comprised in the black sample user and the white sample user.

14. The apparatus according to claim 8, wherein the predetermined mapping rule comprises:

determining a weight of the user in any risk dimension, and obtaining an overall average weight and standard deviation of all users in the risk dimension, so as to determine a standard normal distribution function of the user in the dimension; and

calculating a standard weight of the user in the risk dimension based on the standard normal distribution function of the user in the dimension.

15. A computer device, comprising a memory, a processor, and a computer program that is stored in the memory and that can run on the processor, wherein when executing the program, the processor implements the method according to claim 1.