The Dynamic Identification Method without Identification Code

Field the Invention

The present invention involves a fully dynamic authentication without identifier, belongs to the information security field.

Background of the Invention

For computer network user authentication, now generally the method of the static identification code (user name and series number etc.), combined with the password (the cryptogram set by the user) is used to confirm the user's identification. Since the static identification code and password in this method remain unchanged during their transmit from the user's terminal to the server for identification authentication, they may be intercepted and captured by a certain hacker in the course of information transmit between the user's terminal and the server and may be utilized by the attacker to imitate an authorized user to beat. Aiming at eliminating this defect in the above static authentication, a new user authentication method has developed based on the above authentication method and the modification from static password to dynamic password (i.e. static identification code + dynamic password). Quite a few products based on this new authentication method have been launched to the market, such as the Dynamic ID card of two-factor authentication based on "cryptographic key – time (event)" provided by the RSA Security Incorporation, which will produce dynamic password automatically on different time for authentication. In fact, any user who uses the dynamic password for authentication will get his dynamic password variation based on a certain rule, and the hacker may makes use of the weakness that the static identification code remains unchanged to follow up and analyze it. He would be able to crack the variation law of the dynamic password and, after capturing enough information, mimic the authorized user to raise attacks.

159159

G00001

Purpose of the Invention

The invention is to provide an authentication that the hacker could not trace and analyze.

Technical Scheme of the Invention

In the fully dynamic authentication method without identifier of the invention, the user's original identification code and authentication code having been encrypted dynamically will be transmitted by the user terminal to the server, and will be decrypted there for identification confirmation.

In the authentication method of the invention, the identification code and authentication code are encrypted and decrypted unitedly. The results of each encryption are different from all the others and there is no a static identification code or feature to be identified each time the user's identification is authenticated, therefore the hacker would not be able to trace, record and analyze the user's authentication information. Thus actually the cracking object of the hacker has to be changed from the variation law of a single user to those of all users, which provides higher security.

Brief Description of the Drawings

Figure 1 is the schematic diagram of the flow of the above authentication method of the invention.

Detailed Description of the Preferred Embodiment

Shown in Figure 1, the original codes are composed of identification codes I_1, I_2, ...I_k and authentication codes P_1, P_2, ...P_k. During authentication, the above original identification codes and authentication codes are encrypted, and a fully dynamic authentication code (M_1, M_2, ...M_k, M_{k+1}, M_{k+2},... M_{k+n}) varying in each authentication is produced, and then the

dynamic identification code (M_1, M_2, ...M_k, M_{k+1}, M_{k+2},... M_{k+n}) is transmitted to the server. The fully dynamic identification code will be decrypted in the server and the original identification code I_1, I_2, ...I_k and the original authentication code P_1, P_2, ...P_k will come out again for the corresponding authentication.

The above encryption course may be set to be carried out by the encryption software or hardware in the user's terminal and any encryption technology may be adopted without any limitation to the encryption method. For instance, the dynamic encryption result may be got by varying encryption method in each authentication or by constant encryption method but varying cryptographic key in each authentication, or even by dynamic encryption method. On the other hand, the fully dynamic authentication code without identifier may be decrypted by the same encryption algorithm system in the server as used in the user's terminal, or by corresponding public cryptographic key in the server while the encryption is done by the private cryptographic key.

The invention is not limited to the above embodiment. The core of the invention is: both the identification code and the authentication code are transformed into the fully dynamic identification code (both the original identification code and the authentication code do not exist any longer), which is transmitted to the server for authentication. Therefore, those authentication methods only by the remained dynamic identification code without authentication code shall belong to the protective scope of the invention.

Claims

1. A fully dynamic authentication method characterized by: the user's original identification code and authentication code are encrypted dynamically in the user terminal and a fully dynamic authentication code is produced there and is transmitted to the server, and the fully dynamic authentication code without identifier will be decrypted in the server for identification confirmation.

2. The fully dynamic authentication method without identifier in the Claim 1, characterized by: a same dynamic encryption algorithm system is adopted both in the user's terminal and the server for encryption and decryption.