Asian Journal of Information Technology 5 (12): 1470-1472, 2006

Hardware Key for Information Systems Users Authentification

Asad Mahmoud Al-Naser
Applied Science Private University, MIS Department, Amman, Jordan

Abstract: The new hardware-software authentification complex of information systems and networks users was developed. In this paper an introduction method of the multi user modes of access rights was used. At concurrence decrypted and a reference line standard procedure of identification is carried out and the user gets access to resources of system.

Key words: Digital certificate, user authentification, hardware key

INTRODUCTION

Wide development of computer technologies is at present observed. They take root into productions, scientific researchers, and a family life. In investigation of it various information computer systems and networks develop, beginning from local and finishing world global. More and more than trading, financial and legal operations are translated in the electronic form. Therefore, sharply there is a problem of restriction and distribution of access to the information for users of information computer systems[1,2].

The solution of this problem provides the solution of two problems: the user authentification problem and the user identification problem. The user authentification process should solve, whether there is an object of authentification that for whom it gives out itself. At identification of the user of information computer system access to all resources of this system should be given it address to which it has the right[3].

Problem of access restriction in information systems: The problem of restriction and distribution of access to the information for users of common use information computer systems and networks is solved at a level of operational systems. A method of introduction of the multi user modes with distribution of access rights is used. In such systems each user has the identifier and the password and with there help authentificate itself in system. The identifier, the password, access rights, system adjustments make a structure of the user, which identifies the user[1].

At creation of a structure rights are given the user on:

- An entrance in system;
- Access to system resources;
- Access to file system;
- Access and an opportunity of modifying of adjustments of the system environment;
- Access to a network.

Creation of structures and distribution of rights is the task of the system administrator, who, accordingly, has the highest priority in system and access right responds[2].

As the password of the administrator gives, actually, the not limited access to the information of users, the majority of attacks of malefactors directed on disclosing the password of the manager. Thus various, rather effective mean are used: Programs of recording of the keyboard, the program of kidnapping of a file of passwords, programs of reading and selection of passwords. This problem becomes a simpler at presence of a plenty users. A vivid example of such organization may be the big educational institutions[2,3].

In the operational systems stipulated authentification procedure and identification of users with the use of the identifier and the password. But the passwords authentification is symmetric cryptosystem with all its lacks. Besides as a rule, operational systems use weak crypto algorithms. Therefore rather frequently there is a necessity of additional program and hardware maintenance use. The task of the offered system, which is a superstructure above standard means of the operational systems are blocking an entrance in system even if to the malefactor the password of the user or the manger is known[1,3].

Architecture of authentification system: The alternative of password authentification is the object authentification mechanism with the use of digital certificates. At use of digital certificates except for checking and checked parties in authentification process the third party takes part. This so-called: arbitrator to which trust both parties. Arbitrator keeps public keys of clients and on the basis of the mechanism of digital certificates guarantees conformity of a public key to the subject. Such circuit is used in asymmetrical systems, and authentification is carried out on the basis of public keys of users, which are sent, with the help of digital certificates.

The international union of telecommunications in 1988 published standard ITU-T X.509 (earlier CCITT X.509) or ISO/IEC/ITU 9594-8, as a part of recommendations of Directory X.500. It defined a standard format of certificates X.509[3].

The digital certificate is structure of the certain format, which is unequivocal authentificate an object. It contains the necessary standard information on the organization which has given out the certificate, some service information and the certain data about the subject to whom the certificate is given out[2,3].

Structure of the offered hardware- software complex is shown in a Fig. 1. The system consists of three basic modules: the server of digital certificates, hardware user key and user authentification system on personal computers.

The server of digital certificates provides generation of pair's keys (public and private) for users; creation and management of certificates according to recommendation ITU-T X.509v3; and except for it, management and synchronization of the distributed database of certificates[2].

Hardware user key is the independent module, which is connected to the computer of the user through the serial interface. It includes the private user key and RSA encryption algorithm crypto core[1].

The user authentification system is a superstructure above the operational system standard authentification module. After OS loading it intercepts management and will carry out authentification procedure behind the password and if necessary, using the hardware key. After the authentification management is transferred operational system.

Functioning of authentification system: Let's consider, functioning a complex in the basic modes. In an information computer network the new user is registered. If, according to a security policy of a network, to it necessary additional authentification, the pair keys is generated and the new certificate is created using the server of digital certificates. Using special programmatic, the private user key writes to hardware key. The created certificate with an open key is kept in a special database of the server of certificates. Besides this certificate, if necessary, is transferred in local databases of user authentification systems on personal computers (PC). From this moment the user becomes to known to information system[1,2,3].

The user of an information network starts work. Before input of the name and the password in a standard authentification window it connects hardware key through the serial interface to the PC. If the user is not

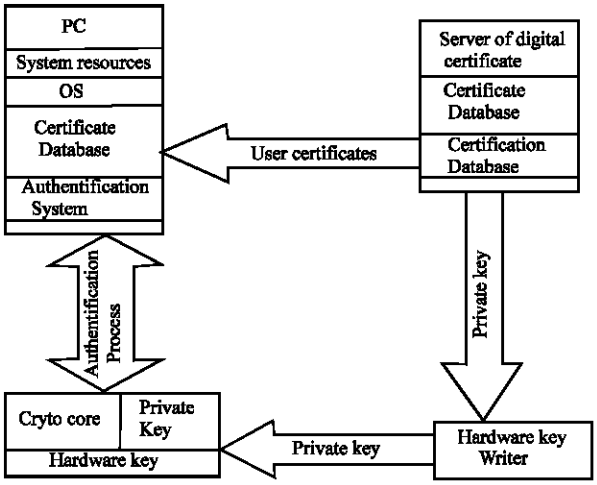

Fig. 1: Structure of authentification system

registered on given PCs the information on it is loaded into a local database of user authentification systems from the server of certificates.

The user authentification systems system receives a name and the password and checks according to a database necessity of hardware key usage. If such necessity is not present, a name and the password of the user are correct, the user starts work.

If it is necessary additional authentification the system generates a random siring and transfers it to hardware key. The hardware key inscription algorithm crypto core, using the private key of the user, ciphers string and transfers in user authentification system. The system, having the public key of the user in a local database of certificates, deciphers the received string. At concurrence decrypted and a reference line standard procedure of identification is carried out and the user gets access to resources of system[2].

Realization of authentification system: The user authentification module is realized as dynamic library DLL (Dynamic Link Library) that redefines necessary functions of standard users authentification library MS GINA. It intercepts management at the moment of a user entrance in system. As there is no necessity to copy all functions MS GINA, was created so-called cover. Its task is redefinition of all functions of standard library, but necessary functions are realized only. And all others cause standard functions MSGINA.dll[1].

Hardware user key is realized as the two-layer printed-circuit-board with bilateral accommodation of elements in the separate case. On the board are placed: a standard socket for consecutive interface DB9, a microcircuit of a serial interface physical level of ADM203JN of form

Analog Devices and microcontroller MSNP430F112IA of firm Texas Instruments. The microcontroller realizes crypto core, in its flash-memory the private key of the user also is kept. Flash-memory is protected from reading from the outside by security bit. Over all dimensions of the device 35×50×20 mm. A power supply of hardware key is carried out from the serial interface of the PC[1,2].

The server of certificates is a program complex, which includes the generator of keys, the center of certification, and the distributed database of certificates. Addition of users in system is carried out through the appropriate graphic user interface of the certificates server. The server of certificates functions on the separate computer of information system[1].

The offered user authentification system allows isolate authentification process from influence of the users that essentially raises reliability of authentification process.

CONCLUSION

Thus, the hardware-software authentification complex of information systems and networks users was developed. It supplements standard means of operational systems and raises resistance breakings. As the hardware key functions through the serial interface of the PC, such system may work practically on any computer, including the built-in solutions. Taking into account low cost of introduction compared with other solutions and high reliability of functioning, such system may be used at operation of different information computer networks.

REFERENCES

1. Housley, R., W. Ford, W. Polk and D. Solo, 1999. Internet X.509 Public key Infrastructure: Certificate and CRL Profile. RFC 2459.
2. ITU-T Recommendation X.509, 2001. Information Technology-Open Systems Interconnection, The Directory: Authentification Framework.
3. Zyma, I.M., 2000. Safety of global network technologies, SPb.: BHV.