Appl. Comput. Math., VOL. 1, NO. 1, 2002

Functional - technological aspects of realization of access control tasks in corporative networks

A.M. Abbasov, R.M. Alguliyev**, R.K. Alekberov***

**Azerbaijan State Economical University, e-mail: ali@dcacs.ab.az*

***Information - Telecommunication Science Center of NASA*

e-mail: rasim@dcacs.ab.az

e-mail: rashid@dcacs.ab.az

Abstract

The functional-technological aspects of realization of tasks of access of controlled objects in protected informational-network environment are addressed in this article with the purpose of that, the analysis of principles of corporate networks building on the basis of inter-network screens with virtualization and segmentation of their resources has been carried out.

1. Introduction

A modern corporative scale information system is a close interlacing of various information resources called for becoming not only a basis of information environment of a company, but a flexible tool of organizational management in complicated and constantly changing conditions. In this situation a complex approach in ensuring information security becomes particularly important. [1,2].

To ensure nowadays a reliable protection of corporative network (CN) resources, designers of security system must undertake a range of organizational and technical steps. Inter-network screens (INS) play especial role in that, being the main means to control the access to CN resources with aim of prevention intrusions on the part of malefactors. Up to the recent time, the INS functions have been oriented towards fairly simple scheme of access:

1. An access was controlled at one point located on the route of connection of CN to Internet or some other public network representing potential threat.
2. All subjects of access were sub-divided into groups by their IP-addresses, mostly into two groups of internal and external users.
3. External users were allowed to use one or two Internet services to access internal and external network resources.

2.Architectural approach to realization of tasks of access control in protected network environment

Nowadays, realization of tasks on control of reciprocal access between CN and Internet is becoming increasingly complicated because of wide use of different kinds of and alternatives to connections between CN and Internet or through Internet as well as strict requirements to protection of resources from internal threats. Moreover, involvement of practically all sub-divisions of a company in automated processing of information and posing by them different requirements to protection of information owned by them during its processing and transfer through critical points of access control bring to necessity of using INS even between internal sub-networks [1,3].

The use of several INS with the limits of single CN requires implementation of operational setting of parameters on the basis of existing authentication rules between subjects of the network as well as co-ordination of their functionality with account of requirements set forth in security policy. In other words, co-ordination of CN in question is necessary to process the users packets correctly in irrespective of access point through which their route is passing. With aim of realization of this security ensuring function, it's necessary to develop centralized access control systems at al controlled points of CN, since under new conditions the changes in relation to subject of access, because together with sub-networks, groups of users and even individual users become subjects of access more often [4].

This is connected, first, with connection of various categories of users to CN through Internet and other global networks, and they need to be given various accesses to internal resources. Second, user orientation is the implication of use of INS for control of traffic between internal sub-networks, which adds to subjects of inter-network access enormous amount of resources and employees of various sub-divisions of a company. In result of this, together with other functions, INS is required to identify big number of user groups, where employees of a company, who work within the limits of CN, remote users and clients using Internet services, are included.

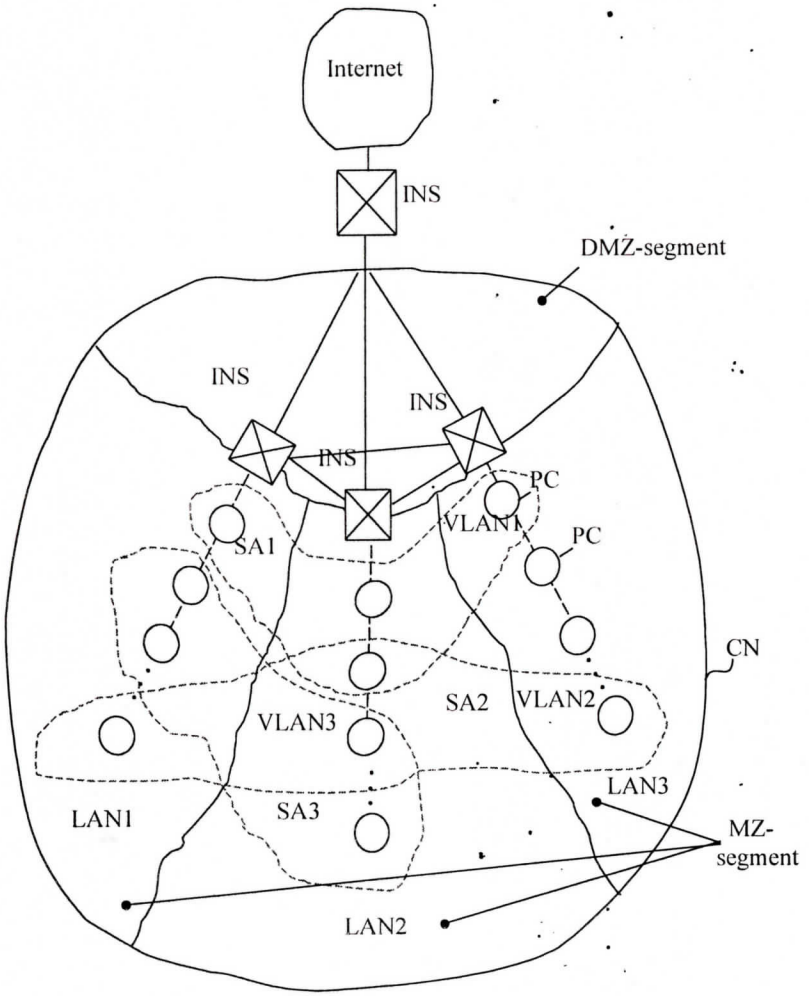
Classification of those user groups by their IP-addresses, which INS used to do traditionally, is practically impossible. Therefore, control at users level requires realization of own authentication means of INS with users account information. The use of numerous INS aimed at delimitation of access between individual sub-networks, physical segments implemented as local area networks (LAN). And administrative requirements to co-ordination of

Appl. Comput. Math., VOL. 1, NO. 1, 2002

tasks on access control between closed groups of users, logical segments (virtual LAN-VLAN) brings to the idea of virtualization of network, telecommunications, information and other resources of CN [5].

On the basis of aforesaid, the functional structure of CN with virtualisation of resources, consisting of physical and logical segments, is given in the drawing.

As seen from the drawing given, INS installed between protected (internal) network and external environment (external networks and other segments of CN) controls all flows of information into internal network and out of it.



Drawing. Functional structure of resources virtualisation based CN.

Control of information flows consist of filtration of them implemented on the basis of a set of authentication rules downloaded preliminarily by the centralized system of control to the screen, proceeding from requirements set forth in company's security policy. Together with this, it's expedient to separate cases, when the screens are installed at the boarder with external network from those ones, where screen is installed at the boarder between segments of the same CN [6].

As known, in interaction with external networks, a family of TCP/IP protocols is often used. Therefore, INS must take into account specifics of and conditions under which those protocols are functioning.

For internal screens, the situation is more complicated, because, apart from TCP/IP, at least Novel Netware based SPX/IPX protocol must be taken into account as well. In connection with this, internal screens must, in most cases, support multi-protocol mode.

It should be noted that INS can be realized at one of the levels of etalon model of open systems interaction, depending on requirements to the level of protection of these or those segments of the network.

Proceeding from these possibilities, INS, apart from blocking of data flows violating security policy, can hide information about network protected, thus hampering actions of potential malefactors. So, the screen realized at application level, can act in the name of subjects of internal network, in result of which, users of external network will maintain interaction with INS exclusively, and in no way will have an opportunity to get information about internal structure of the network.

The analysis of principles of virtualization and segmentation of CN, foreseen for realization of tasks of access control, indicates that performance of INS and requirements to the level of protection at individual points controlled relate conversely to each other. Moreover, the use of more than one INS in CN leads to increase of costs associated with CN administering and operating and increases the risk of unauthorised access from malefactors' side. Let's note that from technical point of view, introduction of centralized database of authentication rules across all objects controlled in CN, maintaining of its actuality in implementation of settings in parallel with the changes in interrelation between objects of authentication rules in INS, is difficult, but feasible task.

As mentioned earlier, the logical segment intended to form protected information

environment for some closed groups of CN users, are made up with the use of VLAN technologies. VLAN ensures high level of network security, ensured with aid of its own Security Administrators (SA), because through connection to the port of protocols analyser concentrator, it's possible to filter all data out on the matter of detection of and prevention from threats transferred in the segment given. If every device is connected to dedicated port of switchboard, then each of them receives only those packets that are addressed to the device connected to the port. Analysis of scientific-technical literature and experience of leading foreign firms shows that there are several main reasons that make Network Security Administrators give more attention to VLAN technology [7].

The most obvious of them is that such virtual networks are easy to bring in line with requirements of closed group of users to the network environment. Amongst other advantages is simplification of administering, higher efficiency in using throughput capacity and even higher level of security in the network. Control of relocation and adding (or distraction) of VLAN users is implemented within short time period and without change to physical structure of CN. Apart from that, with creation of numerous VLAN throughput capacity of CN is used much more efficiently than in traditional networks. When organizing VLAN, the network is broken down into wide-broadcasting domains, the traffic of which is limited by predetermined domain, and does not transferred to all stations in the network. Another reason for wide use of VLAN is in simplification of the process of logically isolated networks creation, which have to be connected with aid of routers, which are serious barriers on routes of error traffics from one network to another one. Actually VLAN are organized on the basis of grouping of ports or protective preparation of MAS-addresses, implemented with aid of switchboards, in which the tasks of performance increasing are resolved for each VLAN simultaneously with the task of isolation of those networks from each other for control over users' rights on access and creation protective barriers between them.

3. Conclusion

As seen, the aforesaid touches only some of the aspects of implementation of control function on the access in CN as well as in interaction with open network environment. Without doubt, realization of aforesaid functional-technical aspects of implementation of control of access to controlled object in protected information-network environment creates necessary preconditions for conduct of scientific-technical research in given area and development of

respective methods, algorithms and software allowing usage of them in design and operating of CN, built on the basis of physically and logically separated segments with virtualization of their potential resources.

References

1. *R.M. Alguliyev,* Methods of synthesis of adaptive systems for information security ensuring in corporate networks. Monograph. Moscow, URSS, 2001, pp. 247
2. *M. Kulgin,* Corporate networks technology. Encyclopaedia. Cpb: Piter, 2000, pp.704
3. *R. Alguliyev, R. Alekperov,* Principles of organization of security information systems in corporative networks. Proceedings of the Fourth International Conference on New Information Technologies, Minsk, Belarus, Vol.1, 2000, pp. 56-58.
4. *R.M. Alguliyev,* Architectural basis of authorised access security to Corporative networks. Transactions of Azerbaijan Academy of Sciences. Series physical-technical and mathematical sciences. Vol. XX, Baku. "Elm", No.1, 2000, pp.176-186.
5. *P.B. Busschbach,* Toward QoS-capable virtual private networks. Bell Labs Technical Journal No.4, 1998, pp.161-175.
6. *C. I. Dalton, J.F.Griffin,* Applying military grade security to the Internet. Computer Networks and ISDN Systems No.5, 1997, pp.1799-1808.
7. *M.K. Reiter,* High confidence distributed systems. IEEE Internet Computing No.6, 1999, pp. 52-55.
8. *P.Morisi,* Seven enterprise scale inter-network screens. Networks and communication systems. No.2, 1999, pp.109-121.

Dr. Ali M. Abbasov received his degree in engineering from the Moscow Power Engineering Institute in 1976. He received his Masters degree in engineering on completion of his postgraduate studies at the Institute of Cybernetics of the Ukrainian Academy of Sciences in Kiev in 1980. After that Dr. Abbasov has spent several years working as Senior Researcher, Head of Laboratory and Chief Engineer at the Institute of Cybernetics and Department of Computer Aided Control Systems of the Azerbaijan Academy of Sciences. In April 1992 he was promoted to the position of Director of the Department of Computer Aided Control Systems of the Azerbaijan Academy of Sciences. Over the period of 1992-1997 he managed to transform the Department into a leading organization in the field of applied information and web-based technologies in Azerbaijan. In 1997 the Department was given a higher status of Information-Telecommunication Scientific Centre of the Azerbaijan National Academy of Sciences, and Dr. Abbasov remained a Director of the Centre till May 2000. Over the whole period of his directorship with the then Department Computer Aided

Appl. Comput. Math., VOL. 1, NO. 1, 2002

Control Systems and now Information-Telecommunication Scientific Centre, Dr. Abbasov could develop strong ties with Scientific Centres of similar profile in Western and Eastern Europe and North America. Being an active member of international scientific computer networks community, he was appointed as a National Coordinator of BITNET/EARN (European Academic Research Networks) and then TERENA (Trans-European Research Educational Networking Association).

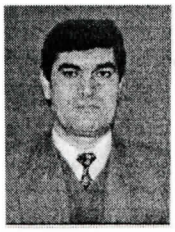
In parallel with his administrative and organizational activity, Dr. Abbasov has always been actively involved in research work in the field of computer network-based distributed data processing systems and knowledge-based systems for control of technological processes of different nature. In 1994 he received his Doctor of Technical Science degree in the field of distributed data processing.

He published more that 100 scientific articles with significant number of them published abroad and he is an author of a monograph dedicated to the main subjects of his research. He participated and made presentations on his scientific achievements at numerous international conferences and symposiums. Along with this, he has been actively involved in educational activity being a lecturer at the Baku State Technical University for many years.

In May 2000 Dr. Ali M. Abbasov was appointed as a Rector of the Azerbaijan State Economical University, which is his present place of work, and in June 2001 he was elected as a Active Member of the Azerbaijan National Academy of Sciences. At the same time he continues his research activity through heading one of the research groups at the Information-Telecommunication Scientific Centre of the Azerbaijan National Academy of Sciences.

Dr. Rasim Alguliev received his degree in Computer Engineering from the Azerbaijan Polytechnic Institute in 1979. After that he joined the Institute of Cybernetics of the Azerbaijan Academy of Sciences in capacity of engineer and continoued, in parallel, his postgraduate studies with the same Institute. In 1994 he received his Candidate of Technical Sciences degree in the field of Information Processing and Control Systems.

Developing further his career in the field of Computer Engineering and Information Technology, Dr. Alguliev has made a career from Senior Engineer through to Chief Engineer of Computer Aided Control Systems Department of the Azerbaijan Academy of Sciences. The Computer Aided Control Systems Department was created in 1986 within the structure of the Academy of Sciences and since then has developed into leading organization in the field of applied information and web-based technologies in Azerbaijan. In 1997 the status of the Department was upgraded to Information-Telecommunication Scientific Center of the Azerbaijan National Academy of Sciences and Dr. Alguliev was promoted to the position of Deputy Director of this Centre. Since the beginning of 2000, he has been Acting Director of the Centre. In this role he has concentrated on further strengthening of positions of the Centre as the most innovative and leading organization in the field of applied information technology within the structure of the National Academy of Sciences as well as in Azerbaijan. Along with his organizational and administrative activity, Dr. Alguliev has continued his scientific research activity in the field of Computer Engineering and Information Technology. Being an Acting Director of the Centre, he heads up one of the Research Groups of the Centre and has recently prepared and submitted for approval to Supreme Attesting Commission of the Azerbaijan Republic his Doctoral dissertation. He is the author of a big number of scientific publications and a monograph devoted to the issue of security in corporate computer networks, a field of science, which has become the main focus of Dr. Alguliev's scientific research over the last few years. He participated and presented the results of his research work at numerous scientific conferences and seminars both, in the country and abroad.



Rashid G. Alekberov , was born in 1953, Chief of Department of ITSC of NASA. Fields of interests: Computer network, network security, computer simulation, corporative network.