computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific Journal of Computing

USERS BEHAVIOR MODEL IN TASKS OF COMPUTER SYSTEMS SECURITY ANALYSIS

V.P. Shyrochin[1)], V.E. Mukhin[2)], Hu Zheng Bing[3)]

1) Ukraine, Professor
2) Ukraine, Associate Professor
3) China, P.h.D
National technical university of Ukraine "KPI"

Abstract: *Security of computer systems of various purpose and the appropriate information technologies appreciably depends on tools of user identification and authentication, and also on tools of the analysis of their behavior and behavior of their programs during reception of access to those or other information resources. This article is devoted to a substantiation of a method of use of a known formalism - state machine for modeling users behavior and to testing of protection tools on detection of attempts of the non-authorized access to information resources, including at early stages of preparation for such actions.*

1. INTRODUCTION

Recently the special attention is paid to such new direction in the field of protection of the information in regional and corporate networks (LANs), as **adaptive security of computer networks**. This direction consists of two basic technologies - the analysis of security (security assessment) and detection of attacks (intrusion detection). In this article the analysis of the most perspective methods and the tools concerning the second technology of maintenance of adaptive security of computer networks is executed. In a number of sources [1, 2, 3] it is offered to use model of the final states machine for modeling abnormal actions of legal users in corporate computer systems and networks. However, amount of information gained by such model of users behavior appreciably depends on opportunities of registration "login" states - actions during identification or authentication of users.

Modern status of attacks modeling and detection problem. Among program and hardware tools which are included in system of information security of corporate computer networks, tools of protection the information are often allocated and used [1], which have been built - in to operational system (mechanisms of sharing access, safe filesystems, safe information exchange protocols, reservation ability) are effectively used; tools of security analysis (at host and network level); and also systems of monitoring of intruders attacks detection (intrusion detection system - idm), with use of one of two technologies: detection of abusing (misuse detection - md) and detection of anomalies (anomaly detection - ad). Systems of monitoring md - idm contain a set of the signatures describing connections and traffic types which specify that concrete attack on computer system is taking place. The second class of systems of monitoring ad - idm uses sets of models of the "normal" the network traffic, updated eventually. The traffic which are not appropriate standard models are marked as abnormal and steadfastly investigated by tools of service of the security manager of system.

Use of second technology AD - IDM more and more attracts attention of researchers, and more than 50 of such subsystems are already developed . The most of monitoring subsystems are intended only for one OS, usually UNIX (for example Kerberos), others are adjusted to concrete architecture of a network and OS (for example Satan), and the third are intended for detection of concrete type of anomalies (attacks) (for example, Crack). - This work is devoted to questions of emulation of abnormal behavior and testing of systems of monitoring AD -IDM of class.

In article tools of imitating modeling of tools of security monitoring in view of abnormal behavior of users and by inclusion of users authentication mechanisms using personal keys are offered, and other, including biometric characteristics. It is shown, that, in spite of significant delays of identification and authentication procedures , an opportunity of testing and duly detection of

abnormal actions on the basis of performance and the analysis of the users state machine essentially grow.

The safe channels organization problem in networks which are called virtual private networks (Virtual Private Network - VPN), may be decided on the basis of two approaches: 1) with the protected final hosts cooperating through an open network, or 2) with the special security equipment on borders of protected area and an open network (firewalls). Technical opportunities of the organization of safe channels are the most various. They may work at various levels of OSI model. Functions of most known SSL protocol correspond to a representative level of model, and the new version of IP network protocol provides all functions of protection: mutual authentication, encryption and integrity maintenance, and the tunneling protocol PPTP protects the data at a channel level [1].

In modern OS'es according to a single entrance principle it is necessary for user to pass all procedures of authentication for granting access to all resources of a network. For this purpose the authentication centralized service, supported by one of network servers (log server) on which registration data database named budgets of users is stored is provided. The registration data alongside with other information necessary for good security contain the data on identifiers and passwords of users. The main problem of realization of authentication schemes is necessity to avoid transfer of the password in unprotected channels.

For research the first approach to the organization of the protected channels is chosen on the basis of the password reusable use and with use of a "call-word". In a basis of Windows NT network security the concept of the domain as sets of users, servers and workstations lays, the registration information about which is stored in general database SAM (Security Accounts Manager database). Centralized help service "Directory Services" carries out also function of users authentication, which at a logic entrance in system executes a client part of service. The domain users authentication is carried out on the basis of their passwords ciphered with the help of a key, stored on a smart-card. The logic organization of the users authentication scheme in Windows NT on the basis of the password repeated use is submitted in a Fig. 1.

At a logic entrance to system the user enters the name in the host - identifier and the password. The client part of a authentication subsystem transfers query to the server storing a database of SAM budgets. The query contains non-encrypted the user identifier, but the password is not transferred in such way. On the client side the password is ciphered on concrete algorithm - 1 with a personal confidential key of user K1. The same algorithm - 1 and a key is applied at storing the digest *d1* the password in database SAM.

On the server side the digest *d1* is calculated preliminary. In reply to the arrived query, a server part of a authentication subsystem generates the random number of casual length named "call -word" *S* (challenge). It is used as a key for encryption of the digest *d1* according to algorithm - 2 and, thus, the answer - digest *d2*, which is transferred on a network to the log-server is formed.

In parallel on the log-server "call-word" *S* is similarly ciphered according to the same algorithm 2 and compared to the received answer - digest *d2* on the server side. The result of comparison testifies to favorable passage of procedure of authentication and thus the user gets access to all or a concrete network resource, depending on realized in system of security politics and rules of access sharing.

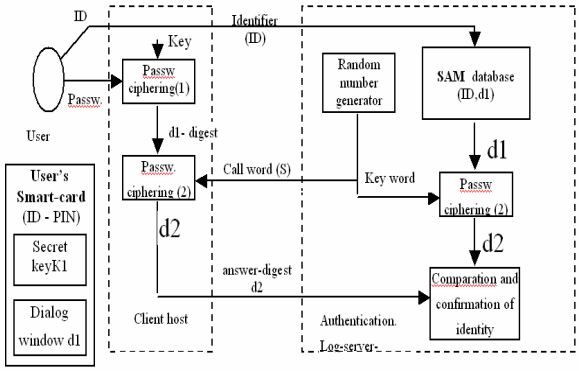

Fig.1 - User authentication scheme with reusable password use.

2. SYSTEM EMULATION

For modeling access granting processes and emulation of attacks of legal infringer are offered tools of imitating modeling of access rights granting processes yo user groups to resources of the distributed system in structure of workstations, routers, servers of applications, the log-server. The stream login - actions structure in modeled system, is submitted on Fig. 2.

Modeling is based on the event-driven approach. Each action of many users in the beginning is processed by the module of a dialog box of the top level. These events will be added to FIFO list (turn FIFO), for the subsequent processing in the appropriate module after a delay, which it is possible to change or set as an information stream of service. The possible events connected to users, may be: turn on set top box (to turn on a dialog box of registration), turn off stb (to switch off a dialog box), login yes (registration successful), login no (registration refused), movie order true (correct

individual key) movie order fails (wrong individual key).

On Fig. 2 the organization of a stream of events in modeled system which is initiated by an login to system is submitted. Events of logins to system are

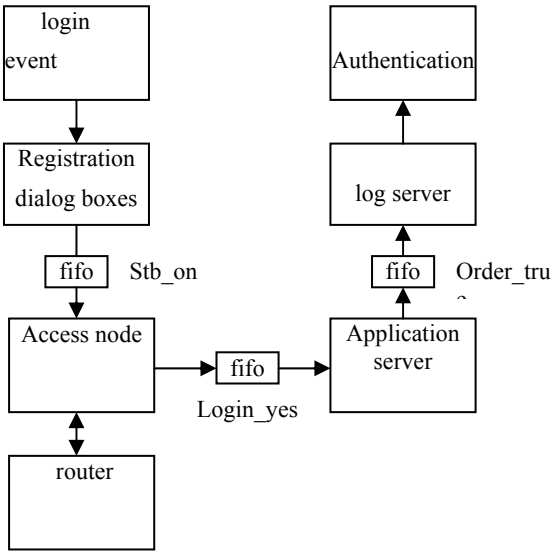

Fig.2 – Login – action stream structure.

transferred from dialog boxes of the top level to the access site (IP the switch) through emulated FIFO list.

Delays, which take place at transition from the main dialog box to the site of access, are reproduced here. From the event access site are transferred to the module - to the router, which counts statistics of routing events. These events also are transferred the protected application server which initiates authentication then the login to system is registered. Independently from whether there was an login to system that is defined (determined) at a user actions emulation stage, log-server generates Authentication Notification (the notice on authentication).

Thus, all events pass through system, and the appropriate modules generate recordings in report magazine, during occurrence of these events. For each component and for everyone emulated transfer of the data on a network the appropriate configured delay is entered. The amount of the traffic taking place through router for various events also can be configured.

The offered model is rough approximation of a real environment of the distributed system. For example, connections between system components are more complex, than in ours emulated system. However, though the statistics of the router is removed through time intervals obviously bigger, than time of a network transfer, it is supposed that to model at IP level of packages is not necessary.

In model static delays and traffic amount in emulated system are used. In real system these values will vary on loading of network etc. transition to use of dynamic variables will not need a lot of time and it will be realized in the following version of the program - the emulator.

The certain problem is also that emulation of actions of users, including attacks, appeared rather slow in the event that set of users show in parallel a plenty of individual keys. The decision of a problem may be optimization on execution time of critical sites of the program of emulation.

3. EMULATION OF THE USER

The main element at modeling attacks on a protected network resource is the universal model of the user behavior, which will allow setting various characters of legal and illegal users actions. As it was told above, *for attacks emulation it is offered to use the user state machine as the finite automate of user behavior in VoD service* . The finite automate, which is realized on this step, is represented in a Fig. 3.

In a state 0 user has on the local host the switched off dialog box of the top level (stb). He may turn it on and pass to a state 1. In a state 1 it may try to login to system. If procedure of login has passed successfully, he passes to automata's state 2 where may show the individual key, for example, on a smart-card or on USB mass Fig.4.

If attempt login to system has not succeed, he forwards to state 3 where may continue attempts to login to system until it will be not possible to him, or he will surrender and will switch off the dialog box of the top level. In a state 2 user may show an individual key. If attempt of presentation of a key has not passed successfully he passes to state 4 where may continue attempts of presentation of a key until these attempts to not be finished by success or he will not switch off the dialog box of the top level. Thus, actions of legal and illegal users, which provide conducting magazine of events in system are modeled.

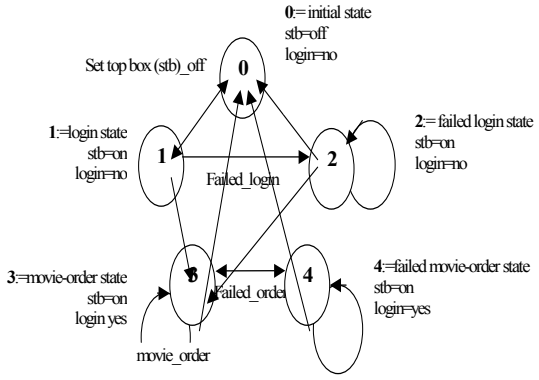

Fig.3 - User state machine in model of monitoring of abnormal actions.

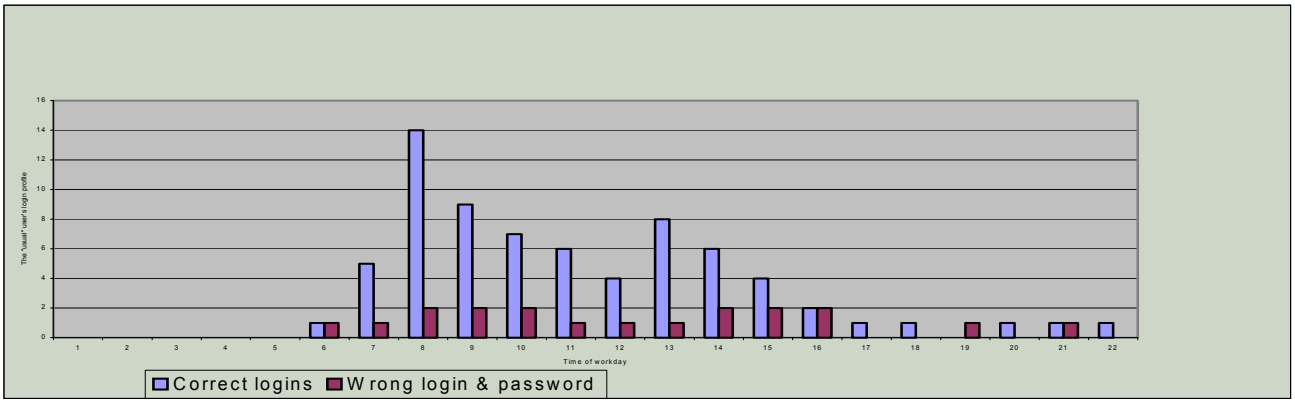

Fig.4 - Profile average quantity of correct and incorrect queries of system users during workdaystorage.

The statistics received at the authentication data analysis in real system, was used for setting of the appropriate probabilities of transitions of the finite state machine for different statuses, and for definition of a time interval starting from an entrance in any state until the termination of the certain transition. The information on time of day and day of week is necessary here for a coordination of various events in modeled system with authentication data in real system.

4. EXPERIMENTS

The list of the events described in of real system magazine, for example, on the data [2, 3], gives not enough information that happened in system and consequently it is difficult to sort the most serious events. Simple overlook the list with quantity of the unusual events caused by each user is more effective. The users who have got in top of the list, should be exposed to more detailed analysis of their profiles in system and other diagrams, with concerned with these users.

On Fig. 4 according to data [3] the example of the general profile of "usual" user in system is presented, with average quantity of logins to system is submitted, which users have made in various time of day and quantity of refusals at attempt of an login to system. As too many work is required on researches of each event about which it is spoken in the report, appeared expedient to analyze behavior of the users who have shown the maximal deviation from norm.

On Fig. 5 profile of the suspected user in the system, registered under number 6 is submitted. This user uses system only from 8 o'clock in the morning till 6 o'clock in the evening. The structure on Fig. 5 looks normal except that during some intervals of time from 13 there are no mistakes at attempt of an login to system, while in the morning till 13 there are a lot of mistakes. At more detailed research of behavior of the suspected user #6 it is revealed, that in the list of reports on abnormal behavior he far overtakes all other users. Any other user for such time interval had no more than 2 inadequate actions.

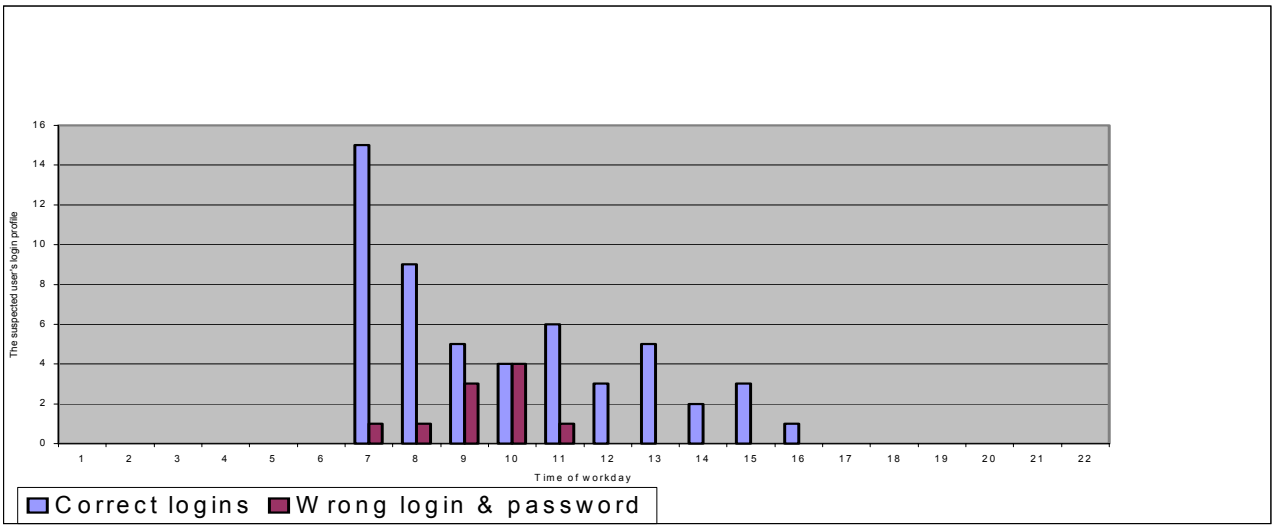

Fig.5 - Profile average quantity of correct and incorrect queries of suspected system users during workday.

On fig. 6 the quantity of logins to the system, made by the user #6, and refusals of logins to system is shown during 24 days. In an interval from 7 numbers up to 13 dates by him it was made more than 50 logins to system daily, however the quantity of refusals in access even is more than successful logins to system. According to data presented by firm [3] reidentification has shown, that it not the usual user, and one of accounts of system process. Appeared, that these problems have appeared right after improvements of system, and within one month the system was used incorrectly.

The profiles of users #6 and #11 were used for calculation on users attacking system state machine. The technique of calculations will be submitted in other work, but the analysis of the data of audit and the appropriate structures of users groups allows to draw the following
preliminary conclusions:

1. Formation of profiles allows to reveal anomalies in actions of users which are reflected in periodic bursts of activity in reception of refusals, be within a working day or during lasting many days work;
2. The analysis of profiles does not give the sufficient information users state machine, as it is necessary to analyze the data of audit by definition of transitions frequencies from a state in a finite state machine;
3. As the abnormal behavior of the user essentially concerns to non-stationary processes during abnormal activity it is necessary to form given - matrixes of probabilities of transitions for each abnormal state that demands the big volume of calculations;
4. For calculation of probabilities of transitions and the task of the user attacking system state machine, it is necessary to estimate rate of actions of the user, i.e. with what minimal period queries to system arrives from him;
5. For imitating modeling attacks on protected system it is expedient to use also Petry networks as the most effective device of the cooperating processes description, especially at a plenty of a corporate network users [4, 5].

5. CONCLUSIONS AND COMMENTS

Experiments have determined some difficulties in definition of behavior anomaly. Despite of all problems, the offered method has some unique features. Experiments have shown, that it is possible to distinguish the usual user of system from the user or the programs, carrying out abnormal actions. Even with the limited number of parameters in a profile, changes in behavior remain obvious enough. It is represented also possible to distinguish users interfering in system, from usual programs by check login profiles and used hosts. The additional opportunity given by system of modeling is an opportunity to find mistakes in behavior of system.

The rating of the offered program tool, certainly, is limited, but it has shown main problems and mistakes of the given method. Instead of managing list of users behavior imitating model it is possible to use the special algorithm determining time of the following inclusion of a registration dialog box, based on probability of turning on of this window in various time and various days of week. Also it is possible to take into account time of day for login to system and presentation of a key right after the user has turned on registration dialog box.

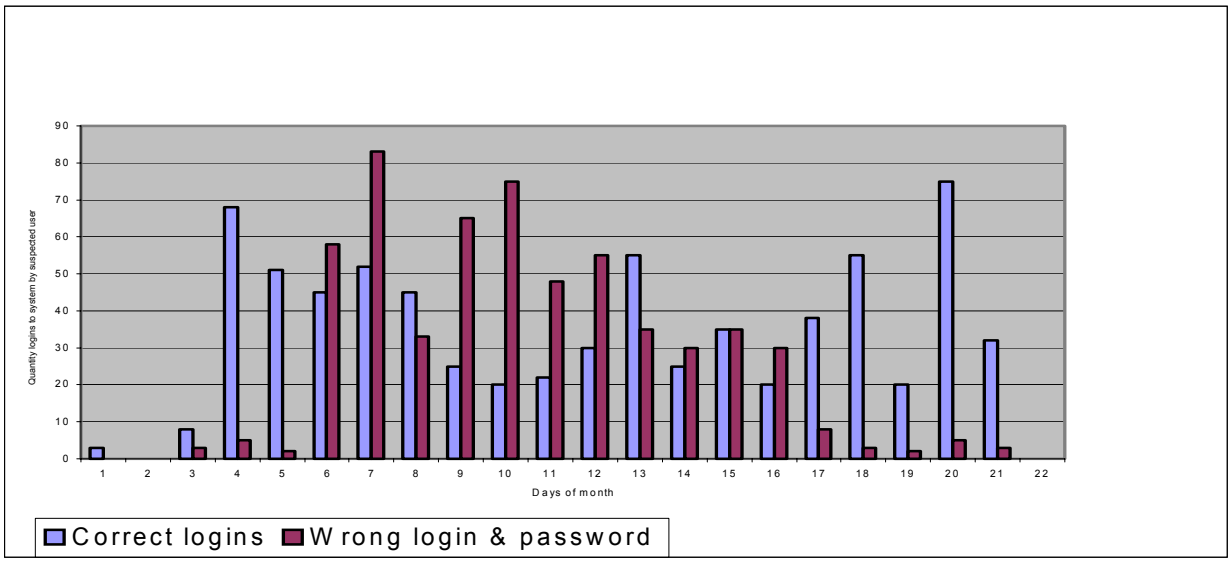

Fig.6 – Profile of correct and incorrect queries of suspected system users during a month.

A lot of time is spent on search of numerical values of transitions probabilities of user state machine, but this method allows to model behavior of the user more adequately in view of the real data collected in reports of audit means. These data also were used, for example, for definition of time delays of system components, and also the network traffic generated by clients of system.

Emulation of the user and modeling of abnormal actions monitoring system are realized using software methods. Actions of virtual users were used for data input in target modeled system, for generating the final data, which may be used for testing.

6. REFERENCES

[1] *В.Г. Олифер, Н.А. Олифер Сетевые операционные системы. СП-б: Питер. 2001. 546 с.*

[2] *M. Chung, N. Puketza, R. Olsson, B. Mukherjee. Simulating concurrent intrusions for testing intrusion detection systems. Paralleling intrusions. In Proceeding of the 1995 National Information Systems Security Conference, pages 173-183, Baltimore, Maryland, October 10-13 1995.*

[3] *H. Debar, M. Dacier, A. Wespi, S. Lampart. An experimentation workbench for intrusion detection systems. Technical Report RZ2998, IBM Research Division. Zurich Research Laboratory. Zurich, Switzerland. March 1998.*

[4] *В.П. Широчин, В.Е. Мухин, А.В. Кулик. Вопросы проектирования средств защиты информации в компьютерных системах и сетях. К: "Век". 1999.- 112 с.*

[5] *В.П. Широчин, В.Е. Мухин . Формализация и целевая адаптация средств аутентификации в компьютерных сетях. Управляющие системы и машины. Тематический выпуск: Интеллектуальные и корпоративные сети. N 5/6, 2000. с. 59-65.*

Shyrochin Valerij Pavlovich *was born 1939 year in t. Tulchin of Ukraine, doctor of technical sciences, professor of the computers engineering and computer science, works into National technical University of Ukraine "Kiev politechnical institute" from 1962 year. Area of scientific work: mathematical theory Petri-nets in tasks of design of safety Software of special computer systems, methods and programming means of computer imitation and simulation of complex systems, processors and algorithms digital signal processing, methods and krypton algorithms of information security in computer systems. In the field of scientific interests suggests and develops the conception and architecture of the emotionally and moral-oriented artificial intelligence, that is realized the processors and functions of men conscious, subconscious and superconscious. Graduated 8 candidates of technical sciences. Has more than 150 scientific and literary published works, including three monographs and twenty methodical manual - text lectures.*

Vadim Mukhin *was born in Kiev in 1971. Received Master of Science Degree in 1994 and Ph.D. in 1997 from National Technical University of Ukraine "Kiev Polytechnic Institute". Associate Professor of Computer System Department of NTUU "KPI". Main scientific interests: users authentication and security monitoring in computer networks; theory of the safety and security of the computer systems and networks.*