VOL. 10, NO 22, DECEMBER, 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

IDENTIFICATION AND COUNTERACTIONS TO ATTACKS OF MALEFACTORS IN THE AUTOMATED WORKING SYSTEM

Krotov L. N., Krotova E. L. and Bogdanov N. V.
Perm National Research Polytechnic University, Perm, Komsomolsky Ave., Russia
E-Mail: denisova.galina@gmail.com

ABSTRACT

Article is devoted to the hot topic of identification of the malefactor in the automated computer system. In the article, standard models of the system of identification of users are described, and methods of optimization and increase of functional capabilities of the similar system are offered. Main areas of work: statistical techniques, wavelet transformation, reduction of load of the computer system by reduction of volumes of the expert knowledge bases checking legality of the operations which are carried out by the user by means of transfer of these functions for the self-training monitoring system of current status of system with use of statistical decisive rules. In the article, the subject of development of modern valuation methods of crypto firmness of the enciphering mechanisms used in cryptographic protocols using Edlmana-Lipton's model is touched.

Keywords: automated working system, malefactor, computer security, statistical modeling, technology comet, overview.

1. INTRODUCTION

At the present stage of development of systems of information security support for identification of malefactors, still broad application is found by the method based on drawing up the base of heuristic knowledge of the behavior of the legal user. Rules and borders in which the legal user of the automated system can act are rigidly registered in this base. At such principle of work, the deviations in the behavior of the user exceeding the fixed threshold are regarded, as sign of malicious actions. Owing to large number governed possibility of self-training at the system constructed by such principle, the lowest. For updating of the set of behavior models of legal users it is also supposed to replace once, a year the used rule set with the new.

The research group offers a new approach to condition monitoring of system based on constructions of a model of the legal user. The profile of the parameters describing the behavior of the legal user is supposed belonging to the class of strictly steady distributions. This hypothesis allows departing from narrow framework of the assumption of normality of distribution of the majority of the observed values describing the standard behavior of the user of the automated system. The hypothesis of normality of observed values does not allow evaluating the necessary volume of selection for the creation of the reliable statistical decisive rule. Transition to wider class of the alternatives including normal distribution, Cauchy's distribution, Levi, and many others will allow constructing the most demonstrative criterion for distinguishing of profile of the legal user from the violator's profile. Unlike classical method of forming of behavior models, by filling of the knowledge base history of actions of users, it is offered to use in exchange the self-training statistical decisive rule allowing building credible intervals for all parameters of mathematical model of the legal user. Besides, using modern methods of nonparametric statistics it is possible to determine a critical number of parameters in which outputs for borders of credible intervals are possible.

2. PROBLEM STATEMENTS AND LITERATURE REVIEWS

For the solution of the problem of choice of the most well-tried cryptographic remedies in data transfer protocols, it is supposed to use Edlmana-Lipton's models from logic DNA for assessment crypto - firmness of the used encryption algorithms. The first important theoretical work connected with information security in DNA logic it is possible to call on applying molecular computation to the Data Encryption Standard which is carried out by scientists Edlmany, Roveysy and others in 1999. In this work, the algorithm of cracking of the known encryption algorithm DES is completely described; calculations of all necessary resources for this purpose are carried out. The main center of researches is California Institute of Technology. Professor Edlman, who is the author of this scientific direction, heads the research, group. Also scientists from other institutes of the United States research. In studying of DNA logic, the group of Veytsmanovsky Institute in Israel is engaged in the certain significant directions. There are separate groups of scientists, which are engaged in DNA logic in the different countries of Europe. However, their researches have mainly theoretical character. In Russia similar experiments and especially nobody researches. No textbooks or monographs of the Russian authors were published; however, there are translations of foreign editions, for example "the DNA computer. New paradigm of calculations" authors of Paun G., Rozenberg G., Salomaa

A. quite complex and not trivial challenge, which consists in choice of way of creation of web application, is set for the developer of the web applications implementing secure system of access to some resource for today. Different aspects of this task, within the existing web technologies, were discussed in works of many research teams, as domestic (Vendorov A.M., Kholchaeva A.V., Yusupova N.I., Zikov S.V., Jogolev E.A., Melnikov A.V., Bikov M. Yu.), and foreign (M. Fernandez, D. Florescu, A. Levy, P. Lockemann, D. Suciu). The standard solution of this task provides creation of web application on the basis of two elements - the client and the server, using different solutions, both on and to ensuring data accessibility and on ensuring their protection, on each of the parties the exchange between which is carried out on the classical model of synchronous interaction in look web applications request answer offered T. Berners-Lee.

Besides, the important issue is the interaction model with the legal user who has lost the authenticating data, for example, lost the password of access to a web resource. The majority of the applications demanding passing of procedure of authorization provides service of recovery of the password. At the standard approach to the solution of this task, the message with the guide to the following actions comes to e-mail specified at registration. Also, what to do if because of attack of the malefactor e-mail was unavailable to you? Whether is it possible to recover the lost contacts? So that the answer to the matter was positive, we have developed a system of recovery of the lost access using confidential persons. At preparatory stage in the Center of Authorization (CA) the list of experts-guarantors who can confirm the personality of the legal user in which join is formed:

- The entrusted communication links with guarantors, for example, e-mail addresses, phone numbers, etc.;
- Competence of guarantors, in the form of weighting coefficients;
- Whom is the guarantor for the user: family member, friend, colleague, etc.

As soon as the user understands that has lost access to the accounting entry, he has to report about it in CA.

3. METHODS

After passing by the user of the system of protection against bots of CA creates a session of recovery of the password (SRP), somehow to identify the user. Also, temporary accounting entry (TAE) as a name for which number SRP serves is created. Using TAE access to the list of guarantors is provided, the authentication process and, in case of success is traced, the user receives the new password.

There are two most probable causes for which the user can address for the new password. Alternatively, its accounting entry was cracked, or he has forgotten the old password. What exactly has occurred depends on that how long last time the password was changed? The less time has passed between change of the password, and the address to CA, the probability of cracking is higher. The period during which the accounting entry will be considered allegedly cracked, we will call pre-moderation time. If the request of the user gets to the pre-moderation interval to the addressed user, the list of guarantors is transferred.

If the password during this time did not change, the user could forget it simply. That will make sure of it, CA sends to the legal user the message in which asks to resolve or forbid procedure of recovery of the password. The more time will not be the answer; the probability of loss of the password is higher. Therefore, if, after pre-moderation time, the answer has not been received, the list of experts-guarantors is transferred to the user.

Further CA itself sends messages to all experts-guarantors from the list, the description of the current situation and with a request to contact the legal user, using the entrusted communication link, for example, personally or by phone. Also in the message, there can be instructions that are more detailed and recommendations about a check of the identity of the user.

Having received the list of experts, the user contacts each of them and describes the problem. Also, the user tells to each of guarantor's number of the SRP.

After that, the expert can address in CA where will have to specify:

- Number SRP of the user;
- Way of user authentication;
- Degree of confidence in the identity of the user on rating scale of experts of guarantors;

Set of these data will also be an assessment of the expert-guarantor. Thus, not anybody except the expert and CA will know expert assessment that will not allow the malefactor to select only positive estimates for CA.

After registration of enough estimates, CA analyzes their reliability and sufficiency.

If conditions are satisfied, authentication is considered successfully passed and on TAE the new password from the accounting, entry is sent.

Now the increasing value is gained by the concept of cloud computing that cornerstone application programming is, having difficult web interfaces.

One of important problems of requests about the web the interface consists that is initial in the messaging protocol of the client and the server there was no concept of a session. At transfer of different information systems

on cloudy Wednesday, it leads to the emergence of some problems of information protection (potentiality of illegal access to means of conversion and information transfer on communication links).

Cardinally other solutions of asynchronous interaction in web applications, with the sentence of new technologies, have been offered in works of D. Crane, P. McCarthy, A. Russell, I. Fette, A. Melnikov, G. Wilkins, D. Davis, M. Nesbitt. Some these technologies have received the name Comet. The part of these technologies assumes input in a two-element model of a web application, the third Comet-servers element that carries out the asynchronous interaction between the client and the server, thereby doing web application by Comet-application.

Comet-technologies allow to implement asynchronous interaction when can be the initiator of data transmission not only the client, but also the server that meets the requirement of fast obtaining information designated earlier for number of specific business processes in stack of web technologies.

However, the creation of Comet-applications is not reflected in the formalized approaches and demands analytical study and the mathematical description both concerning Comet-application in general, and concerning its separate elements unique to these applications, such as Comet-servers. Also, methods and security features of information exchange of such applications, which are interned in the principle of operation of the application, have not been offered.

Thus, development of the ways and methods of creation of the reliable web applications working in real time and at the same time satisfying to high criteria to availability and confidentiality of data using Comet-technology is actual and perspective task.

Development of Comet-applications is hot topic demanded in world web community. Considering dynamics of implementation of Comet-applications on the web Wednesday, there is need of an increase of the level of confidentiality of transmitted data for Comet-application. For the solution of this priority, the algorithm, allowing supporting the policy of access isolation of users admitted to the organizations at the level of Comet-application and the Comet-server without modification of the last is offered. The offered algorithm of protection of identification data of the client of Comet-application excludes possibility of delivery by the malefactor of for the legal user, and excludes possibility of modification or interception of identification data of the client hostile program environment if the client of Comet-application is executed not in the protected hardware-software environment. The algorithm of data security, transmitted via the Comet-server, allows saving confidentiality of data at Comet-server compromise. The offered architecture of Comet-servers allows reducing damage from the implementation of attacks like "failure in service".

The group of authors locates new technique of estimation of unknown parameters of strictly steady laws of the distributions describing the generalized accidental processes of Cox. Complexity of finding of estimates of unknown parameters at this class of distributions it is interfaced first by that, there is no analytical representation of density for the specified family of distributions, secondly, for significant class of representatives of the selected family there is no mathematical expectation, therefore, the majority of standard procedures of statistical estimation is not applicable. The developed method upon transition to invariants of distribution allows to get rid of the disturbing unknown shift - large-scale parameters, and to evaluate only the form parameter, which allows distinguishing profile of the legal user from the malefactor's profile.

4. CONCLUDING REMARKS

Scientific novelty of work is as follows:

a) Novelty of the adapted algorithm of the selective access isolation allowing to implement for the first time within the Web Socket protocol access isolation of clients to the data sent in Comet-application via the Comet-server, algorithm differs in that implements in one communication link under the Web Socket protocol some channels for different categories of data, entering the new message format for exchange of the protected data in Comet-application providing the indication of category of the sent data, the identifier list of clients by which these data are intended, and message time stamps, for assessment of its relevance [1].

b) The algorithm of protection of the identification data of the client sent the Comet-server, which is based on creation of the protected data packet by means of already known ways of cryptographic conversions for prevention, modification or damage by hostile program environment of the client or the malicious client is for the first time offered [1-3].

c) The new algorithm of increase of confidentiality and integrity of the data transmitted via the Comet-server differs in that protects confidential data on all transit from the Web server to the client via the Comet-server, without influencing operation of the Comet-server, and, thereby, allowing it to process the arriving messages in the regular mode, but without access to their source text. This algorithm increases confidentiality of transmitted data by cryptographic conversion of their source text, with the subsequent transport coding of the received ciphertext, for the exception of unauthorized modification or acquaintance with the text of the transferred message [1, 2, 3, 7, 16, 17].

d) Some new mathematical models of the architecture of Comet-servers under the different classes of tasks solved by the Comet-server, for the implementation of the offered algorithms are developed and described. These models differ in that implement

execution of problems of the Comet-server in different flows of execution that allows the Comet-server, at implementation of attack like "failure in service", to lose only part of the functionality realized by the attacked execution flow, but not to fail completely, and, thereby, to save operability of Comet-application in general [8, 9, 13, 20, 21, 23].

e) The faceted classification of technologies of authentication of users in information system based on such essential signs as extent of automation of authentication system, priority of use of authentication mechanism and the used authentication factor, allowing to estimate adequacy of the used technologies of authentication and compliance with their requirements of security is offered [9-13, 15, 19, 24].

f) The mathematical model of process of social authentication allowing the set number of admissible unsatisfactory estimates is developed to calculate probability of successful authentication with use of method of calculation of time of pre-moderation allowing to recover the password as at its loss, and its change by the malefactor, and method of the analysis of estimates of guarantors on the basis of the theory of indistinct sets allowing to carry out authentication of users by means of small number of authorized representatives with different degree of competence [5, 14, 15].

g) The valuation method of quality of systems of social authentication on the basis of GOST 28195-89 differing in use of new quality indicators, such as convenience of the user, cost intensity and security (the first level), the user's costs of authentication, quality of authentication, quality of the entrusted communication link, quality of the interface, ease of mastering, etc. (the second level), financial expenses, ease of mastering, automation level, etc. (the third level) authentication time, simplicity of preset tuning, availability of the web interface of the center of authorization, etc. is offered (the fourth level) that allows to receive integral assessment of quality of system of social authentication [19, 23].

h) The algorithm of work of automated system of restoring access to the accounting entry based on technology of social authentication by means of authorized representatives at which the decision on restoring access is made on the basis of estimates of guarantors different from the existing analogs by availability of check of the entrusted communication links at stage of forming of the list of guarantors, the analysis of activity of the user during the time frame preceding the appeal to system by calculation of time of pre-moderation, opportunity for guarantors to put down negative marks to confidence in the identity of the user, identification of the initiator of start of system by means of number of session of restoring access, and structure of the data transferred to the user in the list of guarantors is developed [5, 6, 18].

REFERENCES

[1] Tyulkin M.V., Krotova E.L., Krotov L.N. and Kapger I.V. 2012. Development of architecture and the organization of information flow in Comet-servers for Comet model web applications with the scheme of the interaction of WEBSOCKET. Models of the architecture of the Comet-server//Bulletin of the Izhevsk state technical university, No. 3, Izhevsk. pp. 118-120.

[2] Tyulkin M.V., Krotova E.L., Krotov L.N. and Kapger I.V. 2012. Development of architecture and the organization of information flow in Comet-servers for Comet model web applications with the scheme of the interaction of WEBSOCKET. Description of the Comet-server//Bulletin of the Izhevsk state technical university, No. 2, Izhevsk. pp. 118-120.

[3] Bogdanov N.V., Krotova E.L. and Shaburov A.S. 2015. Technique of counteraction to attacks like SQLinjection//Science and business: ways of development,Tambov. 6 (48): 38-40.

[4] Malkov A.A., Krotova E.L. and Krotov L.N. 2011. The principle of work of expert systems for recovery of passwords from accounting entries on social networks//the Bulletin of the Izhevsk state technical university, Izhevsk. 4: 147.

[5] Malkov A.A., Krotov L.N. and Krotova E.L. 2011. Search of optimum time of pre-moderation in automated systems of social authentication of final instance//Perspective of science, Tambov. N2 (29): 73-77.

[6] Malkov A.A., Krotov L.N. and Krotova E.L. 2012. Numerical methods of the analysis of expert estimates in systems of social authentication//Management system and information technologies, Voronezh, ISSN: 1729-5068. 1(47): 62-65.

[7] Tyulkin M.V., Krotova E.L., Krotov L.N. and Kapger I.V. 2012. Management of information transform and access isolation for devices of exchange of management systems in the example of the Comet model//the global scientific potential, St. Petersburg. 4 (13): 83-88.

[8] Tyulkin M.V., Krotova E.L., Krotov L.N. and Kapger I.V. 2012. Development of methods of management

of information transforms and access isolation for devices of exchange of management systems in the example of the Comet model. Part 2-implementation//Natural and technical science. 2 (58): 348-351.

[9] Tyulkin M.V., Krotova E.L., Krotov L.N. and Kapger I.V. 2012. Development of methods of management of information transforms and access isolation for devices of exchange of management systems in the example of the Comet model. Part 1 - the Clive protocol//Perspectives of Science, Tambov. 4 (31): 68-72.

[10] Karpova O.O., Osipovich A.E., Krotova E.L. and Krotov L.N. 2011. Approach to the creation of a model of protection of the automated system against illegal access//Bulletin of the Izhevsk state technical university, Izhevsk. 4: 148-149.

[11] Krotov L. and Krotova E. 2012. Statistical modeling based on the unit of random sums for the construction of decision rules in the problems of early diagnosis of cancer. Trilateral Russia-Germany-France Workshop. Oncology: on the Frontiers of Molecular Genetics, Biophysics and Medicine. pp. 20-21.

[12] Krotova E.L. and Krotov L.N. 2013. Regional conference "Competition of the Russian Federal Property Fund - Perm Krai. 10 years: results and perspectives. The conference is held with the financial support of the Russian fund of fundamental researches and the Ministries of the industry, innovations and science of Perm Krai. April 11-12. Section 1. Mathematician, Mechanic and Information Scientist.

[13] Tyulkin M.V., Kapger I.V., Krotova E.L. and Krotov L.N. 2012. Development and implementation of the method of the authorized start and functioning of the protected software product in the potentially hostile hardware-software environment. Information Protection Questions. Moscow. 4 (99): 16-20.

[14] Gorbunov Y.A. 2009. Using a Probabilistic Approach to Distinguish between Legitimate User's and Intruder's Profiles. Applied and Industrial Mathematics Review. 16(3).

[15] Gorbunov Y.A. 2009. Determining the Parameters of the Mathematical Model of the ARM User Profile. Applied and Industrial Mathematics Review. 17(2).

[16] Nesterenko V.A. 2006. Statistical Techniques for Detecting Network Security Violations. Information Processes. 6(3): 208-217.

[17] Karaichev G.V. and Nesterenko V.A. 2010. Network Anomaly Detection through the Statistical Analysis of the IP Packet Headers. Proceedings of Higher Education Institutions. North Caucasus Region. Natural Sciences. 4: 13-17.

[18] Almgren M. 2003. Consolidation and Evaluation of IDS Taxonomies. Proceedings of the Eight Nordic Workshops on Secure IT Systems, NordSec.

[19] Lad M. 2006. PHAS: A Prefix Hijack Alert System. 15th USENIX Security Symposium.

[20] Huston G.M. Rossi and Armitage G. 2011. Securing BGP - A Literature Survey. IEEE Communications Surveys and Tutorials, 2.

[21] Tumoian E. and Anikeev M. 2005. Network-based detection of passive covert channels in TCP/IP // LCN '05. IEEE Conf. on Local Computer Networks. Washington DC., USA.

[22] Ariu D., Tronci R. and Giacinto G. 2011. HMMPayl: An intrusion detection system based on Hidden Markov Models. Computers and Security. 30(4):221-241.

[23] Internet Security Systems. IBM X-Force. 2012. Trend and Risk Report. IBM Global Technology Services, 2013.

[24] Gorbunov Y.A., Krotov L.N. and Krotova E.L. 2014. Detection of an Intruder in an Information System through the Check of Statistic Hypotheses by Certain Statistic Criteria. World Applied Sciences Journal. 29(12).