Journal of Theoretical and Applied Information Technology
10th August 2015. Vol.78. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MATHEMATICAL MODELS OF THREATS OF UNAUTHORIZED ACCESS TO SENSITIVE INFORMATION OF MOBILE NETWORK SUBSCRIBERS AND MEASURES TO PROTECT MOBILE SYSTEM

D.M. MIKHAYLOV, A.V. STARIKOVSKIY, A.V. ZUYKOV, M.I. FROIMSON, A.S. SMIRNOV, N.V. SYCHEV A.YU. BORUCHINKIN, S.D. FESENKO
National Research Nuclear University “MEPhI” (Moscow Engineering Physics Institute)
Kashirskoe highway 31, 115409, Moscow, Russian Federation
E-mail: polynna@yandex.ru

ABSTRACT

The issue of mobile devices’ security is now of great interest as they store and process data more valuable for users than the data stored and processed on personal computers. This paper deals with the development of models of a threat of unauthorized access to confidential information of subscribers to cellular networks, namely: mathematical model of the brute force attack, mathematical model of attacks using software exploits, mathematical model of an attack using additional equipment for its implementation, and mathematical model of attacks using instrument bugs and malicious logic. The article also discloses approaches to the protection of confidential information in cellular communication networks. The implementation of mathematical models discussed in the paper will significantly enhance the information security of mobile devices.

Keywords: *Brute force attack, data protection, exploits, malicious logic, mathematical model of threat/attack, unauthorized access.*

1. INTRODUCTION

Nowadays the share of smartphones and tablet computers in relation to traditional personal computers is observed to increase. A smartphone in terms of functional units (central processing unit, random-access memory, etc.) is actually a computer with small functional differences, which, for example, include the presence of a modem. Like a personal computer, it is running an operating system (OS), which is by its design concept and operating principles in many ways similar to common operating systems for personal computers. Meanwhile, smartphones store and process data, which are usually not less and often even more valuable for its users than the data stored and processed on personal computers: contact lists, private correspondence using SMS-service, notes that the user makes by special software of the smartphone, subscribers call lists with reference to time, e-mail messages and other data. [1]

Data stored on the smartphone is often more up-to-date than data stored on a personal computer, and therefore usually more valuable. A huge number of scientific papers deal with the problem of confidential information of mobile device users’ vulnerability. [2-6]

For example, Mulliner in [7] tells about attacks that can be performed using near field communication (NFC) technology in NFC-Enabled Mobile Phones. Bose and Shin investigate the propagation of mobile worms and viruses spreading primarily via SMS/MMS messages and short-range radio interfaces such as Bluetooth [8]. Also mobile application can be subjected to intrusion [9].

Thus, the main threats to the security of information transmitted via the transmission channel of cellular networks are the following:

— implementation of the passive radio listening;

— attack on the equipment of network subscribers;

— wiretapping of communication channels of network operators, change, distortion, redirection of transmitted information;

— operator equipment overloading, bringing out of operation;

— intentional selling of confidential information to third parties by telecom operators;

— intentional provision of false information to the user with the intent to deceive, mislead or sabotage;

— data gathering through third-party applications installed by the user;

— vulnerabilities usage in operating systems of phone equipment;

— vulnerabilities usage of integrated systems;

— usage of confidential data of users by the software and hardware producing companies for exterior purposes.

Consequently, the problem of protection of mobile devices and the information stored and processed by them from malicious software and illegal actions of third parties is rather an acute issue. It is especially true in case of a local armed conflict. Obviously, data leakage during the fast flowing conflict may lead to verified actions of the enemy. Moreover, use of the untrusted personal mobile devices may lead to revealing the data concerning the military units stationed in the conflict zone even before combat actions.

Several papers have been devoted to the issue of mobile threats and attacks mathematical modeling [10-12] that provide the basis for further improvement of information security of mobile devices. However, as new malware and attacks are created every day, the existing mathematical models should comply with the growing security requirements and be up to date.

It is logical that before proposing measures to improve the protection of the system elements from unauthorized access to information, it is necessary to develop a model of a threat of unauthorized access to confidential information of subscribers to cellular networks.

That is why this paper is devoted to development of mathematical models of threats, which can endanger security of mobile devices and information stored and processed by them. The paper also provide the approaches based on the developed mathematical models to protection of confidential information in cellular communication networks. These models can be used during the development of information protection means.

The implementation of the mathematical models will significantly enhance the information security of mobile devices.

2. MATHEMATICAL MODEL OF OFFENDER

So let us provide a mathematical model of an offender receiving access to a network subscriber's data.

$$\left\{\begin{array}{l}
L(t) = \left(\begin{array}{c}\sum_i \binom{n1}{1} f(t,T)_i \mathrm{OR} \sum_j (\sum_i \binom{n2}{1} f(t,VLR_j)_i \\ \mathrm{OR} \sum_i \binom{n5}{1} f(t,HLR_j)_i)\end{array}\right) \mathrm{AND}\ 1 \\
V(t) = \left(\begin{array}{c}\sum_i \binom{n1}{1} f(t,T)_i\ \mathrm{OR} \sum_j (\sum_i \binom{n3}{1} f(t,MSC_j)_i \\ \mathrm{OR} \sum_i \binom{n4}{1} f(t,BSC_j)_i)\end{array}\right) \mathrm{AND}\ 1 \\
P(t) = \left(\sum_i \binom{n1}{1} f(t,T)_i\ \mathrm{OR} \sum_j (\sum_i \binom{n5}{1} f(t,HLR_j)_i \right) \mathrm{AND}\ 1 \\
\qquad F(t) = \left(\sum_i \binom{n1}{1} f(t,T)_i \right) \mathrm{AND}\ 1
\end{array}\right.$$

where VLR (Visitors Location Register), MSC (Mobile Switching Centre), BSC (Base Station Controller), HLR (Home Location Register) – structural units of the mobile network; L – geolocation data; V – voice data; P – personal data. Function $f(t,X)_i$ within the given mathematical model describes the i-type attack.

Next, consistently analyze the known types of attacks and derive the representation of attack f. For this sake let us briefly analyze the attacks subscriber's personal data is likely to be subjected to.

The simplest attack is an attack, the essence of which is to exploit malicious logic, both software and hardware (undeclared device capabilities in the threats classification). Physical connection to device, remote attacks by wireless communication channels or by wire communication channels, attacks using fake access points or electronic screening tools, as well as any other attacks that are associated with breaking the password, can be attributed to a single class of attacks – attack using brute force. [2], [13]

In a separate class stand out attacks that involve the use of software exploits. Finally, another class of attacks is the attacks which are based on the use of specialized equipment, namely virtual cells. [14]

The proposed division into four classes of attacks allows us to consider four models of attacks based on different time dependences of success of each one. The proposed division covers all the possible types of attacks as well as the grouping allows developing common dependence.

3. MATHEMATICAL MODEL OF BRUTE FORCE ATTACK

Brute force attack [15], [16] is one of the most common methods of obtaining unauthorized access to any information system containing a pair of authentication username-password in its security perimeter. It is mainly due to the fact that almost any attack (except malicious logic and instrument bug) sooner or later is stopped by at authentication system (whether Wi-Fi authentication system or an operating system built-in authentication for obtaining privileges). Brute force attack occurs both when you try to gain unauthorized access to subscribers' telephones and to GSM-network infrastructure.

In general, the brute force password attack allows to gain access in 100% of cases, but the duration of the attack, determined by the total number of combinations and speed of brute force can take a long time even with a short password of 5-10 characters.

Assuming passwords equiprobable the probability density function can be made

$$p(t) = \frac{v}{N_1} * t, t \in [0; \frac{N_1}{v}], \qquad (2)$$

where N_1 – number of possible combinations, v – password check speed.

Along with the total brute force method, there are also dictionaries of commonly used passwords [17]. These dictionaries are based on statistical data on the most commonly used passwords and provide average efficiency of 10-25%, according to various estimates. Thus, taking the probability of finding the password in the dictionary for 15%, the function of the probability density looks as follows

$$p(t) = 0{,}15 * \frac{v}{N_2} * t, t \in [0; \frac{N_2}{v}], \qquad (3)$$

where N_2 – number of passwords in the dictionary.

We now consider the application of existing methods of protection against brute force attacks. Depending on approaches, these methods can be summarized as:

— organizational methods – password policy introduction;

— technical methods – the introduction of mandatory time intervals between authentication attempts.

In terms of representation of the successful password attack probability distribution function, the following amendments to the formula are made:

— password attack speed v becomes a time function (or a constant depending not only on the speed of the communication channel, but also on the system settings);

— restriction on the minimum password length and as a consequence, the minimum value of the total number of combinations N_1 is imposed;

— regular application of the periodical password change policy "resets" the probability of a brute force attack;

— password resistance check eliminates the possibility of a dictionary attack, as correctly implemented mechanism of resistance verification also uses search through potential password dictionary.

Thus, in general, introduction both of organizational and technical measures to protect the system from a brute force authentication attack makes total brute force method the only opportunity to distinguish a password by brute force. The probability distribution function looks as follows

$$p(t) = \frac{v(t)}{N_1} * t, t \in [0; \min(\frac{N_1}{v}; T_{\text{password change}})],$$
(4)

where $T_{\text{password change}}$ is the period between compulsory password changes.

4. MATHEMATICAL MODEL OF ATTACKS USING SOFTWARE EXPLOITS

Gaining unauthorized access by using exploits is the second most common type of attacks against digital infrastructure in order to overcome the security perimeter. Using exploits is the only way to get quick access to perform remote code and to elevate privilege, but exploits are mostly compartmentalized to certain types of operating systems and service software that runs within them. [18]

Mathematical analysis of exploits is aimed not only at description of the current state in the sector of information security, but also at defining a trend, because fundamental changes in the field of information security are not expected until the renovation of the principles of electronic computers functioning. Therefore, the existing trends, well traced by analyzing currently available statistics for mobile and desktop operating systems, will be valid when extrapolating them to the next version of the OS and software.

The dynamics of developing and closing of vulnerabilities in software is defined by the following characteristics:

— all identified vulnerabilities by the next operating system major upgrade (i.e. upgrade concerning the first or second digit of a version) become closed;

— developing of new vulnerabilities almost entirely lays in the field of developing additional functionality;

— continuous vulnerabilities (i.e. vulnerabilities applicable both to previous and new OS) can be considered negligible;

— patch-diffing is a vulnerabilities identify method when updated code is analyzed and to speculations about the vulnerabilities that have been closes in relation to old versions are made. It allows an attacker to detect the so-called 'first-day' vulnerability that were found and closed by the developers;

— possibility to detect the zero-day vulnerabilities, as a rule, are determined by architecture of each specific design solutions and varies slightly from version to version.

Based on the foregoing, it is possible to make a mathematical model of the amount of exploitable vulnerabilities for a given OS version or service software. Number of exploited vulnerabilities is the power of the set below

$$\mathrm{E(V)} = \{\mathrm{k}_0 * \mathrm{N(V, V-1)} \cap \mathrm{k}_1 * \mathrm{N(V, V+1)}\}, \quad (5)$$

where E(V) – the total number of vulnerabilities in the version V of operating system or software; k_0 – vulnerability factor for one new line of code, which can be obtained for any software that exists for several updates – affects the number of zero-day vulnerabilities that were found after the release of the next version;
k_1 – vulnerability factor for one new line of code identified by developers only – affects the amount of the first-day vulnerabilities that were found by patch-diffing after the next release.

It is important to note that at any particular moment exposure of any particular OS or service software to zero- and first-day vulnerabilities can also be evaluated by network information about corresponding vulnerability sales.

Knowing the number of exploitable vulnerabilities, the attack function for an attacker using exploits can be made based on the following criteria:

— each exploit has a finitesimal execution speed, depending on the particular type of exploit;

— attacker uses a standard set of exploits, some of which are not applicable to this platform, which leads to a loss of time during the attack.

Attack function in this case takes the form (the worst case, where attacker first uses inappropriate exploits)

$$\mathrm{f(t)} = \sum_{\mathrm{i}}\{\mathrm{M} / \mathrm{E(V)}\}_{\mathrm{i}} * \mathrm{T_i} + \{\mathrm{M} \cap \mathrm{E(V)}\}_0 * \mathrm{T}_0, \quad (6)$$

where M –variety of exploits the attacker possess, $\mathrm{T_i}$ – time spent on execution of each exploit.

As can be seen from the attack function, the fundamental possibility of obtaining unauthorized access using exploits can be a priori estimated, knowing the specific version V of the operating system used or mounted on a GSM-network infrastructure segment, as well as number M of exploits the attacker possess. The possibility of obtaining unauthorized access exists if $\mathrm{M} \cap \mathrm{E(V)} \not\equiv \{\}$, that is, if there is intersection of the set of exploits and OS vulnerabilities.

Let's generalize the attack function to the case when the target system, in addition to the basic software includes installed service software, which also has vulnerabilities

$$\mathrm{f(t)} = \sum_{\mathrm{i}}\{\mathrm{M} \setminus \cup_{\mathrm{j}} \mathrm{E_j(V)}\}_{\mathrm{i}} * \mathrm{T_i} + \left\{\mathrm{M} \cap \cup_{\mathrm{j}} \mathrm{E_j(V)}\right\}_0 * \mathrm{T}_0, \quad (7)$$

Here we move from one set of operating system vulnerabilities to a set of sets, including service software vulnerabilities.

Let's list the methods which, on the basis of a mathematical model, can be used to reduce the probability of successful attacks via exploits:

— using the latest versions of the software allows to exclude from the list of exploits vulnerabilities ones detected by patch-diffing (i.e. first-day vulnerabilities);

— reduction in the number of service software also reduces the likelihood of a successful exploit attack;

— fundamentally different approach is to use different models of data protection directly within the system that involve the attacker's access to the data. Such a model is, for example, Bella La Padula model (19), also known as the Mandate data access model.

5. MATHEMATICAL MODEL OF ATTACK USING ADDITIONAL EQUIPMENT FOR ITS IMPLEMENTATION

Gaining unauthorized access to data through the use of additional equipment, namely – virtual cells that cause the mobile device to switch from the base station of the mobile service provider to a fake base station, is a specialized attack that can be carried out solely on mobile phones. [20], [21].

During the attack the intruder gains access to the whole data traffic, normally flowing through the provider's network – voice data, packet exchange data and short messages (including USSD-messages, normally considered to be protected and even used by automated teller machines to transmit sensitive data). [14], [21]

Disclosures through the virtual cell assume knowledge of subscriber's location with high accuracy (about 5-10 m), i.e. geolocation data must have already been disclosed.

Success of an attack is mostly determined not by time but rather by distance to the mobile unit, since the probability of switching to a cyber-base station is directly proportional to the strength of the received signal from the cell.

Because the virtual cell has no means of active influence on the mobile device, the attack through it belongs to a class of sniffing-attacks. It makes sense to introduce the concept of threat function that is directly proportional to the time and distance to the subscriber. Disclosure intensity is entirely determined by the intensity of subscriber's activity in GSM network. Threat function can be described as follows:

$$f(t) \sim \int_{t_1}^{t_2} t * r(t)dt, \qquad (8)$$

where r(t) – time dependence of the distance from the virtual cell to the subscriber's mobile phone.

Based on this representation we can make recommendations to ensure the safety of the mobile device from unauthorized access to data through the virtual cell:

— software for locating phone within range of virtual cell should detect the presence of the wiretap equipment in a minimum time;

— subscriber who moves within a small range for a long time is at the greatest risk. For critically important objects virtual cell detection should be done by stationary means.

6. MATHEMATICAL MODEL OF ATTACKS USING INSTRUMENT BUGS AND MALICIOUS LOGIC

Considering the proposed approaches, a mathematical model of the attack using instrument bugs or malicious logic is relatively simple [2].

Obviously, the presence of malicious logic theoretically allows an attacker to have constant access to data stored or processed in the system [2], [22]. Assume that the start time of data transmission as resulting actions of the malicious logic is negligible, as well as data time transmission. This assumption can be considered valid, given the specific features of mobile communications.

However, it is obvious that every tab has a so-called activation time, i.e. the time from which the active tab starts data collection and transmission. This time should be divided separately, as activation time is the moment a malicious logic can be identified and retaliatory measures can be taken by the defending side. We denote such time as T_a. Then the following statement is true

$$f(t) = \begin{cases} \int_{t_1}^{t_2} t * l(t)dt, t > T_a \\ 0, t < T_a \end{cases} \qquad (9)$$

where l(t) –function describing the quality of connection to the global network (or local if the attack is carried out on the local network) at each time point.

Obviously, the main measures to ensure the protection of sensitive GSM-network user's data must be to use verified software that is guaranteed to be free of malicious logic or has service software that can promptly detect unauthorized activation or data transmission.

7. FORMATION OF APPROACHES TO THE PROTECTION OF CONFIDENTIAL INFORMATION IN CELLULAR COMMUNICATION NETWORKS

Based on the proposed mathematical models we can draw some conclusions, in particular:

— it can be assumed that sensitive data stored and processed in mobile networks cannot be reached by a potential attacker for some time t;

— in mobile networks can quickly become obsolete and lose value. For example, geolocation information may not be of interest to an attacker, if he gets it in time that exceeds the time required for an adequate reaction to the object of attack;

— there is a large number of mobile network elements that need a higher level of protection to withstand the attacks;

— customer interested in protecting sensitive data in a mobile communication system cannot hope to succeed protecting only one segment of the mobile network;

— customer interested in protecting sensitive data, has limited resources to be spent on the protection of it;

— in different circumstances customer can be interested in protecting one type of sensitive data more than the other.

Incompleteness of available resources in relation to the foregoing analysis of attack possibilities is obvious. The issue of duplicating resources to improve the reliability and security of the system is not considered in the article. First, these techniques can hardly be implemented for mobile communication network. Second, it is quite an expensive way for the conditions of mobile communication. Duplication related aspects are being considered in dedicated studies, which are ongoing and have wider frame of analysis, rather than attack confrontation.

Figure 1 shows a diagram of the existing segments of the mobile network that can be subjected to an attack and proposed upgraded counteractions.

Analyzing modern attack and protection methods, as well as decomposition of the mobile network elements allows us to offer a number of fundamentally new concepts of information security implementation:

— mobile virtual secure network operator based on the concept of a virtual operator (MVNO – mobile virtual network operator), which allows to use an authorized service provider equipment and implement protection of data channels;

— virtual cells detection equipment;

— trusted mobile operating system.

These concepts allow to influence the time of disclosure in the mobile communication network in accordance with the forequoted mathematical models. In particular, the concepts allow to increase the time during which the confidential information will not be disclosed to the attacker.

The figure depicts:

— DLP – Data Loss Prevention;

— VOIP – Voice over IP-gateway.

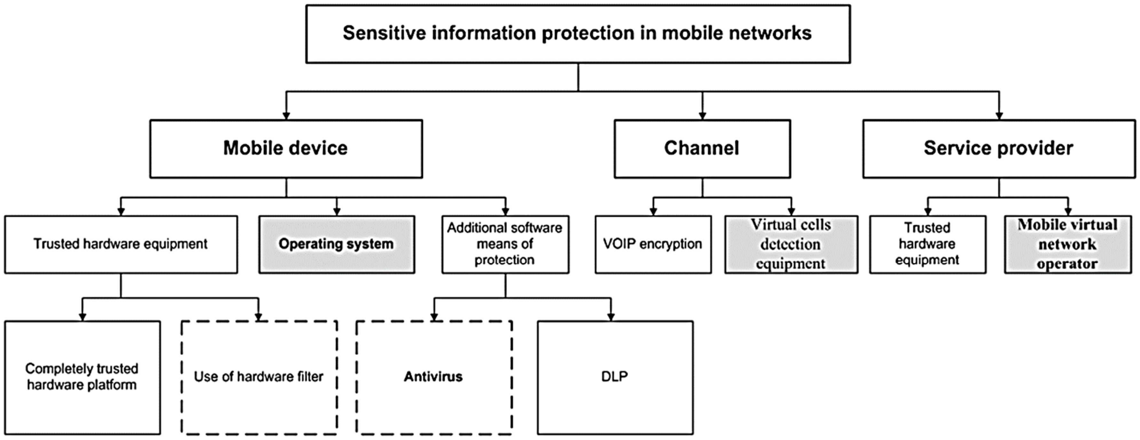
Sensitive information protection in mobile networks
Mobile device
Channel
Service provider
Trusted hardware equipment
Operating system
Additional software means of protection
VOIP encryption
Virtual cells detection equipment
Trusted hardware equipment
Mobile virtual network operator
Completely trusted hardware platform
Use of hardware filter
Antivirus
DLP

Figure 1: A chart of existing mobile network segments, which can be attacked and proposed upgraded security measures.

8. CONCLUSION

Thus, in the article the mathematical analysis of threats, including attacks by programs, exploits, brute force attack and use of the virtual cell on a subscriber's mobile phone is described. Based on analysis, there were measures proposed to improve the security of system components against unauthorized access to information.

It should be noted that there are alternatives to the proposed fundamentally new concepts of information protection and modernization ways of the existing ones that are not inferior to the proposed solutions in terms of complete information protection and sometimes surpass them but much more costly. In this article we basically do not dwell on a detailed comparison of the cost parameters of the proposed solutions. Give only the basic principles on which these assumptions were made:

— mobile virtual network operator conception is based on the assumption that the provider's communications network can be divided into switching subsystem and radio subsystem. Proceeding from this, a special (virtual) dedicated radiophone access system can be created, which will use the existing access network of so-called group of basic providers. On the basis of this division virtual hardware of the dedicated system only can be replaced with the trusted, while leaving the rest of the equipment. Meanwhile it still leads to information security system upgrade through working with the virtual system and SIM-cards used in mobile devices.

Even without detailed calculations in terms of economic viability, use of a mobile virtual network operator as a means of sensitive information protection is evidently competitive;

— use filtering as a solution for undeclared commands is much more justified in terms of the economy, rather than developing own hardware solutions from the very beginning. First, in-house development of trusted hardware (all items of equipment) by definition takes more resources than developing a trusted equipment element. Secondly, according to the current state of the technological development in Russia and standing behind in several key areas, high-quality playback of foreign counterparts cannot be expected soon;

— trusted operating system for mobile devices is unique; it is suggested to abandon using firmware for mobile devices, which did not prove to provide an adequate level of usability;

— virtual cells detection equipment is unparalleled.

It is planned to perform testing of the proposed mathematical models, checking and improving their accuracy.

REFERENCES

[1] Froimson M.I., Kutepov C.V., Tarakanov O.V., Sheremetov A.V. Basic principles of a secure operating system for mobile devices. Journal Specialized machinery and communication №1, 2013. Moscow 2013. Pages: 43-47.

[2] Mikhaylov Dmitry, Zhukov Igor, Starikovskiy Andrey, Kharkov Sergey, Tolstaya Anastasia, Zuykov Alexander. Review of Malicious Mobile Applications, Phone Bugs and other Cyber Threats to Mobile Devices. Proceedings of 2013 5th IEEE International Conference on Broadband Network & Multimedia Technology (5th IEEE IC-BNMT 2013), November 17-19th 2013 Guilin, China. Pages 302-305.

[3] A.G. Beltov, I.Yu. Zhukov, A.V. Novitskiy, D.M. Mikhaylov, A.V. Starikovskiy. Security issues of mobile devices. Journal Security of information technology, № 2 additional. Moscow, 2012. Pages 5-7.

[4] Xinxin Liu; Xiaolin Li. Privacy Preserving Techniques for Location Based Services in Mobile Networks. 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW). Pages: 2474 – 2477.

[5] Jamaluddin, J.; Zotou, N.; Edwards, R.; Coulton, P. Mobile phone vulnerabilities: a new generation of malware. IEEE International Symposium on Consumer Electronics, 2004. Pages: 199 – 202.

[6] Biancucci, G.; Claudi, A.; Dragoni, A.F. Secure Data and Voice Transmission over GSM Voice Channel: Applications for Secure Communications. 2013 4th International Conference on Intelligent Systems Modelling & Simulation (ISMS). Pages: 230 – 233.

[7] Mulliner, C. Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones. International Conference on Availability, Reliability and Security, 2009. ARES '09. Pages: 695 – 700.

[8] Bose, A., Shin, K.G. On Mobile Viruses Exploiting Messaging and Bluetooth Services. Securecomm and Workshops, 2006. Pages: 1 – 10.

[9] He Zhu; Changcheng Huang; Yan, J. Vulnerability evaluation for securely offloading mobile apps in the cloud. IEEE 2nd International Conference on Cloud Networking (CloudNet), 2013. Pages: 108 – 116.

[10] Semenov, S.; Davydov, V.; Engalichev, S. Mathematical modelling of the spreading of software threats in computer network. International Conference on Modern Problems of Radio Engineering Telecommunications and Computer Science (TCSET), 2012.

[11] Ali, M.; Falcone, P.; Sjoberg, J. Model-based threat assessment in semi-autonomous vehicles with model parameter uncertainties. 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), 2011. Pages: 6822 – 6827.

[12] Macia-Fernandez, G.; Diaz-Verdejo, J.E.; Garcia-Teodoro, P. Mathematical Model for Low-Rate DoS Attacks Against Application Servers. IEEE Transactions on Information Forensics and Security, 2009 (Volume: 4, Issue: 3). Pages: 519 – 529.

[13] D.M. Mikhaylov, A.S. Smirnov, A.M. Tolstaya, N.V. Kuznetsov. Using of bugs to perform attacks on mobile devices. Abstracts of the 10th Kurchatov Youth Scientific School 2012. Moscow, 2012. 278 p. Pages 134.

[14] Mikhaylov D.M., Starikovskiy A.V., Zuykov A.V., Tolstaya A.M. Data analysis system and detection of changes in the level of data security in wireless networks. Journal «Specialized machinery and communication» №5 2013. Moscow 2013. Pages: 42-44.

[15] Klaas Apostol. Brute-force Attack. SaluPress; 2012. 64 p.

[16] Lars R. Knudsen, Matthew J. B. Robshaw. The Block Cipher Companion; 2011. Pages 95-108.

[17] Dictionaries and lists of passwords. Electronic resource uinC Team, 2007. URL: http://www.uinc.ru/forum/faqs/wordlist.shtml.

[18] Whitman,Michael. Chapter 2: The Need for Security". Principles of Information Security, Fourth Edition. Boston, Mass: Course Technology; 2012. p. 53.

[19] David Elliott Bell. Looking Back at the Bell-La Padula Model. Proceedings of the 21st Annual Computer Security Applications Conference. 2005. Pages: 337–351.

[20] Gottumukkala, V.P.V.; Pandit, V.; Hailong Li; Agrawal, D.P. Base-station Location Anonymity and Security Technique (BLAST) for Wireless Sensor Networks. IEEE International Conference on Communications (ICC), 2012. Pages: 6705 – 6709.

[21] Zhukov Igor, Mikhaylov Dmitry, Froimson M.I., Kharkov S.M., Rubin D.T. Algorithm for detection of untrusted mobile base station. Journal «Specialized machinery and communication» №5 2013. Moscow 2013. Pages: 45-48.

[22] Ivanov Pavel. Mobile phones` bugs and mobile security. Information Security, №6, 2012. Pages: 30-31.