

S. Atanov¹, Y. Seitkulov¹, G. Balbayev¹, S. Zhuzbayev¹, G. Tulesheva²

¹L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

²Satbayev University, Almaty, Kazakhstan

E-mail: yerzhan.seitkulov@gmail.com

MATHEMATICAL MODELS OF SECURITY ATTACKS ON MOBILE CELLULAR SYSTEMS

Abstract. The need to protect smartphones and mobile devices from attacks on their internal resources is due to their multiple growth in number, as well as their share among gadgets with Internet access. The paper aims to analyze and create mathematical models of the most common types of attacks on mobile devices. Based on the constructed models and their analysis, ways are proposed to prevent and neutralize intrusions into the operating system of smartphones and other mobile gadgets. Methods: applied analysis using elements of probability theory and mathematical modeling. Results: the features of the mechanisms for the formation of vulnerabilities in mobile devices are determined. Important aspects of determining the effectiveness of modern technologies for protection against cyber attacks on mobile devices are identified. A brief review of the main approaches to mathematical modeling of typical attacks on mobile networks is given. Requirements for the effective choice of protection methods depending on the type of attack class are formulated. Basic recommendations for ensuring the security of a mobile device are formulated. Methods are proposed to reduce the probability of hacking the system through the most common and typical attacks.

Keywords. Smartphones, information security, brute force attacks, exploit programs, software and hardware backdoors.

Introduction.

One of the main trends in the digital economy is the increase in the share of cellular push-button phones and smartphones in relation to personal computers. In terms of relative productivity growth, smartphones outperform computers. According to the consulting agency Gartner, in the second quarter of 2022, global shipments of smartphones reached 352 million units, while shipments of personal computers for the same period amount to about 30 million units. The growing trend in the supply of smartphones is also noted by the International Data Corporation, predicting growth in 2023 at the level of ten percent.

A smartphone, like a personal computer (PC), runs an operating system (OS). And the structure of this OS is similar in principle to the common OS for personal computers. At the same time, smartphones store and process operationally significant data, which in the work refers to data that is valuable to the owner for a certain time, after which their importance can be neglected.

Modern research suggests that every year the number of cyber-attacks on mobile devices, which include smartphones, is increasing [1-3]. The choice of effective protection against such attacks directly depends on the understanding of what methods, software and hardware were used in the attack [4-10].

When developing agent to prevent attacks on mobile devices, one should rely on mathematical models of the most common attacks.

Materials and methods.

Here are some types of common attacks according to Check Point Software's Mobile Security Report 2021. The attacks discussed and analyzed below are basic. By basic attacks, we mean those attacks to which all possible attacks on mobile devices are brought.

Basic attacks are:

1. Attacks using the brute force method;
2. Attacks using malware exploits;
3. Attacks using additional equipment;
4. Attacks using software and hardware backdoors.

Let's consider these attacks taking into account the specifics of cellular communications.

Attacks using the brute force method

This type of attack is based on a simple enumeration of all characters using various algorithms and is the most common and simple method of obtaining unauthorized access to data. Typically, cell phone security includes username/password authentication. Almost any attack (the exceptions are software and hardware backdoors) sooner or later stops at the level of the authentication system (whether it is a Wi-Fi authentication system or built-in authentication in the OS when obtaining privileges). A brute-force attack occurs when an attempt is made to gain unauthorized access to both subscriber cellular devices and infrastructure elements of cellular mobile communication systems (CMCS).

As a rule, this method of guessing a password by brute force allows you to gain access in 100% of cases, but the duration of the attack is determined by the total number of combinations and time. And this can take considerable time even with a small password length of 5-10 characters, which will be shown below.

Results and Discussion.

Considering the passwords to be equally probable, it is possible to compose an attacking function $f_p(t, X)$, which is based on the method of guessing passwords for software of size X .

We use models from probability theory, knowing the symbols and keyboard layout of cell phones. Let's introduce the concept of $f_p(t, X)$ – a function whose value is equal to the probability that the password will be guessed in time t .

$$f_{\Pi}(t, X) = \frac{v}{N_1} * t, \quad t \in \left[0; \frac{N_1}{v} \right], \quad (1)$$

where N_1 is the total number of combinations, v is the speed of checking combinations.

Along with brute force, there are also applies dictionaries of the most frequently used passwords. These dictionaries are compiled on the most frequently used passwords based on statistical data and give an average efficiency of about 10-25% [10]. Taking the probability of finding the password in the dictionary as a variable, we get

$$f_p(t, X) = a * \frac{v}{N_2} * t, \quad t \in \left[0; \frac{N_2}{v} \right]. \quad (2)$$

Where N_2 is the number of passwords in the dictionary database.

Consider now the application of existing methods of protection against brute force attacks, those are the following solutions:

- organizational methods - creation of a unique password policy;
- software methods - the introduction of mandatory time intervals between attempts to enter the cell phone authentication system.

From the point of view the password-guessing probability distribution function makes the following corrections to the equation:

- password guessing speed v becomes a function of time (or a constant adjusted by system settings);

- there is a limit on the minimum password length N_1 ;
- applying a policy of regular password changes;
- a password strength check that eliminates the possibility of a dictionary attack, since a correctly implemented strength check mechanism also uses a dictionary lookup of a potential password.

Thus, in the general case, when organizational and technical measures are introduced to protect the authentication system from password guessing attacks, the only possibility remains to guess the password by brute force. Then the probability distribution function takes the following form:

$$f_p(t, X) = \frac{v(t)}{N_1} * t, \quad t \in \left[0; \min\left(\frac{N_1}{v}; T_p\right) \right] \quad (3)$$

Where T_p is the mandatory password change period.

To test this attack model, a modern discrete graphics card model RTX 2070 and the 16-core Intel Core i9-12900K processor have been used, which made it possible to sort out passwords much faster than the central processor. The results are shown in Figure 1.

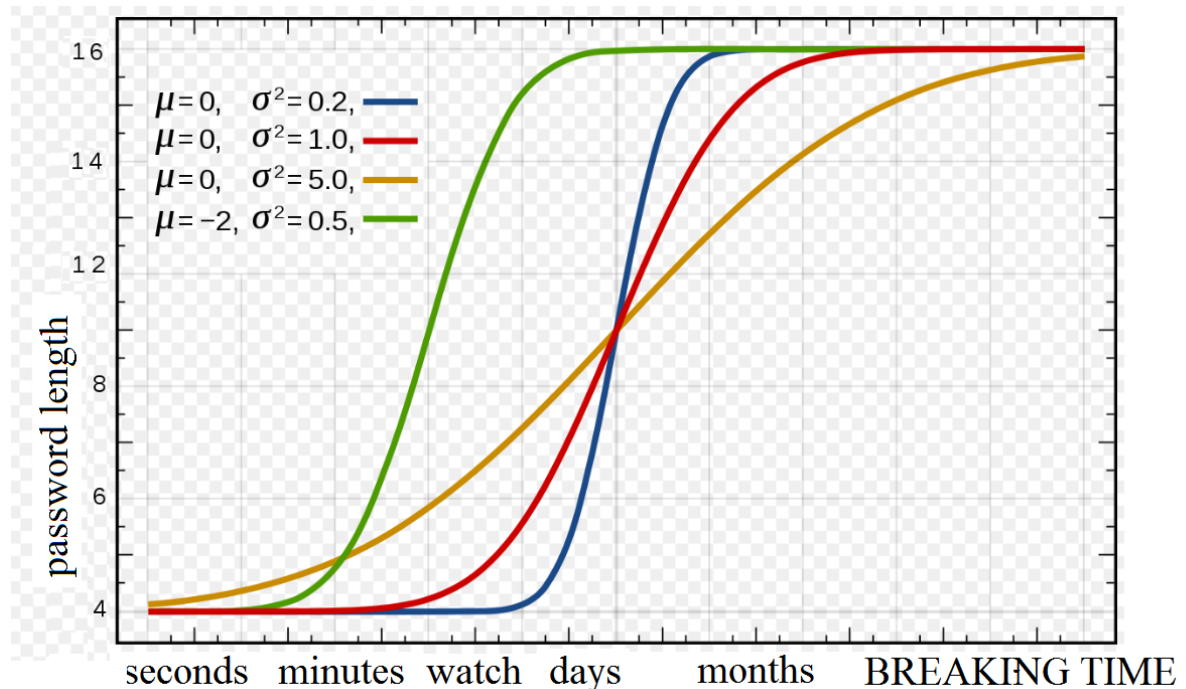


Figure 1 - Brute force attack

So if we calculate by this equation the time it takes to enumerate all numerical passwords up to 9 characters long ($S=3*10^6$, $N=10$ (numbers), $i=8$), we would get only 14 seconds. Thus, protecting a cell phone only in the speed dial mode practically does not provide full protection and can be used as a formal protection against children or accidental pressing, and the brute force limit mode can be easily removed by an attacker programmatically. Thus, the brute-force attack method is good either for a small number of characters in the set, or for passwords of small length (4-5 characters). However, it takes 490 days to search for all possible passwords, which can include 224 printable characters with a maximum length of only 6 characters, which is also clearly seen from the simulation data of distribution function according to equation 3.

Attack using malware exploits

Unauthorized access using exploit programs is by far the most popular type of attack on digital cellular systems.

Exploits are a subset of malware. They contain data or executable code that can exploit one or more vulnerabilities in a computer's software. Often, attackers use web pages to spread exploits, and they can also arrive through email messages. Some websites covertly and implicitly place malicious codes and exploits in their advertisements. Exploits are the only way to quickly gain remote code execution and privilege escalation, but exploits are mostly narrow-minded. And they are created only for certain types of operating systems of cell phones and smartphones and service software running within them. Figure 2 shows an example of how an exploit kit might try to use a device after visiting a compromised web page. For instance, exploits Angler is widely known for being able to detect antiviruses and virtual machines, and also uses encrypted files to make it difficult to investigate. The Nuclear Pack is no less dangerous, it infects Java and Adobe PDF with exploits, and later injects Caphaw, a dangerous well-known banking Trojan.

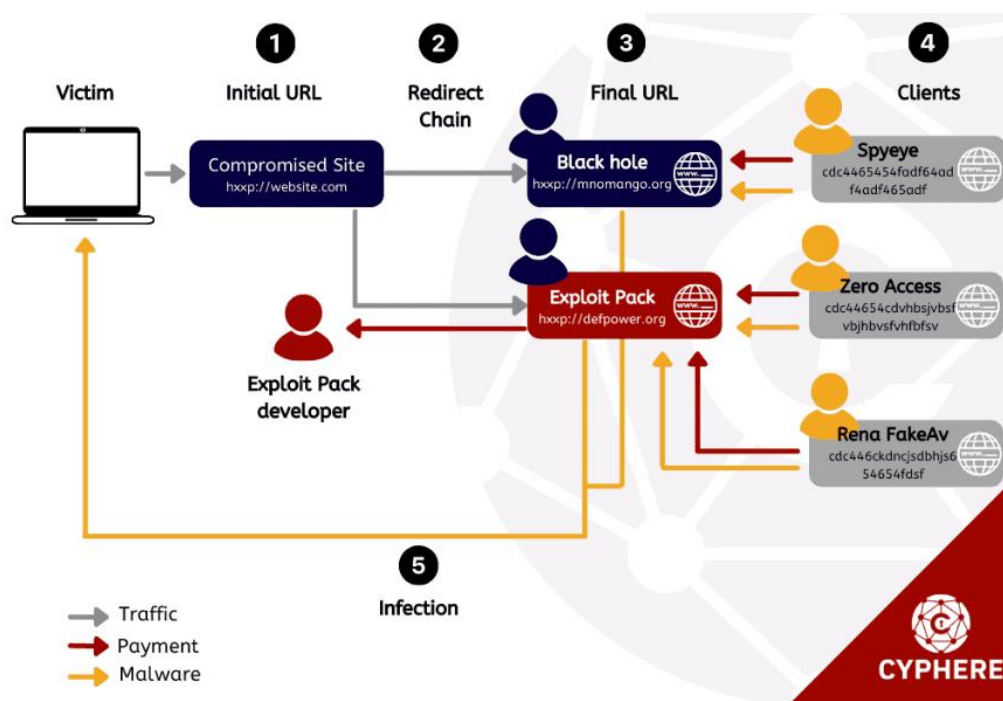


Figure 2 - General scheme of infecting user computers using exploits
Source: <https://thecyphere.com/blog/vulnerability-threat-exploits-relationship/>

Conducting a mathematical analysis of exploits aims not only to describe the current state in this sector of information security, but also to determine the trend since fundamental changes in the field of information security are not expected until the principles update of electronic computers operation.

The first exploits and the malware they download were created by lone hackers. Today, several groups of attackers are already working according to this scheme, and each has its own task: some create and sell exploit packs, others ensure that users come to the start pages of exploits like sheep to the slaughter (provide traffic). And finally, a group of professional attackers write malicious programs distributed during a drive-by attack. The most dangerous option for this is hacking the pages of legal sites and infecting them. At the same time, users visit by themselves a familiar site, and this is enough for a drive-by attack to start and the exploit pack to covertly and in a delayed mode begins its destructive work.

A complex algorithm of work forces us to apply the theory of modeling complex systems and set theory for modeling processes. The dynamics of the appearance and closing of vulnerabilities in software are determined by the following characteristics:

- all identified vulnerabilities to the next major update (i.e. update in the first or second digit of the version) and later OS become closed;
- the emergence of new vulnerabilities is almost entirely associated with the appearance of additional functionality;
- identification of end-to-end vulnerabilities (i.e. vulnerabilities that are valid for both the previous and the new version of the OS) can be considered negligible;
- detection of vulnerabilities using the patch-diffing method, when updated code is analyzed and assumptions are made about the vulnerabilities that it closes relative to older versions, allows the offender to detect the so-called first-day vulnerabilities that the developers themselves found and closed;
- the detection of zero-day vulnerabilities, as a rule, for each specific development is determined by the architecture of the solution, and varies slightly from version to version.

An analysis of existing attacks makes it possible to compile a mathematical model of the number of exploited vulnerabilities for a given version of the OS or service software. The number of identified vulnerabilities is considered as the cardinality of the set below.

$$E_v = K_0 \cup K_1, \quad (4)$$

where E_v is the set of vulnerabilities for a given version "V" of the operating system or software, K_0 is the set of zero-day vulnerabilities for this software, and K_1 is the set of first-day vulnerabilities for this software (Figure 3).

The susceptibility of a specific version of the OS or service software to day zero and day one vulnerabilities can also be assessed from the statistics of the corresponding vulnerabilities available on the network.

Knowing the number of exploited vulnerabilities, it is possible to compose an attack function for an attacker based on exploits, based on the following criteria:

- the exploit has a finite execution speed, depending on the specific type of exploit;
- the attacker uses a standard set of exploits, some of which are not applicable on this platform, which, according to the first point, leads to a loss of time during the attack.

Taking into account that $f_{\exists}(t, X)$ is a function, the value of which is equal to the probability that an exploit will be found in time t , then the attack function on element X , for which software exploitation is possible, in this case, it takes the following form:

$$\begin{cases} f_{\exists}(t, X) = 0 \text{ при } t \in \left[0, \sum_i T(\{M \setminus E_v\}_i) \cup T(\{M \cap E_v\}_0)\right] \\ f_{\exists}(t, X) = 1 \text{ при } t \geq \sum_i T(\{M \setminus E_v\}_i) \cup T(\{M \cap E_v\}_0) \end{cases}, \quad (5)$$

where M is the set of exploits owned by the attacker, T is the mapping of the set of exploits to the set of their corresponding execution times T , $\{M \setminus E_v\}_i$ - a set of exploits that attackers have, but which are not applicable to the system in question, $\{M \cap E_v\}_0$ is the set of exploits related to the system under consideration.

The very possibility of an attacker gaining unauthorized access through exploits can be estimated by knowing the version of the OS used by the user or installed in the cellular network infrastructure, as well as having a set M of the attacker's exploits. The possibility of a fraudster gaining unauthorized access exists when there is an intersection of many exploits of the offender and OS vulnerabilities.

We list the methods that, based on this mathematical model, can be used to reduce the likelihood of a system being damaged by attacks using exploits. This is first of all:

- the use of the latest versions of the software makes it possible to exclude from the list of exploits the vulnerabilities found through patch-diffing (i.e. first-day vulnerabilities);
- reducing the amount of service software, which also reduces the likelihood of a successful attack by exploits;
- a fundamentally different approach - the use of various data protection models directly within the system, assuming that an attacker has access to data.

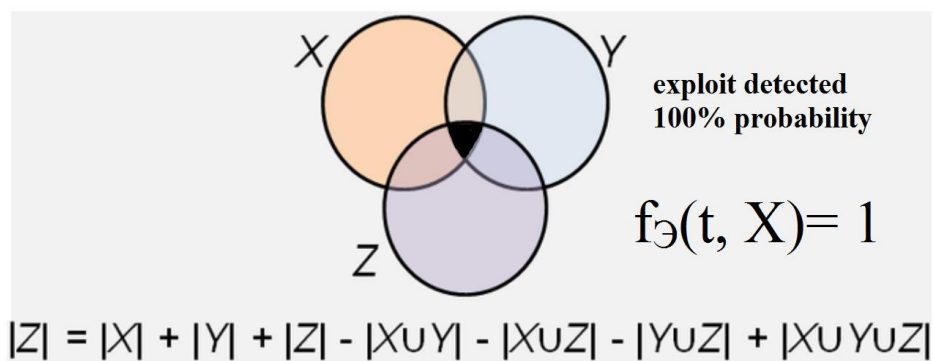


Figure 4 - Programmatic analysis of the Bell-LaPadula model for three sets

In the latter case, such a data protection model within the system is, for example, the Bell-LaPadula (BLP) model, also known as the mandatory data access model, the result of the program analysis is shown in Figure 4.

Attacks using additional equipment

Obtaining unauthorized access to data through the use of additional equipment, namely virtual cells, forcing the mobile device to switch from the base station of the cellular operator to a fake base station. This is a specialized attack that can only be carried out on mobile devices and requires special equipment.

During the attack, the attacker gains access to all data traffic that normally flows through the CMCS - voice data, packet data and short messages (including USSD messages that are normally considered secure and even used by ATMs to transfer sensitive data).

Since a virtual cell does not have the agent of actively influencing a mobile device, an attack through it belongs to the class of sniffing attacks. Thus, we can formulate the following recommendations for ensuring the security of a mobile device from the threat of an attacker gaining unauthorized access to data through a virtual cell:

- programmatic determination of the location of the phone in the virtual cell coverage area should determine the presence of listening equipment in the shortest possible time;
- the subscriber, who moves within small limits for a long time, is exposed to the greatest danger. For critical objects, virtual cell discovery must be performed by fixed means.

Attack models using software and hardware backdoors

The mathematical model of an intruder using software or hardware backdoors is quite simply implemented, taking into account the approaches proposed in the previous paragraphs.

Obviously, the presence of a backdoor allows an attacker in theory to have permanent access to the data stored or processed in the system. We will assume that the start time of the transfer of the data received as a result of the actions of the backdoor is negligible, just as the time of transfer of the data itself is short.

But at the same time, it is obvious that any backdoor has a so-called activation time, that is, the time from which the backdoor begins active data collection and transmission. This time should be singled out separately since it is the moment of activation of the backdoor that can be identified and be the reason for retaliatory measures on the part of the defending side. Let's denote this time as T . Then for this type of attack, the statement is possible:

$$f_7(t, X) = \begin{cases} 1, t \geq T_a \\ 0, t < T_a \end{cases} \quad (6)$$

where X is an element of the CMCS network, for which an attack using a backdoor can be relevant.

Thus, the main measures to ensure the protection of CMCS subscriber data should be the use of verified software. Moreover, it must be guaranteed not to have backdoors. This does not exclude the need to have service software and hardware capable of detecting the activation or the fact of unauthorized data transfer.

Having considered the list of basic attacks on mobile devices, we can say that mathematical modeling methods allow us to systematize the approach to classifying attacks. The use of the above approaches and models will allow targeted selection of effective methods of protection against such attacks.

Conclusion

Mathematical modeling and formalization of the most common attacks on mobile devices lay the foundation for the development of attack protection methods. An analysis of the architecture of existing attacks and existing protection methods allows us to suggest the feasibility of developing and using a number of technical solutions, namely:

- the use of a virtual secure communications operator (MVNO - Mobile virtual network operator), which allows you to switch to trusted equipment and protect data transmission channels;
- the use of special tools (scanners) to detect virtual cells in the radio channel;
- use only trusted OS for mobile devices;
- In addition, it is proposed that it is advisable to modify existing technical protection solutions in terms of adding to them:
 - method of protecting the hardware platform for mobile devices using a specialized hardware filter;
 - new technical solutions to ensure anti-virus protection.

By doing the above, the basic principles of preventing and neutralizing intrusions into the system of mobile devices can be formed.

Acknowledgments.

The Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Program No. fund this research BR18574045). Also many thanks to Dr. Mussiraliyeva Zhynar, Professor of the Al-Farabi Kazakh National University, for technical support (typing, searching analytical information on the Internet, literature review).

REFERENCES

- [1] Bazhenov S.V., Korovin S.D., Sukhov A.V., Makeev V.I., Omsk, 2012. Problems of protection of modern means of communication / Omsk, Academy of Military Sciences, 2012. 104 p.

[2] SJ Alsunaidi and AM Almuhaideb, “Security Methods Against Potential Physical Attacks on Smartphones,” 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-6. DOI: 10.1109/CAIS.2019.8769458

[3] Egorova A.I., Borisenko P.S., Attacks through third-party channels on smartphones on the example of electromagnetic attacks and methods of countering them // Proceedings of the VII Congress of Young Scientists. St. Petersburg. 2018. pp. 45-47.

[4] Butakova N.G., Sitnikov T.A. Analysis of the causes of vulnerability of mobile applications and means of protection // REDS: Telecommunication devices and systems. 2016. Vol. 6. No. 4. pp. 534-537.

[5] Mikhailov D.M., Fesenko S.D., Zhukov I.Yu., Nasenkov I.G. The impact of embedded software bugs on the security of mobile phones // Problems of information security. Computer systems. 2015. No. 2. pp. 86-90.

[6] Mostovoy R.A., Levina A.B., Sleptsova D.M., Borisenko P.S. Side channel attacks on mobile phones. Bulletin of Computer and Information Technologies. 2019. No. 12 (186). pp. 46-53.

[7] Beltov A.G., Zhukov I.Yu., Mikhailov D.M., Starikovskiy A.V., Tolstaya A.M. Attacks on mobile phones using the automatic configuration mechanism. Security of Information Technologies. 2012. Vol. 19. No. 2S. pp. 22-25.

[8] Rapetov A.M., Shishin O.I., Aristov M.S., Kholyavin V.B., Savchuk A.V., Zhorin F.V. Methods for obtaining access to data stored on a mobile device and processed by it // Special equipment and communication. 2014. No. 1. pp. 7-13.

[9] R. Spreitzer, V. Moonsamy, T. Korak and S. Mangard, “Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices,” in IEEE Communications Surveys & Tutorials, vol. 20, No.1, pp. 465-488, Firstquarter 2018.

[10] J. Jose, T.T. Tomy, V. Karunakaran, Anjali Krishna V, A. Varkey and Nisha C.A., “Securing passwords from dictionary attack with character-tree,” 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 2301-2307. DOI: 10.1109/WiSPNET.2016.7566553

Сабыржан Атанов, т.ғ.д., профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, atanov5@mail.ru

Ержан Сейткулов, ф.-м.ғ.к., профессор, Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан, yerzhan.seitkulov@gmail.com

Ғани Балбаев, PhD, ассоциированный профессор, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Казахстан, gani_b@mail.ru

Серік Жузбаев, PhD, профессор, Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

Гүлнар Тулешева, PhD, қауымдастырылған профессор, Satbayev University, Алматы, Қазақстан, tulesheva.gulnara@mail.ru

ҰЯЛЫ БАЙЛАНЫС ЖҮЙЕЛЕРІНЕ ҚАУІПСІЗДІК ШАБУЫЛДАРЫНЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕРІ

Аңдатпа. Смартфондар мен мобильді құрылғыларды олардың ішкі ресурстарына шабуыл жасаудан қорғау қажеттілігі олардың санының бірнеше есе өсуіне, сондай-ақ Интернетке қол жетімді гаджеттер арасындағы үлестеріне байланысты. Мақаланың мақсаты-мобильді құрылғыларға шабуылдың ең көп таралған түрлерінің математикалық модельдерін талдау және құру. Құрылған модельдер мен оларды талдау негізінде смартфондар мен басқа мобильді гаджеттердің операциялық жүйесіне кірудің алдын алу

және бейтараптандыру әдістері ұсынылған. Әдістері: Ықтималдық теориясы мен математикалық модельдеу элементтерін қолдана отырып қолданбалы талдау. Нәтижелер: мобильді құрылғыларда осалдықтарды қалыптастыру механизмдерінің ерекшеліктері анықталды. Мобильді құрылғылардағы кибершабуылдан қорғаудың заманауи технологияларының тиімділігін анықтаудың маңызды аспектілері анықталды. Ұялы желілерге типтік шабуылдарды математикалық модельдеудің негізгі тәсілдеріне қысқаша шолу жасалады. Шабуыл класының түріне байланысты қорғаныс әдістерін тиімді таңдауға қойылатын талаптар тұжырымдалған. Мобильді құрылғының қауіпсіздігін қамтамасыз ету бойынша негізгі ұсыныстар тұжырымдалған. Ең көп таралған және типтік шабуылдар арқылы жүйені бұзу ықтималдығын азайту әдістері ұсынылған.

Түйінді сөздер. Смартфондар, ақпараттық қауіпсіздік, шамадан тыс шабуылдар, эксплуатациялық бағдарламалар, бағдарламалық жасақтама және аппараттық артқы есіктер.

Сабыржан Атанов, д.т.н., профессор, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан, atanov5@mail.ru

Ержан Сейткулов, к.ф.-м.н., профессор, Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан, yerzhan.seitkulov@gmail.com

Гани Балбаев, PhD, қауымдастырылған профессор, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Қазақстан, gani_b@mail.ru

Серик Жузбаев, PhD, профессор, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан

Гульнара Тулешева, PhD, ассоциированный профессор, Satbayev University, Алматы, Казахстан, tulesheva.gulnara@mail.ru

МАТЕМАТИЧЕСКИЕ МОДЕЛИ АТАК НА МОБИЛЬНЫЕ СОТОВЫЕ СИСТЕМЫ

Аннотация. Необходимость защиты смартфонов и мобильных устройств от атак на их внутренние ресурсы обусловлена их многократным ростом числа, а также их долей среди гаджетов с доступом в Интернет. Целью статьи является анализ и создание математических моделей наиболее распространенных типов атак на мобильные устройства. На основе построенных моделей и их анализа предложены способы предотвращения и нейтрализации вторжений в операционную систему смартфонов и других мобильных гаджетов. Методы: прикладной анализ с использованием элементов теории вероятностей и математического моделирования. Результаты: определены особенности механизмов формирования уязвимостей в мобильных устройствах. Выявлены важные аспекты определения эффективности современных технологий защиты от кибератак на мобильные устройства. Дан краткий обзор основных подходов к математическому моделированию типичных атак на мобильные сети. Сформулированы требования к эффективному выбору методов защиты в зависимости от типа класса атаки. Сформулированы основные рекомендации по обеспечению безопасности мобильного устройства. Предложены методы снижения вероятности взлома системы с помощью наиболее распространенных и типичных атак.

Ключевые слова. Смартфоны, информационная безопасность, атаки методом перебора, программы-эксплойты, программные и аппаратные бэкдоры.
