Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies

Volodymyr Buriachok[1[0000-0002-4055-1494]], Dmytro Ageyev[2[0000-0002-2686-3854]], Oleksii Zhyltsov[1[0000-0002-7253-5990]], Pavlo Skladannyi[1[0000-0002-7775-6039]], and Volodymyr Sokolov[1[0000-0002-9349-7946]]

[1] Borys Grinchenko Kyiv University, Ukraine
[2] Kharkiv National University of Radio Electronics, Ukraine
p.skladannyi@kubg.edu.ua

Abstract. The article considers the methods that affect the operation of the intrusion detection system. Using the "disconnection task," a two-stage criterion for detecting anomalies in computer networks has been formed, which provides an analysis of network infrastructure characteristics and their identification with specific computer attacks and provides the ability to respond to possible attacks in real-time.

Keywords: Intrusion Detection Systems, Anomalies, Signature Analysis Method, Statistical Analysis Method, Neural Networks, Invasion Detection Model, Attack.

1 Introduction and Task Setting

Based on the annual rate of increase in the number of incidents in cyberspace, we can conclude that it is necessary to independently include in the integrated information security system critical infrastructure of automated means of detecting computer attacks and other dangerous divisions, including threats of man-made and natural (random) nature.

Modern Intrusion Detection Systems (IDS) to achieve information security goals constantly monitor the functioning of hardware and software platforms of the network infrastructure and record several quantitative and qualitative indicators of their work:

$$\{X_1(t), \ldots, X_N(t)\} \quad (1)$$

where t is the time at which the measurement of the indicator $X_k(t)$.

Such indicators, in particular in the NIDES system [1], are:

- Ability to use the CPU separately by the system and the user.
- Time to complete the process.
- Total amount of memory used during the execution of the process and its maximum size during execution.

- Number of open files at runtime; the number of page failures.
- Amount of information read from the disk.
- Number of I/O characters during application execution.
- Username changed during the execution of the application.
- Start time of the application.
- Number of signals received during the execution of the application.
- Application was running on the remote station and the name of this station
- Name of the application that was used on the remote station.
- Application was running on the local station and the name of this station, the name of the application used on the local station, etc.

2 Problem Formulation

With this in mind, this article aims to build a model of intrusion detection system that would detect network anomalies in real-time and with the least error, as well as find answers to the following questions [2]:

- What happened online?
- What was attacked and how dangerous is the attack?
- When and where did the attack start?
- Who is the malefactor?
- How and as a result of what there was the invasion?

Accordingly, the complexity of the attacking party's tasks to create cryptographic software tools for attacks is significantly simplified, and the effectiveness of solving problems of recovery (decryption) of cryptosystem data, which are encrypted with software tools for attacks, has an objective tendency to constant decline from year to year. At the same time, there are such groups of threats related to reliability [3–5]:

- Cryptographic primitive programming errors.
- Errors in the use of cryptographic primitives in crypto providers.
- Errors in transferring parameters to the crypto provider and returning processing results.
- Errors in the failure of the hardware platform.
- Accidental and intentional violations of the integrity of programs and data of crypto providers.

These factors may be prerequisites for the formation of hidden channels of leakage of information about the operation of cryptographic software tools for attacks. Consider two options for attacks on the implementation of software tools for attacks that do not involve the presence of critical information about their work.

3 Crypto Attack Mechanics

Premise 1. There is a certain cryptographic software tool for attacks (cryptosystem) with secret keys based on a stable block symmetric cryptographic algorithm, which provides encryption in output feedback (OFB) mode or otherwise tampering with feedback [6]. It is necessary: to build an attack on the implementation of the specified cryptosystem to ensure the possibility of partial or complete recovery of information (decryption).

This mode of operation of the crypto algorithm is widely used to build fully connected communication networks, in which each subscriber must send a message to any other subscriber of this network.

This mode is characterized by the presence of an initialization vector IV is random number, which provides at an acceptable level the probability of not overlapping the cipher in the case of using one key *K* for some time [6]. The idea of the attack on this cryptosystem is to implement a fictitious random data generator of the crypto algorithm, which is included instead of the real pseudorandom number generator, provides a hidden repetition of initialization vectors or keys. As a result, some messages will be encrypted in the same way:

$$\begin{cases} \widetilde{S}_1 = \widetilde{T}_1 + \widetilde{\Gamma}_j \\ \dots \quad \dots \quad \dots \\ \widetilde{S}_{m_j} = \widetilde{T}_{m_j} + \widetilde{\Gamma}_j \end{cases} \tag{2}$$

where $\tilde{T}_1, \dots, \tilde{T}_{m_j}$ are open messages; $\tilde{\Gamma}_j, j = \overline{0.2^k - 1}$ is a sequence of gamma characters formed from a single initialization vector and an algorithm key; $\tilde{S}_1, \dots, \tilde{S}_{m_j}$ are corresponding encrypted messages.

In this case, depending on the number of equally encrypted messages m_j and redundancy of the source texts of the messages, the corresponding encrypted messages can be partially or completely decrypted [7]. To repeat the initialization vectors IV the random bit generator should be used as follows:

$$IV = \langle \varphi(\alpha_1, \alpha_2, ..., \alpha_k) \rangle = \langle \beta_1, \beta_2, ..., \beta_b \rangle \tag{3}$$

where $\alpha_1, \alpha_2, \dots, \alpha_k$ is the sequence of random bits; $\varphi(\dots)$ some unambiguous function that expands the random sequence to a given size b; $\beta_1, \beta_2, \dots, \beta_b$ is coordinates of the initialization vector.

To solve the problem, we first calculate the allowable number of random bits to provide the required number of repetitions of equally encrypted messages. Let in the network *M* subscribers, each of whom sends on average daily $\overline{\mu}$ messages for each connection direction. With *T* is public key validity period (days). Then the average number of messages sent $\overline{N}$ is the value:

$$\overline{N} = \binom{M}{2} \cdot \overline{\mu} \cdot T \tag{4}$$

During the specified period, the average number of repetitions $\overline{R}$ each of 2^k the values of vectors of random bits $\langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle$ in the case of their even distribution will be:

$$\overline{R} = \frac{\overline{N}}{2^k} = \binom{M}{2} \cdot \overline{\mu} \cdot T \Big/ 2^k \quad . \tag{5}$$

Based on equation (5) we obtain an estimate of the allowable number of random bits:

$$k \le \left\lfloor \log_2 \binom{M}{2} \cdot \overline{\mu} \cdot T - \log_2 \overline{R} \right\rfloor \tag{6}$$

Using inequality (2) in each case of the attacked network, it is possible to calculate the allowable number of random bits to provide an average static number of $\overline{R}$ equally encrypted messages. Of course, random data used for cryptographic transformations are subject to statistical testing, but the length of the vector is quite small. IV (block length for most standard cryptographic algorithms is 64 or 128 bits) significantly limits the ability to apply statistical criteria. To check the uniformity of the distribution of sequences of this length, the criteria of frequencies of signs and bigram are mainly used [8], which puts forward the appropriate requirements for the expansion function. Therefore, it is clear that to ensure the equal occurrence of bigrams in the binary vector $\langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle$ appropriate value k choose a multiple of four (there are four options for bigram 00, 01, 10, 00).

For example, in the case of a special network that includes $M = 10$ subscribers with an average intensity of sending messages during the validity of one network key $\overline{\mu} \cdot T = 10$ to obtain the average number of repetitions of encryption $\overline{R} = 2$ it is necessary to have several random bits no more $k \le 7$.

To hide statistical dependencies in vector IV and obtain the required number of bits in the corresponding expression as a function φ, you should use a stable hash function, such as MD5, which is part of the standard set of Windows algorithms, or similar. Thus from 128 bits of the digest which we receive using a hash function, we will use the necessary quantity.

Premise 2. Suppose that there is a software tool for implementing attacks (cryptosystem), built on a stable symmetric block cryptographic encryption algorithm in OFB mode using public key distribution based on the El Gamal protocol [6]. The task is to organize an attack on the implementation of the cryptosystem in such a way as to ensure complete decryption.

Initially, the operation of the cryptosystem in the El Gamal protocol using a cyclic element g of some field and the secret key of the asymmetric algorithm x is formed public key y:

$$y = g^x \bmod p \tag{7}$$

where p is some large prime number, 1024 bits long.

To encrypt the session key of the symmetric algorithm, a random number k is generated, the value is calculated:

$$y_1 = g^k \bmod p. \tag{8}$$

and the secret key of the symmetric algorithm is encrypted K:

$$\delta = K \cdot y^k \bmod p. \tag{9}$$

Pair (δ, y_1) together with the encrypted message is transmitted to the owner of the secret key x, which is based on the obtained pair (δ, y_1) calculates the secret key of a symmetric algorithm K:

$$K = \delta \cdot y_1^{-x} \bmod p. \tag{10}$$

We organize an attack on the specified protocol by substituting a random number k with a pseudo-random one so that the testing system does not reveal this fact. Let $k \in \{\xi t., t=1,2,\ldots,\Psi\}$, at the same time power Ψ the set of valid values of the pseudo-random number k choose a fairly large, but less than the performance of a specialized computer system for the search of keys for a reasonable period.

Calculation of possible key variants K y in this case we carry out using International Planned Parenthood Federation (IPPF) proceeding from the equation (10) based on a set of admissible values of pseudorandom number $\{\xi_t\}$ [9].

As a result, it should be noted that access to information of the "true" random data generator and methods of its substitution in each case depends on the hardware and software platforms on which the IPPF, the peculiarities of its implementation, the presence of an automated system of protection against unauthorized interference. her work, etc. To create a fictitious random number generator, it is possible to use a sequence of Mersenne numbers $M_p = 2^p - 1$, if p is a simple number, M_p also simple.

4 Methods of Analysis

It is known that the efficiency of the IDS system significantly depends on the applied method of analysis of the original data. Currently, the following main methods are distinguished [1]:

1. Signature methods of analysis.
2. Statistical methods of analysis.
3. Hybrid methods of analysis with the function of self-learning.

4.1 Signature Method

Signature methods of analysis are based on the fact that most attacks and their scenarios are generally known. In this approach, the signatures of invasions determine the characteristics and conditions of the objects, the occurrence of events that are signs of attempted attacks (invasion), and their relationship. Of course, signature methods of

analysis use intrusion signature databases that are supported by the security system. In this case, the order (sequence) of actions performed or initiated by the user or information process (program) is compared with known signatures. A sign of an attempted security breach may be partial compliance of the sequence of events with the signature.

Anti-virus scanners that work with a database of virus signatures are typical representatives which implement this idea. Their advantage is a fairly high speed of analysis. The effectiveness of signature methods of IDS can be increased through the use of methods of artificial intelligence. The advantages of statistical methods of analysis in IDS include:

- No need for a large amount of memory to store controlled variables.
- Ease of detecting deviations in the data characterizing the behavior of users and processes.
- Ability to analyze quantitative and qualitative data of different nature of origin as a parameter in the analysis.
- Disadvantages of statistical methods include difficulties in generating statistics of the normal behavior of users and processes.

4.2 Hybrid Method

Hybrid methods of analysis with the function of self-learning include:

- Teaching methods for the classification of examples.
- Neural networks.
- Genetic algorithms.

To achieve the goal set in the work, it is advisable to use statistical methods exactly. This allows, using the well-known "problem of disorder" [10]: to form a two-stage criterion for the detection of anomalies in computer networks, to overcome the connection of statistical methods to the model of usual (normal) users' behavior.

Step 1. Let's suppose that two complex hypotheses are considered concerning the random sequence $X = \{x_t, x_t \in R,\ t = \overline{1,N}\}$ under analysis: H_0: the sequence X is stationary with a single probability distribution function, H_1: the sequence X is a concatenation (the result of "gluing") of two stationary random sequences with different distribution functions:

$$X = X_1 || X_2, \tag{11}$$

where $X_1 = \{x_t, t = \overline{1,n^*}\}$, $X_2 = \{x_t, t = \overline{n^*+1,N}\}$, $n^* = [\theta N]$, $0 < \theta < 1$

It is necessary to estimate the point of "gluing" n*. It is believed that the sequences X_1 and X_2 differ in one of the two-dimensional distribution functions, namely, the probability distribution of the vector (x_t, x_{t+2}):

$$F(u_0, u_1) = P\{x_t \le u_0, x_{t+2} \le u_1\} \tag{12}$$

to the moment $t_1^* = n^* - 2$ including is equal to $F_1(u)$, and at $t \geq t_2^* = n^* + 1$ is equal to $F_2(u)$, and

$$||F_1(u) - F_2(u)|| \geq \varepsilon > 0, \tag{13}$$

where ||…|| is normal sup-norm.

It is known that the distribution function of a finite-dimensional random vector can be approximated uniformly with any accuracy to the probability distribution function of a random vector with a finite number of values. It follows that if we give the set R is a combination of a sufficiently large number of domains $\{Aj,\ j = \overline{1,r}\}$, that do not intersect $A_i \cap A_j = \emptyset$ for i ≠ j, then the vector (x_t, x_{t+2}) can be approximated by a distribution vector with a finite number of values [11].

Therefore, if we are to enter new random sequences

$$V_t^{ij} = I\left(x_t \in A_i, x_{t+2} \in A_j\right),\ \text{де } 1 \leq i \leq r, 1 \leq j \leq r, \tag{14}$$

where $I(A)$ is an indicator of the set A, then at least in one of them there is a change in mathematical expectation.

Therefore, if we use an algorithm that detects a change in mathematical expectation, the same algorithm will detect a change in the distribution function. This fact allowed the work to be limited to the development of only one, a basic algorithm that can detect changes in the mathematical expectation. To do this, to identify moments of "disorders" a family of statistics of the form is proposed:

$$Y_N(n, \delta) = \left[\frac{n}{N}\left(1 - \frac{n}{N}\right)\right]^{\delta} \cdot \left[\frac{1}{n}\sum_{k=1}^{n} x_k - \frac{1}{N-n}\sum_{k=n+1}^{N} x_k\right], \tag{15}$$

where $0 < \delta \leq 1,\ 1 \leq n \leq N-1,\ X = \{x_k,\ k = \overline{1,N}\}$ is the sequence under study.

The given family of statistics in the case of a fixed n is a generalized variant of Kolmogorov-Smirnov's statistics, which is used to test hypotheses of coincidence or difference of distribution functions in two samples. The paper also proves that the statistics in the case of $\delta = 1$ for $N \to \infty$ and maintaining the ratio between the volumes of "glued" implementations minimizes the maximum possible probability of error estimating the moment of "disorder" (minimax in order):

$$P\left\{\max_{1 \leq n \leq N-1} \sqrt{N}|Y_N(n,1)| > C^{(1)}\right\} \to$$

$$2\sum_{k=1}^{\infty}(-1)^{k+1} \exp\left(-2k^2\left(\frac{C^{(1)}}{\sigma_*}\right)^2\right) \equiv f(C^{(1)}), \tag{16}$$

where the parameter σ_* is the standard deviation, $C^{(1)}$ is the limit of the criterion, the excess of which will be perceived as the occurrence of "disorder," the value of n_*, for which it occurred, is the desired moment of "disorder."

Step 2. Having fixed the level of probability α "false alarm" about the disorder, during the statistical processing of real data we determine the level of the threshold of the first level $C^{(1)}$:

$$\alpha = f\left(C^{(1)}\sqrt{N}/\bar{\sigma}_*\right), \tag{17}$$

where $\bar{\sigma}_*$ is the estimate of the parameter σ_* (standard deviation), and N is the sample volume of the sequence under study [12].

In the case of hypothesis H_1 on the representation of the original sequence of measurements in the form of the concatenation of several stationary random sequences with different probability distribution functions, we apply the criterion of the allowable number of triggers ("disorders") *Z*. That is, we assume that the following equation takes place:

$$n_1 + n_2 + \ ... + n_Z = N, \text{де } 2 \le Z < N - 2. \tag{18}$$

For a small number of sequences, the Chebyshev inequality can be used to determine the boundary of the criterion if the random variable *Z* has a mathematical expectation μ and a standard deviation σ for a given $\varepsilon > 0$:

$$P\{|Z - \mu| \ge \varepsilon\} \le \frac{\sigma^2}{\varepsilon^2} \tag{19}$$

If *Z* is a random variable with a single-mode probability distribution with a mathematical expectation μ and a standard deviation of $0 < \sigma < \infty$, then for any $\lambda > \sqrt{8/3} \approx 1.63299$, there is a Vysochansky-Petunin inequality, which improves the estimation of the deviation probability:

$$P\{|Z - \mu| \ge \lambda\sigma\} \le \frac{4}{9\lambda^2} \tag{20}$$

In particular, for a typical deviation of 3σ (three sigmas), the significance level of the criterion is the probability of "false alarm" is calculated as [13]:

$$\alpha = \frac{4}{9\lambda^2} \approx 0.0494. \tag{21}$$

A more accurate result can be obtained for the case of a random variable *Z*, which is the sum of a sufficiently large number of independent random variables ($m \to \infty$):

$$Z = z_1 + z_2 + \ ... + z_m. \tag{22}$$

According to the integral limit theorem, the probability of deviation can be approximated by the normal probability distribution function $N(0,1)$:

$$P\left\{\left|\frac{Z-\mu}{\sigma}\right| \ge t_{1-\alpha}\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t_{1-\alpha}} \exp(-\frac{t^2}{2})dt. \tag{23}$$

Based on (12), we calculate the boundary of the second level criterion:

$$C^{(2)} = \mu + t_{1-\alpha}\sigma\ . \tag{24}$$

Thus, the algorithm for calculating the criterion includes the following steps (Fig. 1).

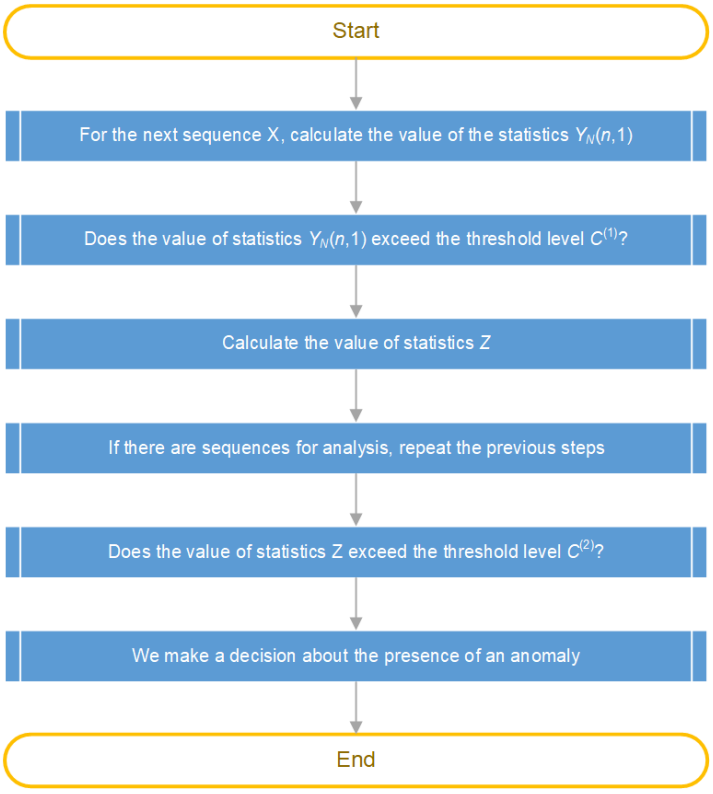

Fig. 1. Intrusion detection algorithm.

It is possible to see that the complexity of the algorithm that implements the proposed criterion is estimated by the value of $O(N)$. Thus, its implementation on the principle of the "sliding window" will not cause a significant load on the computer system.

The most difficult issue for the implementation of the method of detecting anomalies, as in other statistical methods, is the formation of regular behavior of the network infrastructure and its users.

5 Conclusions

In this regard, of particular interest are modern technologies that increase the efficiency of classical decryption methods [6], which using vulnerabilities in a particular cryptographic algorithm and/or protocol provide recovery of the secret key used to create encrypted messages, and/or disclosing the original value of the encrypted information. Thus recovery of the initial information can be full or partial therefore speak about full or partial decryption.

A two-level statistical criterion for detecting anomalies based on measurements of network infrastructure characteristics is proposed, which provides the possibility of

their further analysis to identify them with certain computer attacks. The application of the criterion does not require significant computing resources and provides an opportunity to respond to possible attacks in almost real-time.

References

1. Court, S. S.: Intruder Detection Methods (2004). [Publication in Ukrainian]
2. Kostrov, D.: Intrusion detection systems. Byte **8**(49): 14–21 (2002). [Publication in Russian]
3. Zubov, A. Y.: Cryptographic Methods of Information Protection. Perfect Ciphers (2005). [Publication in Russian]
4. Duhin, A. A.: Information theory (2007). [Publication in Russian]
5. Gorbenko, I. D., Gorbenko Y. I.: Applied Cryptology: Theory. Practice. Application (2012) Buriachok, V. L., Gulak, G. M., Horoshko, V. O.: On the issue of organizing and conducting intelligence in cyberspace. Sci. Def. **2**: 19–23 (2011). [Publication in Ukrainian]
6. Oliynikov, P., et al.: Principles of construction and main properties of the new national standard of block encryption of Ukraine. Inf. Prot. **17**(2): 142–157 (2015). [Publication in Ukrainian]
7. Kelsey, J., Schneier, B., Wagner, D., Hall, C.: Side channel cryptanalysis of product ciphers. 5th European Symposium on Research in Computer Security: 97–111 (1998)
8. Safety and Security Consultancy, https://www.ippf.org/about-us/jobs-and-opportunities/consultancy/safety-and-security-consultancy, last accessed 2020/05/11.
9. Lloyd, E., et al.: Reference Book on Applied Statistics. Vol. 2 (1990). [Publication in Russian]
10. Brodsky, B. E., Darkhovsky, B. S.: Non-Parametric Statistical Diagnosis: Problems and Methods (2000)
11. Shiryaev, A. N.: Probability. Vol. 1 (2007). [Publication in Russian]
12. Vysochansky, D. F., Petunin, Y. I.: Justification of the 3-sigma rule for unimodal distributions. Probab. Theor. Math. Stat. 21: 23–35 (1979)