computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

AUTHENTICATION OF PERSONAL COMPUTERS WITH UNSTABLE INTERNAL NOISE

Elena Nyemkova

Department of Information Technologies Security, Lviv Polytechnic National University
12 Bandera Street, Lviv, Ukraine, 79013, cyberlbi12@gmail.com

Paper history:
Received 17 May 2019
Received in revised form 31 May 2020
Accepted 8 July 2020
Available online 30 December 2020

Keywords:
cybersecurity;
authentication template;
personal computer;
internal electrical noise;
autocorrelation;
stability of signs;
form-factor.

Abstract: The article is devoted to the study of the stability authentication signs of personal computers; possibility of authentication follows from their physical differences as complex electronic devices. This approach provides the ability to remotely automatic authentication in real time. The authentication template was calculated from the sequence of values of the auto-correlation function of the internal electrical noise. It was demonstrated that the noise instability of noise leads to the error in the computer authentication. In order to reduce the error's probability, it was proposed to use the form-factor of autocorrelation function histogram for automatic sorting of noise files. The character of the noise instability had allowed the use of several authentication templates for one computer with instable noise. Each template was designed for the separate stability area. The probability of false authentication was reduced by using two authentication templates for one computer with instable noise, it was 30%. The recommendations were made about determining the priority of access to confidential information for computer with instable noise.

1. INTRODUCTION

1.1 FORMULATION OF THE PROBLEM

The authentication of personal computers based on the internal electric noise in the sound range is aimed at a remote real-time automatic procedure. This technique is promising for increasing the cybernetic security of computer networks, since it allows the authentication of personal computers by their physical differences. Noise is measured by an analogue-to-digital converter (ADC) of the integrated sound card of the personal computer (PC), measurement data are used to generate templates. Authentication by this technique is based on a comparison of templates and it is possible under the condition of noise stationery, which is not always performed in practice.

The stability of authentication signs is crucial for a technique based on measurements of internal electrical noise. The amplitude of such noise is very small, so external electromagnetic interference can completely change the statistical characteristics of the total noise signal. Also, internal electrical noise can be unstable, resulting in a failure to successfully computer authentication on the corporate network. The task is complicated by the fact that in both cases, the instability of the resulting noise is not revealed in any other way, only as a false negative authentication. Therefore, it is important to find a way to identify the presence of external interference or internal noise instability, and specific measurement data is not used in authentication template.

1.2 ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

The question of the noise stability of nonlinear electrical systems in time as an example of open systems with dissipation was considered in a number of theoretical works, including monographs of such authors as Ebeling [1], Nicolis and Prigogine [2], as well as Mehrotra [3]. It was shown that stationary states arise in nonlinear self-oscillating systems. The system may have several stable states. The transition of a system from one stable state to another is determined by the nature of the nonlinearity of the system.

The nature of the external interference, which is generated by consumers in the power grid, is described in detail in the monograph of Fink [4]. These interferences can be categorized as pulsed and monochromatic. Impulse interferences are very short and are characterized by a wide spectrum. Shortest impulse interferences less than 1 μs are considered the most dangerous for electronic devices. But such interferences will not affect the result of the sampling rate of 44.1 kHz, which is the noise digitization. Longer pulse interferences, for example, up to 10 ms, may also not significantly affect the noise measurements because the measurement lasts for several seconds. Monochromatic interferences represent electrical oscillations with a spectrum that consists of one or more narrow spectral lines. The effect of such interferences on the authentication result may be significant depending on the power of the interference and its suppression by the network frequency filter or the input frequency filter of the personal computer.

The last decade has been characterized by a heightened interest in the problem of authentication of electronic devices based on their physical differences [5-12]. It was proved as a result of experiments with various electronic devices, namely: with audio and video recording devices [5], with radiation measurement sensors [7, 9], laptops and personal computers [6], mobile phones [6, 8], and many other electronic devices [6, 10, 11]. The device can be authenticated by: the spectral-correlation characteristics of its internal electric noise [5, 7, 9, 10, 11], the spectrum of its own electromagnetic radiation [6], the vector variation of the signal constellation [8] and the instability of the frequency of the electrical network [12]. The method of determining the probability of correct authentication of an electronic device based on the stability of its template is proposed in the study [6]. In practice, the stability of authentication signs based on physical processes occurring in electronic devices does not imply a complete immutability of the authentication template. The small deviations in the device template between one-time templates and the average template are characterized by the threshold of authentication. Researchers pay great attention to the definition of values of the authentication threshold [5, 6].

The problem of the stability of signs of authentication is common for authentication by the physical differences of the object; similar questions arise in biometrics [13-15]. The problems of statistical stability and deviations from the classical distributions of real statistical data were studied in a number of papers [16-18].

Thus, the problem of the stability of authentication signs should be investigated within each authentication technology for specific operating conditions of electronic devices.

1.3 THE PURPOSE OF THE ARTICLE

The purpose of the article is to study the stability of template authentication, which is formed from the invariants of the autocorrelation function of internal electrical noise in the sound range of personal computers. The study aims at reducing the authentication error for stationary computers with unstable internal electrical noise.

2. MEASUREMENT METHODS

Measurement of internal electrical noise was performed using the ADC of the integrated sound card of the personal computer; the measurement technique is discussed in detail in [19]. Special software [20] allows writing to a file with a .wav extension a sequence of voltage samples, which down to the ADC input, with a sampling rate of 44.1 kHz. The measurements have shown that the noise of stationary computers in the sound range has amplitude of about 200 μV, the noise recording fragment is shown in Fig. 1.

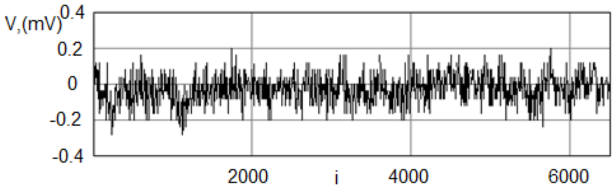


Figure 1 – Noise voltages at the input of the ADC of the stationary computer

The study of the statistical properties of the noise has shown that their amplitude has a Gaussian distribution, and the estimation of the Auto Correlation Function (ACF) of the noise for sufficiently long sequences became similar on ACF for the stationary process (sequences with the number of samples n = 88200 corresponding to the length of the recording 2 s). The following formulas were used to calculate the ACF

$$\begin{gathered} ACF_k = \frac{1}{\mathrm{var}(V)(n+1)}\sum_{i=1}^{n}(V_{k+i}-\bar{V})(V_i-\bar{V}), \\ \bar{V} = \frac{1}{n}\sum_{i=1}^{n}V_i, \qquad . \\ \mathrm{var}(V) = \frac{1}{n-1}\sum_{i=1}^{n}(V_i-\bar{V})^2 \end{gathered} \tag{1}$$

It was also found that the graphic view of the small-scale structure of the ACF practically does not change for different recording files and is unique for each computer, Fig. 2.

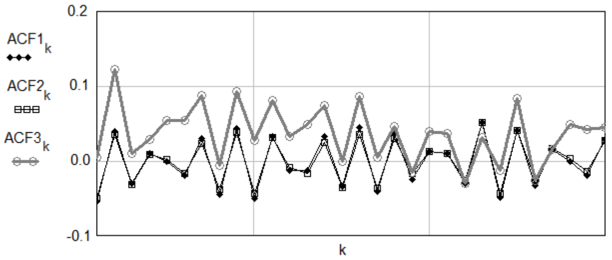


Figure 2 – ACFs (fragments) of the internal electrical noise of two personal computers: ACF1 and ACF2 are calculated from the data of two different recording files from one computer, ACF3 is calculated from the data of the recording file of another computer

This made it possible to enter an authentication template in the form of a bit string [21], the value of which is formed by the following rule

$$B_k = \begin{cases} 1, ACF_{k+1} \geq ACF_k \\ 0, ACF_{k+1} < ACF_k \end{cases}. \qquad (2)$$

By comparing bit templates that are calculated from data of two different recorded files, (i.e. file *I* and file *J*) it can be determined whether the received files are from one computer or from different computers and thus the computer authentication may be made. The Hamming distance is used as a measure of the distance between two bit templates B^I and B^J in this study

$$D = \sum_{i=1}^{N} B_i^I \oplus B_i^J . \qquad (3)$$

A preliminary study has shown that the length of the template in 1000 bits is sufficient for authentication. The typical deviation between the two templates for a single stationary computer is up to 30 bits in length 1000 bits or 3%. The deviation between two templates obtained from two different computers is, on average, more than 200 bits or 20%. These data were calculated for recorded files, which were created at different times, but the series of records were short. So, it is necessary to make a study of the templates' stability for longer series of records. The effects of statistical instability can manifest themselves on long observation intervals, as discussed in [16].

3. DISCUSSION OF RESULTS

Twelve personal computers of the same type were taken for the study of the stability of authentication characteristics by internal electrical noise. The average template has been calculated for each computer, based on the results of 70 series of measurements. The histogram of distances distribution between the one-time templates and the average template for a series of measurements of the typical computer is shown in Fig. 3. Similar results were obtained for eleven computers in the laboratory.

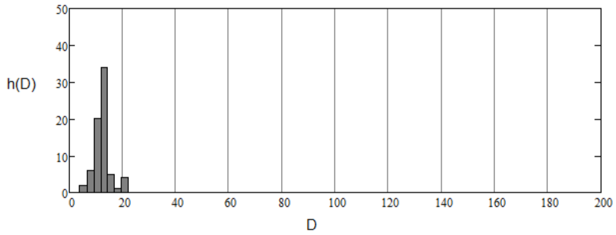


Figure 3 – Histogram of distances between the one-time templates of the computer № 3 and its average template

For a single computer №5 results are obtained that indicate the instability of its internal electrical noise. The distances between the one-time templates and the average template for this computer are shown in Fig. 4. The histogram of distances distribution between the one-time templates and the average template for this computer is shown in Fig. 5.

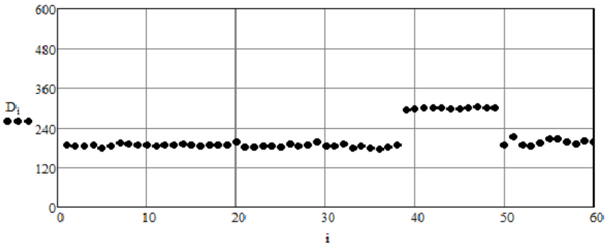


Figure 4 – Distances *D_i* between the one-time templates for record files with numbers *i* and its average template of the computer № 5

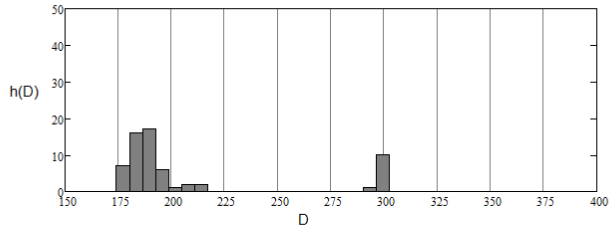


Figure 5 – Histogram of distances distribution between the one-time templates of the computer № 5 and its average template

There is a much larger distance between the one-time templates and the average template. For a computer with the instability of internal electrical noise, the histogram of distances distribution has two modes – the main mode and the lateral mode. The average distance value was 190 bits for the main mode. For lateral mode this distance is even greater – 300 bits. The width of the main mode of a histogram for a computer with instability significantly exceeds the width of the histogram for computers with stable noises.

Investigation of noise recording files from 39 to 49 inclusive for a computer with instability, (see Fig. 4), namely the analysis of their ACF, has shown that there is a monochromatic component in the noise, which significantly affects the structure of the average template. Its presence also explains the increase in the distance between the one-time templates and the average template for noise recording files 39-49.

Fig. 6 presents two noise ACFs for a computer with instability, one of which has a pronounced monochromatic character (the calculations gave a value of frequency 5.5 kHz) and corresponds to the data from file 39. The second ACF in small-scale structure has the character of the white noise ACF and corresponds to the data from file 2.

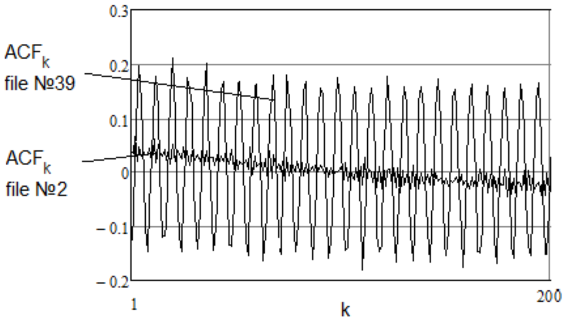
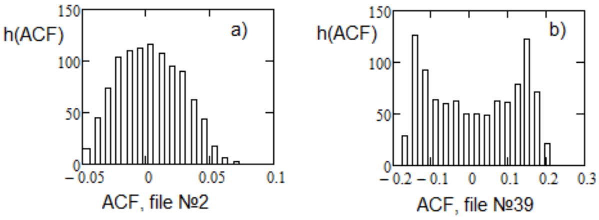


Figure 6 – Two noise's ACFs for a computer with instability for different recording files

The automatic detection of monochromatic interference can be provided by means of different forms of histograms of autocorrelation functions. The histogram of the autocorrelation function of the white noise has a convex form, Fig. 7a), while the histogram of the autocorrelation function of the sum of white noise and monochromatic noise has a concave form, Fig. 7b).



a) b)

Figure 7 – Histograms of ACFs for noise recording files from a computer with unstable noise: a) for white noise, b) for the sum of white noise and monochromatic interference

The area under the central third of the histogram for Fig. 7a) is larger than the area of both the right and left parts. Then, for the histogram of Fig. 7b), on the contrary, the area under the central part is smaller than the area of the lateral parts.

Differences in the form of histograms can be taken into account using the form-factor. To reduce the effect of possible asymmetry of the histogram, it was proposed to calculate the form-factor as the difference between the area under the middle part of the histogram and half the amount of total areas under the right and left end parts of the histogram. The form-factor should be normalized to the total area under the histogram.

This allows entering the form-factor as follows

$$FF = \frac{1}{2}\left(\frac{3\sum_{j=\Delta+1}^{2\Delta} h_j}{\sum_{j=1}^{3\Delta} h_j} - 1\right), \qquad (4)$$

$$\Delta = \left[\frac{1}{3}(n_{\max} - n_{\min})\right],$$

and n_{max} and n_{min} are respectively the maximum and minimum values in intervals of the data range ACF, which are made during the construction of the histogram. To determine the form factor, it is necessary to set the number of intervals to be three times. The form-factor of the histogram for ACF white noise will be a positive number, while the form-factor of the histogram for ACF of the sinusoidal influence will be a negative number. This will automatically exclude measurements that contain a monochromatic influence to calculate the template.

For the histograms shown in Fig. 7, the value of the form factor for the ACF white noise (FF_{wn}) and for the ACF of the sum of white noise and monochromatic influence (FF_{sin}) were respectively $FF_{wn} = 0.539$, $FF_{sin} = -0.32$.

Recording files for the computer with instability, for which the form factor was negative, was rejected, after which the average template was calculated again, as well as the distance from the one-time templates to the average template. It turned out that the graph of the distance had areas of stability. Each area of stability contains approximately 40 points (each point is calculated from data of the separate file), the total recording duration of each area is approximately 7 minutes. The authentication of the computer with instability can be done quite accurately if each area of stability is characterized by a separate average template.

An approach where more than one template could be attributed to the computer with instability is used in the authentication scheme to define the threshold. Next, the authentication results for computer № 5 with unstable noise and computer № 3 with stable noise are shown. The histogram of distances distribution between the one-time templates of computer № 3 and its average template, as well as histograms of distances distribution between the one-time templates of computer № 3 and the average templates of computer № 5, which are marked as 5 and 5A, are shown in Fig. 8. The 22-bit threshold allows for to correctly authenticating the computers with stable internal electrical noise by their average templates, which was confirmed for the computers under study №1-11 except for the №5.

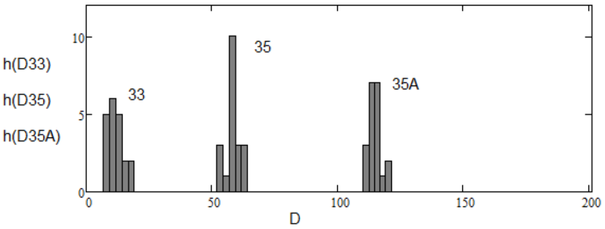


Figure 8 – Histograms of distances distribution between the one-time templates of the computer № 3 and average templates 3, 5, 5A

An attempt by a computer № 3 (and other computers with stable noise) to authenticate as a computer №5 will fail due to a significant excess of the authentication threshold.

Another situation arises when the computer №5 is being authenticated, Fig. 9. Instability noise of computer № 5 causes a fairly large spread of distances between one-time templates and average templates 5, 5A and 3, which leads to the possibility of authentication of computer № 5 as a computer № 3 with a certain probability.

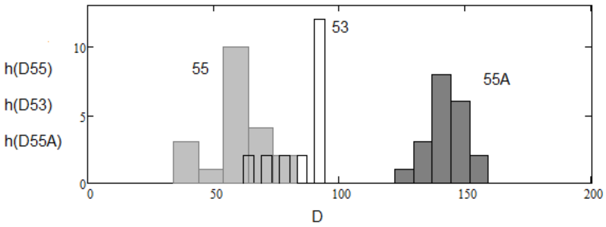


Figure 9 – Histogram of distances distribution between one-time templates of computer № 5 with unstable noise and average templates 3, 5, 5A

The probability of false authentication can be estimated as a percentage of the total area of histograms of distances distribution between templates, which for this research is 30%. An attempt by computer № 5 to authenticate as a computer number 3 in 30% of attempts will be successful.

If the security of the corporate network does not allow false positive authentication, computers with instability should be removed from such a network. In the presence of a hierarchy in access authority, a computer with instability can be used on the network, but its authority should have a higher level in relation to the authority for stable computers. In this case, the information leakage will not occur, even if the computer with instability will enter the system as another stable computer.

It should be noted that the instability of the internal electrical noise of personal computers significantly depends on the model of their performance.

4. CONCLUSIONS

The instability of internal electrical noise for individual PCs, which may be due to both external power supply interference and internal instability, results in a significant change in the authentication template. The consequence of this is the false authentication of the computer in the network.

The automatic verification of the recording file suitability for a template can be performed using the proposed form-factor. The form-factor is calculated from the recording file, its sign identifies data suitability for creating a template. The file with negative form-factor must be deleted. This avoids the negative effects of interference with a monochromatic interference, the presence of which cannot be fixed in another way.

It has been demonstrated that the destructive effect of the instability of internal electrical noise on the accuracy of authentication can be reduced by the introduction of several average templates for one computer. The calculation of templates should be made for areas of stability. Nevertheless, the probability of false-positive authentication remains. Before introducing the authentication system by internal electrical noise, all computers must be tested for the stability of the authentication features. An appropriate solution must be made for the computers which were detected as instability.

ACKNOWLEDGEMENTS

The author is grateful to Professor V. Maksymovich, Head of the Information Technology Security Department of the National University Lviv Polytechnic, for a number of valuable comments and Associate Professor of the Information Security Department Z. Shandra for discussion of the work.

5. REFERENCES

[1] W. Ebeling, *Formation of Structures in Irreversible Processes: Introduction to Theory of Dissipative Structures*, Computer Research Institute, Moscow, Izhevsk, 2004, 256 p., (in Russian).

[2] G. Nicolis, W. I. Prigogine, *Self-Organization in Nonequilibrium Systems*, Wiley-Interscience, New York, 1977, 512 p.

[3] A. Mehrotra, *Simulation and Modelling Techniques for Noise in Radio Frequency Integrated Circuits. PhD thesis*, University of California, Berkeley, 1999, 181 p.

[4] L.M. Fink, *Theory of the Transfer of Discrete Messages*, second ed., Soviet Radio, Moscow, 1970, 728 p., (in Russian).

[5] O.V. Rybalsky, V.I. Solovyov, V.V. Zhuravel, "The system of tools of examination of audio and videotape recording are in Ukraine," *Bulletin of Polotsk State University, Series C, Fundamental Sciences*, issue 4, pp. 15-19, 2018. (in Russian).

[6] C. Yang, A.P. Sample, *EM-ID: Tag-less Identification of Electrical Devices via Electro-magnetic Emissions*, 2016, [Online]. Available at: https://www.researchgate.net/publication/303885731_EM-ID_Tag-less_identification_of_electrical_devices_via_electromagnetic_emissions.

[7] J. Svoboda, M. Schanfein, *Apparatus, System, and Method for Sensor Authentication*, United States, Patent Application Publication, Pub. No.: US 2015/0006115 A1, 2015, 15 p.

[8] J. Hasse, T. Gloe, M. Beck, *Forensic Identification of GSM Mobile Phones*, 2013, [Online]. Available at: https://cryptome.org/2013/08/gsm-id.pdf

[9] B. Baker, J. Sanders, M. Schanfein, J. Svoboda, J. West, *Passive Noise Analysis Studies on Tampering Indication*, 2015, [Online]. Available at: https://www.osti.gov/servlets/purl/1360678

[10] N. Zhao, G. Dublon, N. Gillian, A. Dementyev, J. Paradiso, "EMI Spy: Harnessing electromagnetic interference for low-cost, rapid prototyping of proxemic interaction," *Proceedings of the 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, Cambridge, MA, USA, June 9-12, 2015, pp.1–6.

[11] G. Baldini, R. Giuliani, and G. Steri, "Physical Layer Authentication and Identification of Wireless Devices Using the Synchrosqueezing Transform," *Applied Sciences*, Vol. 8, Issue 11, pp.1–19, 2018.

[12] G. Hua, G. Bi, V.L.L. Thing, "On practical issues of electric network frequency based audio forensics," *IEEE Access*, Vol. 5, 2017, pp. 20640-20651.

[13] T. Pham, W. Ma, D. Tran, D.S. Tran, D. Phung, "A study on the stability of EEG signals for user authentication," *Proceedings of the 7th International IEEE/EMBS Conference on Neural Engineering (NER)*, Montpellier, France, April 22-24, 2015, pp. 122-125.

[14] J.N. Pato, L.I. Millett (Eds.), *Biometric Recognition: Challenges and Opportunities*, National Academies Press (US), Washington, 2010, 182 p.

[15] B.P. Rusyn, Ya.Yu. Warecki, *Biometric Authentication and Cryptographic Protection*, Lviv, Kolo, 2007, 287 p. (in Ukrainian).

[16] I.I. Gorban, "The phenomenon of statistical stability," *Technical Physics*, Vol. 84, Issue 3, pp.22-30, 2014 (in Russian).

[17] I.I. Gorban, *Theory of Hyper-Random Phenomena: Physical and Mathematical Foundations*, Naukova Dumka, Kiev, 2011, 320 p. (in Russian).

[18] A.I. Orlov, "Distributions of real statistical date are not normal," *Scientific Journal of Kuban State Agrarian University*, issue 117(03), pp. 1-20, 2016. (in Russian).

[19] E. Nyemkova, Z. Shandra, "Method of measurement of the identification parameters of sound recorder devices," *Bulletin of the National University "Lviv Polytechnic", series of Computer Systems and Networks*, issue 821, pp. 94-99, 2015. (in Ukrainian).

[20] O. Shmelyoff, *Oscillometer 7.30 – Multichannel Real-Time Spectrum Analyzer*, 2014, [Online]. Available at: http://soft-arhiv.com/load/47-1-0-95. (in Russian).

[21] E. Nyemkova, Z. Shandra, A. Klos-Witkowska, L. Wieclaw, *Network Electronic Devices Authentication by Internal Electrical Noise* in: Kh. Saeed, W. Homenda (Eds.), Computer Information Systems and Industrial Management, CISIM 2018, Lecture Notes in Computer Science, vol. 11127, Springer, Cham, 2018, pp. 474-485.

***Elena Nyemkova** has Doctor of Engineering Science, Associate Professor at the department of Information Technology Security, National University "Lviv Polytechnic", Ukraine. She graduated from the Special Faculty of Physics, Moscow Engineering Physics Institute (MEPhI), Moscow, Russia in 1984. She completed postgraduate studies in MEPhI in the specialty radiophysics, including quantum radiophysics in 1987 and then she defended the thesis in 1988. She is a co-author of the monograph and textbook. She has more than 60 scientific publications. The scientific and professional interests are focused on the fields of cybersecurity, authentication of electronic devices by internal electronic noise, the identification of complex systems by time series of observation variables.*