Яковина В., Чабанюк Я., Федасюк Д. Метод оцінювання та прогнозування надійності програмного забезпечення на основі моделі з динамічним показником величини проекту // Комп'ютинг, Т. 10 (2011), Вип. 2. – С. 97–107. 18. A.L. Goel A guidebook for software reliability assessment // Rep. RADCTR-83-176, Aug. 1983. 19. ГОСТ 27.002-89 Надежность в технике. Основные понятия. Термины и определения.

УДК 004.415

Elena Nyemkova
Lviv Institute of Banking the University of Banking of the NBU

DATA PROTECTION OF BIOMETRIC AUTHENTICATION FOR REMOTE ACCESS TO A BANK ACCOUNT

This article is devoted to the hash function that provides closure of biometrics in information networks for remote access to client account. There is proposed hash function which is described as a table of numbers. Verification of sustainability of cryptographic hash functions is performed. The session key for the hash is determined by the sequence of biometric data. The protocol of mutual authentication of a client and the server of payment system is given. The number of client's safe applications to ATM is estimated.

Key words: biometric template, mutual authentication protocol, transaction, unauthorized debiting, hash function.

ЗАХИСТ ДАНИХ ПРИ БІОМЕТРИЧНІЙ АВТЕНТИФІКАЦІЇ ПІД ЧАС ВІДДАЛЕНОГО ДОСТУПУ ДО БАНКІВСЬКОГО РАХУНКУ

Обґрунтовано вимоги до хеш-функції, яка забезпечує закриття біометричних даних в інформаційних мережах при віддаленому доступі клієнта до рахунку. Запропонована хеш-функція, яка описується у вигляді таблиці чисел. Наведено перевірку криптографічної стійкості хеш-функції. Сеансовий ключ для хеша визначається послідовністю біометричних даних. Запропоновано протокол взаємної автентифікації клієнта і сервера платіжної системи. Наведено оцінку кількості безпечних звернень клієнта до платіжної системи.

Ключові слова: біометричний шаблон, протокол взаємної автентифікації, трансакція, несанкціоноване списання коштів, хеш-функція.

Introduction

Biometric authentication in a computer network is one of the promising areas of information security. Biometric authentication is more secure than passwords and identity documents. It is also the only way to recognize fraud. Currently, biometric systems are not completely reliable in terms of recognition errors, as well as in terms of preservation and transmission of biometric templates online. These difficulties are a barrier to the widespread use of biometric systems in the real world.

Specialists consider two types of attacks in the context of biometric authentication [1–2]. They are forgery attack and data leakage from the database templates. Forgery attack can occur because currently there is no unambiguous method of matching fixed biometric data to their respective owners. Verification

of physiological characteristics or observation of random factors are proposed as a possible solution to this problem. Data leakage from the database templates, and its equivalent – unauthorized interception of data pattern in the network (mobile banking, internet banking) are situations when the information about the template of a legitimate user come to scam's notice.

The following requirements for the security of biometric template are considered. Firstly, physical fakes of biometric features cannot be restored from template data. Secondly, template protection scheme does not affect the result of biometric authentication systems. Thirdly, you can create a variety of templates from one biometrics to replace one of them in case of compromise. Nowadays biometric template protection is carried out through the transformation of biometric features and with the help of biometric cryptosytems. In the latter case protected template contains both a biometric template and the cryptographic key.

This work is devoted to the development of cryptographic biometric template protection method. It is suggested to use the findings in biometric ATMs. It is also possible to use them for authentication in mobile banking. The peculiarity of the suggested protection is the possibility of making a in a secured sketch of authentication information of ATM or mobile device through which customer's bank account is accessed.

Card accounts security is associated with three types of fraudulent transactions defined by ways of access and methods of operations. Ways of access include transactions via cash machines (ATM), payments via terminals in shops (POS) and mobile access to the account via internet banking (CNP).

Although in these three listed methods a client deals with a single object – his/ her own account, and gets access to his/ her account via the same authentication method – entering PIN and presenting card information, levels of fraudulent transactions both in absolute and relative terms for ATM, POS and CNP are significantly different. According to the European Central Bank [3-4] the level of fraudulent ATM transactions accounts for approximately one-sixth of the total number. Methods for identification and authentication of clients, provided they use ATM from year to year, remained virtually the same and the changes concerned the quality of plastic cards - the transition from magnetic stripe to chip. However, this was not a significant obstacle to fraudsters. Various innovations are constantly being tracked and more advanced ways of unauthorized debiting of card accounts are being created.

Requirements on hash function during client's biometric authentication

To date, the following trends determine the progress of protection against fraudulent transactions with card accounts: firstly, the transition to biometric authentication of a client and, secondly, a number of requirements [5] on authentication protocols. Biometric authentication provides a higher level of protection for client's account and therefore client's greater responsibility for what happens to his account. The latter allows to take the responsibility for unauthorized withdrawals from customer's account off banks and reduces banks' losses. That means that biometric authentication benefit both clients and banks. In the ATM sphere the switch to biometrics has already taken place: in Poland and Japan, the transition to biometric ATMs has begun (vascular pattern on client's palm is used). Private Bank has introduced voice authentication for smartphone owners using online banking [6].

There are a number of new requirements on authentication protocols during transactions. One of the main requirements is mutual authentication of a client and the side giving permission to access the card account. The second requirement is mandatory authentication of the device by means of which access is provided. The third one is mandatory encryption of information transferred over the network.

The volume of biometric data is significantly larger than the data for PIN and plastic card number. The size of the biometric data files depends on the type of biometrics. It can be from 256 bytes for fingerprints up to 70 kilobytes for blood vessels drawing hands. Therefore, the hash function, that is used to close information when it is transmitted via network, has to process fairly large amount of information efficiently. Thus, taking into account the class of information system security, a hash function must satisfy the following requirements:

to work effectively with fairly large amount of information (not less than 256 B);

to provide identification and authentication of a client;

to provide identification and authentication of the ATM via which the transaction takes place;

to provide mutual authentication of a customer and a processing center.

The process of identifying a client requires that PIN should be entered. With the advent of biometric ATMs the requirement to remember the sequence of PIN digits can be eliminated. For example, some biometric data positions can be assigned to determine the PIN. Thus, customers have to present their biometrics to ATM, from which data for identification is extracted, the rest of the biometric data is used for authentication. Due to the large volume of biometric data the definition of not one but several PINs for different banks can be provided. The role of plastic card then is reduced to the determination of the bank in which the customer's account is served. If the card is lost, the customer and the bank don't lose anything.

In turn, the hash function demands from data that purport to be biometric data is strictly constant. Real human biometrics may differ very significantly, in the case of iris or picture of the blood vessels. So, biometric templates should be used only those that provide their invariable for all samples of biometric identification.

Construction of hash function and the estimation of its parameters

As a rule, the hash function performs the conversion of semantic information using the session key. To work with biometrics it is proposed to use the sequence of client's biometric data as a session key, and to add the information about ATM, the date of transaction and the sequence of random numbers, known to both ATM and processing center (to enhance security). Semantic information is contained in a special table in which the process of mixing rows and columns is performed.

The original table is a square matrix of numbers that are not repeated. They may be the addresses of matrix cells. The first step is to prepare the table for initialization as a client hash function. To do this cell contents is reliably mixed using cyclic shifts of rows and columns. Four random numbers are generated. The first number determines what will shift: a row or a column. The second number specifies the number of a row or a column. The third number specifies the position at which the shift will start. The fourth number determines the shift direction: left or right for a row and up or down for a column. Applying this operation repeatedly, we obtain reliably mixed matrix. As a quality control of mixing the function of correlation between the original matrix and mixed one is side. Fig. 1 shows the correlation function between two matrices depending on the number of cycles of mixing. Matrix of size 16 by 16 is taken as initial, the number of matrix elements is 256.

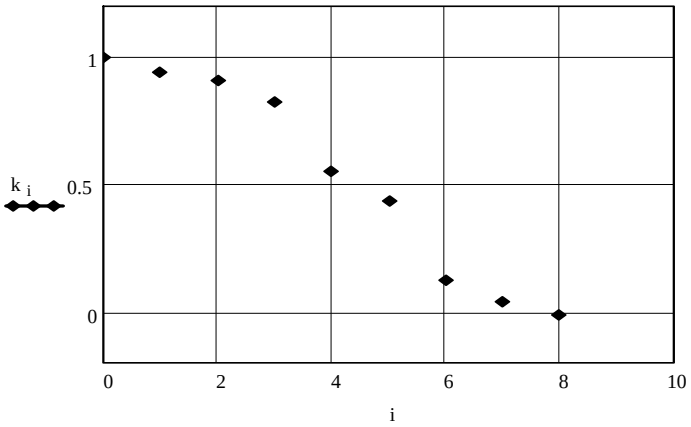

Fig. 1. Correlation between the original matrix and mixed. The number of mixing is 2 raised to the power of "i"

The number of cycles of mixing depends on the size of matrix, the larger the matrix, the greater the number of required cycles. From Figure 1 we can see that for sufficient level of mixing it is necessary to perform not less than 256 cycles, which coincides with the number of matrix elements.

The next operation was performed to test the quality mixed matrix. Sums of the numbers of all columns (similar rows) of the matrix were calculated. Sixteen sums were considered. Results for sums in columns before mixing are shown in Figure 2. Results for sums in columns after mixing are shown in Figure 3. The left side of Figure 2 shows a uniform increase in the values of sums V_i with increasing of the column number *i*. The average value of sums is equal 2040. The right side of Figure 2 shows a histogram of the distribution's density *h* of sums. Vector midpoints of intervals *int* put off along the abscissa.

Frequency of occurrence into the interval of values of sums *h* plotted along the ordinate axis. The analogous quantities are shown in Figure 3.

View of left graph in Figure 2 depends on the specific filling of the original matrix. In our case, the matrix is filled with decimal numbers from zero to 255 in a strictly ascendingly rows. The numbers from zero to 15 fill the first row, the number of 16 to 31 fill the second row, and so on. Therefore, the column sums uniformly slowly increase with the number of column. All sums get into a narrow range of values around the mean value in 2040.

The density of the distribution of sums has the form clearly defined dependence to the midpoints of the intervals. View of the histogram on the right side of Figure 2 depends on the number of partitions of the interval changes in sums. The number of partitions is equal to 7 in the histograms of Figures 2 and 3. Number of values of sums is equal to three for the first and last intervals on the right side of Figure 2. This number is two for the other intervals. Quantity sums in each interval depends on the number of these intervals. For example, exactly two sums are in each interval, if the number of partitions is equal to 8.

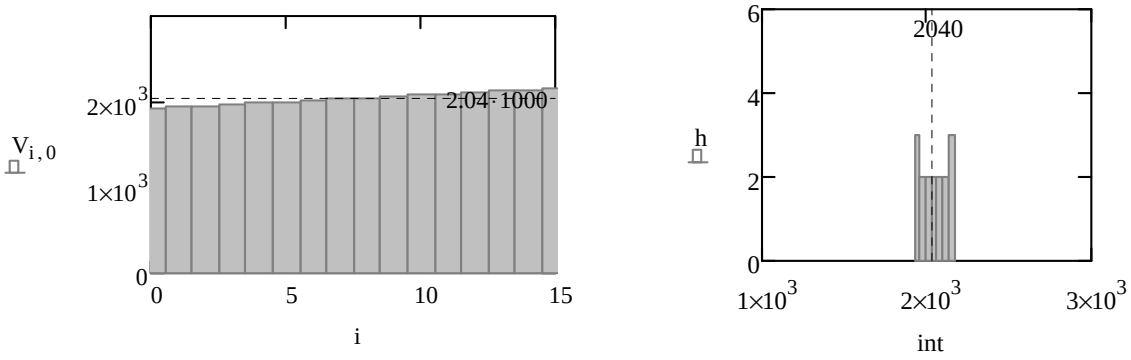

Fig. 2. Sums V of the columns of the matrix and the density distribution h of sums before mixing

As seen from comparison of Figure 2 and Figure 3, the nature of the change of sums changed significantly. It became chaotic. Period, in which sums fall into, broadened considerably (approximately 3.5 times). The shape of the histogram distribution density has the form of a random distribution. Maximum density distribution of sums corresponds to the 2040, form of the distribution is asymmetric. In appearance similar to the distribution of the Poisson distribution with a long left “tail”. Increasing the number of mixings of the original matrix does not change the form of the density distribution of sums. Maximum of the distribution falls on the average value of the sums and asymmetry persists.

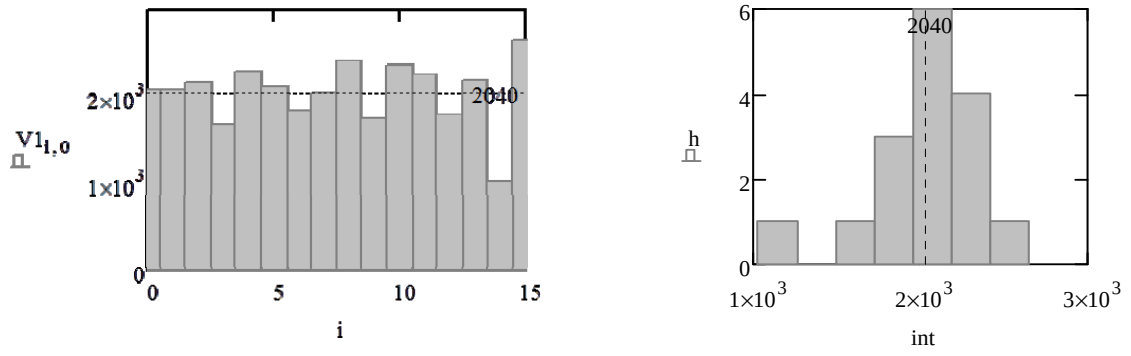

Fig. 3. Sums V1 the columns of the matrix and the density distribution h of sums after mixing

The results of these checks on the cryptographic security of hash functions do not depend on the type of properties, which is filled with the original matrix. For the matrix, the cells of which are recorded zeros or ones, the same results are obtain.

It should be noted that for the numerical simulations a random number generator is used, which is built into the processor MathCAD. For the practical application of the hash function there should be used a

random number generator, which uses noise processes in real physical devices. For example, a random number generator based on the computer sound card well suited for the application.

The second step of preparation is the introduction of user's information. The user enters his/ her identifying information: it can be passphrase, just a set of words, drawing sufficient number of lines, and finally – user's fingerprint. The entered information is transformed into a sequence of numbers that determine further mixing of matrix. Then hash function (matrix) is considered to be initialized and together with client's biometric data (reference data) is stored in bank's database.

Modeling of work of hash function is of interest to a large number of inputs to the client's bank account. The biometric template is modeled as a random number sequence required length. For this numerical experiment, four sequences of random numbers were generated. The first two sequences are random integers in the range from zero to fifteen; the latter two sequences are random integers in the range from zero to one. The length of all sequences is the same and is 256 numbers. Thus the length of the biometric template is 5120 bytes. The initialized matrix is mixed; the order of mixing is given by the generated sequences. Next, we investigate the correlation *Kor(n)* between the initialized matrix and the mixed matrix, depending on the number of mixings *n*. Also, number of coincidences *Eq(n)* of the numbers in cells of both matrices is studied. The result is shown in Figure 4.

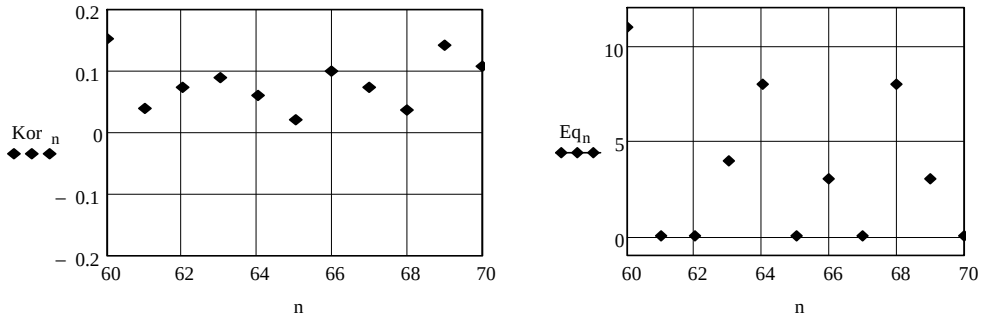

Fig. 4. Correlation function Kor(n) and number of coincidences Eq(n) (of the 256) for the consistent application of biometric template sequence to the hash function. There are achieved from 60 to 70 successive applications of biometric template

As shown in Figure 4, the magnitude of the correlation function is small. This suggests that the value of the sequence of hash functions continue to be random variables. Each client request to the payment system means changing the hash function once. It was established that multiple application of the same biometric template does not change the structure of the random nature of the hash function. The values of the correlation function between the initialized hash function and the hash after repeated applications of biometric template have been investigated for several ranges of the number of applications. All of them were insignificant. For example, Figure 5 shows similar calculations for a range of *n* in the region of 10,000. This corresponds to 10,000 client requests to the payment system.

It is of interest the value of the correlation function of two consecutive hash functions for a large number of customer requests to the payment system. The magnitude of the correlation between two successive hash functions turned be constant and equal -0.025, regardless of how many times a session key was used. Thus it can be concluded that a reliable mixing matrix in the first stage, as well as a sufficient length of the session key (biometric template size) allow to have a low level of correlation between the hash functions for various customer requests to his account.

Briefly mutual authentication protocol between client of bank and processing center can be described as follows. When the client uses ATM biometric data (real time data) is taken, from which identification data is extracted and together with the ATM's ID are sent into the processing center. In the center mixing of previous hash functions is performed according to the reference biometric data, ATM's data and the date of usage. At the same time the previous hash function is sent to the ATM, where the same transactions are performed, but customer's real time data is used as biometrics. Then the first half of the hash function is sent to the Processing Center, where it is compared with the same half of the center. When they coincide the second half of the hash

function is sent to the ATM and compared with the rest of ATM's hash function. When they coincide their mutual authentication is considered to be passed, the client is given access to the account.

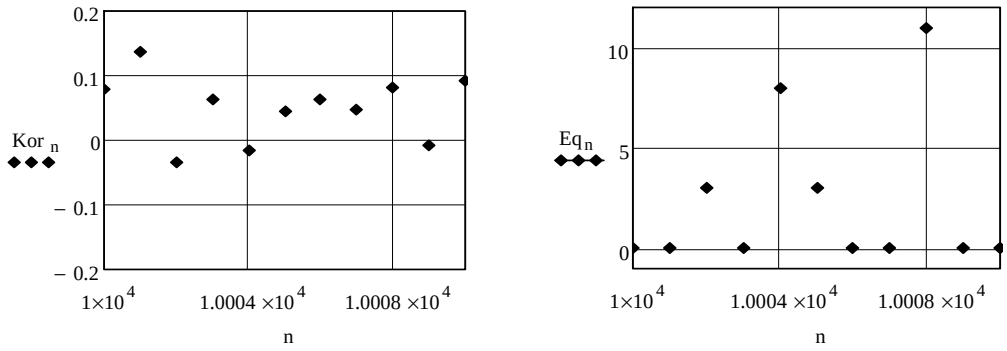

Fig. 5. Correlation function Kor(n) and number of coincidences Eq(n) (of the 256) for the consistent application of biometric template sequence to the hash function. There are achieved from 10000 to 10010 successive applications of biometric template

If a malicious user listens to the network, it may receive two consecutive hash function values. But from these data he cannot determine the order of the permutation, which provides a transition from the first to the second hash for real significant time. To do this, he would have to make $256!/256 \approx (256/e)^{256}\sqrt{(2\pi/256)} \approx 5{,}3 \cdot 10^{59}$ permutations. In addition, it should be noted that up to the biometric template should be added to the data of a particular device, with which the client communicates with the bank. This may be an ATM, POS terminal, mobile device. Therefore, each time the attacker faces the challenge of identity data across devices, which are also not transmitted in its direct form, and are included in the session key for the hash. Thus, the hash function provides almost unlimited number of secure requests to customer account.

Conclusions

Cryptographic protection of client's biometric template for mutual authentication should provide a basic set of measures of protection of information exchange of subjects and objects for K1 class of security. Cryptographic protection is the use of hash function, where in contrast to classical hashes the session key is client's biometric template as well as identification data of ATM or mobile device.

The hash function is described in the form of a table of numbers, the sequence of mixing is determined by the set of client's biometric data, the ATM's ID and the date of transaction. Numerical modeling is performed. The biometric template is constructed as a sequence of random numbers. The presented results of calculation of the correlation function give reason to believe the proposed scheme of generation of the hash function is resistant to brute force attacks Described protocol of strict mutual authentication guarantees the protection of a large number of client's applications to his/ her own account.

1. Mrunal Fatangare, Honwadkar K. N. A Biometric Solution to Cryptographic Key Management Problem using Iris based Fuzzy Vault / International Journal of Computer Applications (0975 – 8887) Volume 15– No.5, February 2011 – p.42 – 46.2. Standard ISO/IEC 24745:2011, Information technology – Security techniques – Biometric information protection. 3. Second report on card fraud Jule 2013 [electronic resource]: - Access: http://www.paymentscardsandmobile.com/wp-content/uploads/2013/08/ECB_Card-Fraud-Report-2013-07en.pdf - ISBN 978-92-899-1013-2 (online). 4. Third report on card fraud February 2014 [electronic resource]: – Access: http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf – ISBN 978-92 -899-1253-2 (online). 5. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах; [electronic resource]: – Access: http://pro-spo.ru/personal-data-security/4040-trebovaniya-o-zashhite-informaczii-ne-sostavlyayushhej-gosudarstvennuyu-tajnu-soderzhashhejsya-v-gosudarstvennyx-informaczionnyx -sistemax (online). 6. Privat service launched Sound Authorization User is privat24, 25/04 2014, [electronic resource]: Access: http://kbs-izdat.com/privatbank-zapustil-servis-zvukovoj-avtorizacii-polzovatelej-v-privat24/ (online).