ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIV INFORMATICS TECHNOLOGIES

UDC 621.391

Evseev S. P.[1], Tomashevskyy B. P.[2]

[1]Ph.D, Associate Professor of Information Systems Department of Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

[2]Ph.D, Leading Research Assistant, Senior Researcher of the Research Department of Missile Troops and Artillery of the Scientific Center of Land Forces, Kharkiv, Ukraine

TWO-FACTOR AUTHENTICATION METHODS THREATS ANALYSIS

The article considers basic methods of two-factor authentication system constructing on the basis of the use of cryptographic mechanisms to ensure the reliability, of formed authenticators, the risk of various methods of online attacks against a variety of two-factor authentication systems is estimated, as well as a system PassWindow is considered, which provides two-factor authentication on the unique ability of the matrix to transmit information in such a way that it is deciphered only to the imposition of the physical signs of the intended recipient pattern and barcode pattern obtained by digital network devices, resistance to the analysis is provided by a unique barcode card pattern generation as unique statistical images, a sequence of characters, or as more extended in an animated version.

The object of the research is the process of improving the integrity and authenticity of data packets in banking transactions security protocols on the basis of two-factor authentication methods. The subject of the study is methods and algorithms of integrity control and authenticity of data packets in banking transaction security protocols on the basis of two-factor authentication methods.

The aim of the paper is to increase the integrity and authenticity of data packets in banking transactions security protocols, a banking transaction, threat assessment on two-factor authentication methods. A comparative analysis of various systems with two-factor authentication PassWindow system in opposition to various Internet attack scenario is being carried out. An effective method for monitoring a practical two-factor authentication PassWindow system in its application to the banking system.

Keywords: two-factor authentication, online attacks, social engineering.

NOMENCLATURE

ID is an unique digital number of a user;

OTP is a password that is valid for only one login session or transaction, on a computer system or other digital device;

PIN is a numeric password shared between a user and a system, that can be used to authenticate the user to the system;

RSA is one of the first practicable public-key cryptosystems widely used for secure data transmission;

SMS is a text messaging service component of mobile communication systems.

INTRODUCTION

Existing authentication systems are based on a user submitting a static pair ID / password to the computer. However, in this case, the pair may have been compromised due to the negligence of users or the possibility for a fraud to guess passwords over [1–4]. Significant time intervals during which the password and the identifier are unchanged, allows applying various methods of interception and selection. To improve the security of a computer system administrators restrict the validity period of passwords, but in a typical case, this time limit is weeks and months, which is quite enough for an malefactor. A radical considers implementing two-factor authentication system, when the system asks a user to provide her with «what you know» (name and possibly a PIN-code), and «what you have» – any hardware identifier associated with the user [1, 2].

The purpose of the article is the investigation of the main methods for constructing two-factor authentication systems, risk analysis of different methods of online attacks against two-factor authentication systems based on the PassWindow system. A comparative analysis of the various two-factor authentication systems in opposition to various Internet attack scenarios is conducted.

1 PROBLEM STATEMENT

Currently, the Internet has become a primary method of communication of our modern life. It will undoubtedly be the main tool for the implementation of shopping and other financial operations. The appearance of these technologies has created a concomitant demand for authentication methods that are based not only on the traditional cryptographic methods (encryption, hashing, digital signature), but also on the methods based on usage of several factors to ensure the authenticity of the person

DOI 10.15588/1607-3274-2015-1-7

performing the financial transaction. Two-factor security system is based on the fact that a user in addition that one knows the password to access a specific user name («login») owns a tool for the corresponding access key. The latter can be an electronic security certificate stored on a computer or received on a personal phone SMS with a verification code or a fingerprint reader scanned by an electronic card reader device [1].

2 REVIEW OF THE LITERATURE

Strict (two-factor) authentication methods are most commonly used in the financial sector however may be used in almost any other field. The main methods of constructing two-factor authentication systems are given in Fig. 1 and can be classified as following [3].

1. Software to identify a specific PC. A special program is installed in a computer, which sets in it a cryptographic token. Then, the authentication process will involve two factors: the password and token embedded in the PC. As the marker is always stored on the computer, to logon the user only needs to enter login and password.

2. Biometrics. The use of biometrics as a secondary factor identification is carried out by identifying the physical characteristics of the person (fingerprint, iris, etc.).

3. Disposable e-mail- or SMS-password. Use of this password as a secondary identification factor is possible by sending second disposable password to one's registered e-mail address or mobile phone.

4. One-time password token. User is presented with the device that generates constantly changing passwords. It is these passwords which are entered by the user in addition to the usual passwords during the authentication process.

5. External control. This method assumes a call from the bank on a pre-registered phone number. The user must enter the password via the phone, and only after that he will get access to the system.

6. Identification using gadgets. This kind of identification is carried out by placing a cryptographic tag on any user's device (e.g. USB-drive, iPad, memory card, etc.). During registration, the user must connect the device to a PC.

7. Card with a scratch-off layer. The user is issued a card with PIN-code, which can be used only once.

The analysis has shown that in the banking systems tend to use two-factor authentication systems based on disposable e-mail- or SMS-passwords, and various types of tokens.

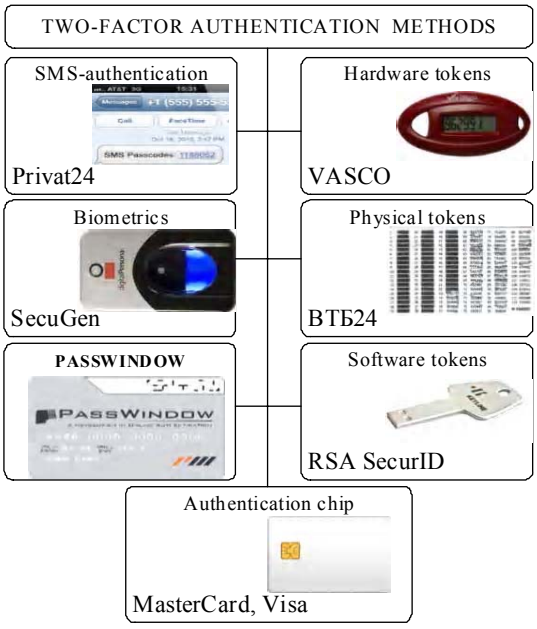

Figure 1 – Basic two-factor authentication systems

3 MATERIALS AND METHODS

Today several companies offer two-factor authentication systems based on the generation of OTP (One-Time Password – OTP), including RSA Security, VASCO Data Security and ActivIdentity.

To implement it the different types of OTP generators are used. OTP Generator is a standalone portable electronic device that can generate and display on a built-in LCD screen digital codes. For a generation of VASCO's Digipass devices one-time password generation mechanism is based on the cryptographic TripleDES conversion of data set consisting of 40 bits of the current time and the 24-bit data vector which are unique for every for each access identifier. The resulting conversion is visible on the display in the form of six or eight decimal digits is read visually and manually entered by the user as a password in response to the authentication application. Frequency of password change thus is 36 sec., so user receives truly a one-time password to login [4].

On the server part of computer system this password is compared with the password generated by the server itself by the same algorithm with the use of the current time on server clock and unique device data that is stored in a special database. In case of coincidence of passwords user is granted with access to the system. Fig. 2 shows the operation of the two-factor authentication systems of VASCO company.

Let concider the authentication based on PassWindow. PassWindow is a way to provide two-factor authentication in the online environment. It includes two matrix parts which are a physical key with a printed pattern on a plastic plate and a digital barcode template presented in the form of an image on an ordinary electronic display, such as a laptop or mobile device display. They generate a unique one-time password and a set of numbers for a particular transaction for a user, when they overlap each other. This password is then used for online authentication and transaction authentication. Information about a specific transaction is included in these figures, such as an account number or amount of the intended

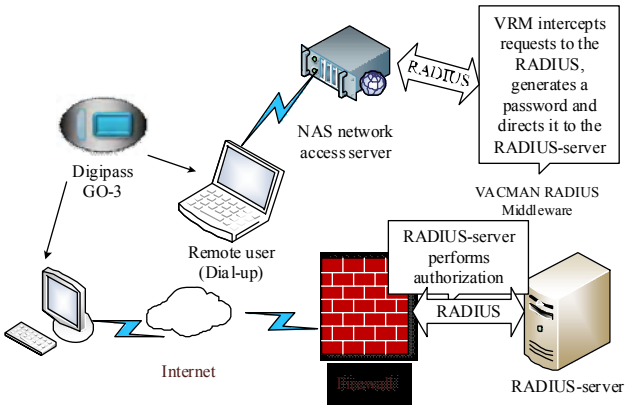

Figure 2 – The principle of operation of two-factor authentication systems of VASCO company

transaction that allows the user to visually confirm the authenticity of the received authentication request. These features make PassWindow one of the very few currently available authentication mechanisms, which provides a robust and accurate protection against the latest network security threats MITM (Man-In-The-Middle) attacks [4].

PassWindow technology is based on the unique ability of the matrix to transmit information so as that it stands only to the imposition of the physical signs pattern of the intended recipient (the user has this information already) after which the barcode template is displayed (challenge pattern) on the electronic network devices, such as computer, smartphone, etc. The combination of the key and the barcode template shows the encoded information only to a single user, moreover a full template preview is only possible from direct view. Any act of barcode interception via electronic devices means that leaked information will not be sufficient to let an attacker know the secret key of the user template during the whole activity term of the card.

Barcode PassWindow templates can exist as unique static images or a sequence of characters in the form of more extended animated version, which is the main topic of this paper. These animated barcodes consist of a sequence of static patterns, each of them contains the encoded characters or have no meaning and simply dynamically add an entropy to the entire pattern. Barcode patterns sequences are dynamically generated by the authentication server so that each of them is unique (and hence it has a sense) only when used together with the key to which it fits. Any interference or counterfeiting of a barcode template will be passively presented to the user in the form of appearance of combinations in a pattern that does not meet the expectations, for example, randomly placed segments that do not contain any characters, random numbers, missing or excessive numbers that appear within a template or performing the verification of data that does not refer to the active transaction.

Any alphanumeric code can be reliably transmitted using the PassWindow method, however the current implementation of the method is aimed at the transfer of short strings of random numbers for their use as a one-time password in conjunction with the figures which identify uniqueness of user authentication transaction. Once a user confirms that the unique information within a transaction encoded in the bar code corresponds to the desired, one can complete the transaction by entering the appropriate one-time password. The main stages of PassWindow are presented in Fig. 3.

Construction and safety profile of transaction authentication codes can be changed dynamically in order to meet a wide range of online authentication specific tasks.

Let concider the safety assessment of two-factor authentication systems.

Analysis of modern authentication systems showed that their security is measured by dividing the difference between the cost and benefits to the attacks on the value of the attacker's protection. So, expensive, though more secure methods, such as cryptographic PKI-units with their own secured communication channels of screens and keyboards are evaluated so low on the scale of security, whereas the banking system is still mainly based on the cheapest and apparently the least secure way of using PIN-codes and

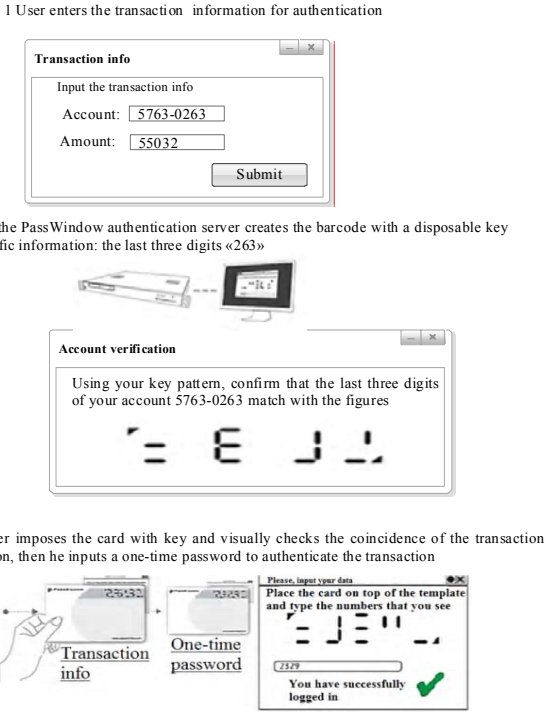

Figure 3 – The main stages of PassWindow

passwords. Total cost and complexity of deploying such devices often outweighs the benefit of their ultra-high security.

Network security threats can be classified into network attacks (information from a remote agent) and local attacks that originate from malicious software already installed on the client system, such as Trojans, rootkits, and so on. Frequently authentication safety assessments are primarily focused on network attacks assuming that the user terminal (i.e. tablet PC, laptop or mobile device) is a protected platform [11–14]. Nevertheless the attacker commonly gains full access to the victim's PC through hidden communication processes remaining from malware that use unpatched security holes in the licensed software.

The common attack methods are:

– compromised online databases – collected information stored in merchant databases is stolen;

– man in the middle / phishing – a third party intercepts and impersonates the client and server to the respective other to record and/or alter their communications;

– social engineering attacks – customers are deceived into revealing their private details to a hacker;

– man in the browser – malware is installed on the victim's computer to report network activity, keystrokes, and screen capture data to the attacker allowing interception during fund transfers in which funds can be unwittingly diverted by altering the information displayed in the user's browser;

– brute-force cracking of user passwords – the server is polled with every possible password combination;

– simple theft – authentication details written down or on a card can be physically taken and copied;

– shoulder surfing – an attacker can surreptitiously watch the user enter their transaction details.

4 EXPERIMENTS

The analysis of PassWindow security threats has shown that the most effective threat is analytic attack on the secret

key (card bar-code). To succeed the algorithm three to five monitoring sessions (OTP Bank transfer by client) have to be accomplished.

Plastic cards monitoring algorithm consists of the following steps.

1. Monitoring of the channel and receiving data by sessions.

2. Transfer data to the indicator class (as binary code), which can be operated as an object (indicator class represents the array of 7 ones / zeros).

3. Verification of the possibility to form «digits» in every position of the card (cycle by all sessions). Inside the cycle a new cycle for each sequence begins, in turn each indicator appears as «true» (we believe that it has a figure in itself).

Inside the cycle the verification is being conducted and if the current position is «true», then a version in which inverted generator indicator is written is being created and in case it is «wrong», position of the indicator is recorded. After each cycle within a single sequence the intersection of the previous versions of the sequence is executed and if all the sequences in the current session had been crossed then we release them, i.e. the end leaves (options) are reviewed and their copies are thrown out.

4. Review of all the sequences in all sessions. The intersection of letters between sessions serially (the first session from the second is a result from the intersection of the third session, etc.). After each intersection adjacent session leaves the leaves are «clean» from copies.

5. The intersection of all session letters among themselves. Cycle through all the letters so each option (leaf) is checked for input by generator data, if it has a conflict with some of the indicators then this letter (option) is discarded. As a result, there will be only one option which does not conflict with any of the sequences of all the sessions.

6. Displaying the final version of output.txt in binary formatted string.

Plastic PassWindow cards monitoring algorithm is shown in Fig. 4.

5 RESULTS

Designation SMS-systems or two-factor authentication based on mobile phones is a mistake, a more precise term is «out-of-band» authentication. Nevertheless with the spread of GSM, smartphones and tablets connected to the network, even this safety advantage may be lost if a user transaction authentication is performed on the mobile device itself. In addition, the growth of unwanted software for mobile devices now allows an attacker to gain access to the authentication codes sent via SMS, not only with the traditional interception by a malicious software [5], but also by intercepting and decrypting data sent over the GSM-network telecommunications [6]. Mobile devices authentication attacks are performed successfully even without such technologies. Instead, an attacker simply impersonating a user of the device, and requests all SMS messages to be sent to another phone number for the entire attack period [3]. Another authentication method uses the camera a mobile device to read the barcode image on the user's workstation, which is coded with the OTP information about the transaction. This method contains the mistake of assuming that the operating system on the user's mobile device is not exposed to such a vulnerability to malicious software, like all other forms of software working with the network [8].

In the case of biometric authentication user data are available for online authentication.

However, biometric authentication devices can not communicate from local devices or network without being confronted by malicious programs and / or «Man in the middle» attacks [9]. This method is also impossible to re-edit after the attacker has posed oneself as a user by using biometric authentication.

Biometric authentication provides a user-friendly way of generating online user name, but listening to the network and a compromised device, the overall safety performance of such methods is not better than when using normal user name and password.

Electronic hardware tokens come in several types and include various security authentication functions.

The most commonly hardware tokens generate one-time passwords (OTP) using cryptographic algorithms with an internal secret key, or, more often, the secret key is generated on the basis of common values of the synchronized system time. User reads the displayed numbers on a device and manually enters them into one's terminals to cross-reference with the authentication server.

This simple method of generating electronic OTP is vulnerable to attacks by an «intermediary» because users are obliged to disclose the OTP without the means of checking the authentication context.

In response, many token manufacturers have added a small digital keypad, significantly increased the token size, but allowing the user to enter information about specific transactions that have been encrypted with a secret key before the user inputs the result to one's terminal. This is a type of verification or signature of a transactions and it does provide some protection against «Man in the middle» attack.

Nevertheless, this method is still vulnerable to attacks using laborious manual process of a transaction signing. Time and attention necessary to perform a manual operation are successfully used to distract the user from the context of the transaction information that one accepts, and, consequently, attacks can be successfully committed on a massive scale [10–11].

Printed OTP lists / number grids. An older method of providing one-time password is printed lists of randomly generated passcodes or transaction authorization codes on a sheet of paper or a sketch-card. Each access code is requested in sequence and is used to authenticate a transaction.

Alternatively, printing the symbol table can be used, and an authentication server will issue a bar code, prompting the characters located in certain coordinates.

Both methods use the keys and the signals that may be communicated verbally. This allows an attacker to ask the user to the next valid code by malware using social engineering and phishing attacks. Moreover, the relatively low lists or grids entropy requires frequent keys change in order to prevent repeated code request by an attacker.

These techniques are vulnerable to the full range of «Man in the middle» attacks for the same reasons that all the authentication methods with an unknown context.

For the sake of PassWindow vulnerability testing against such an attack, was created an hacking algorithm, which tries to use these principles to perform this analysis.

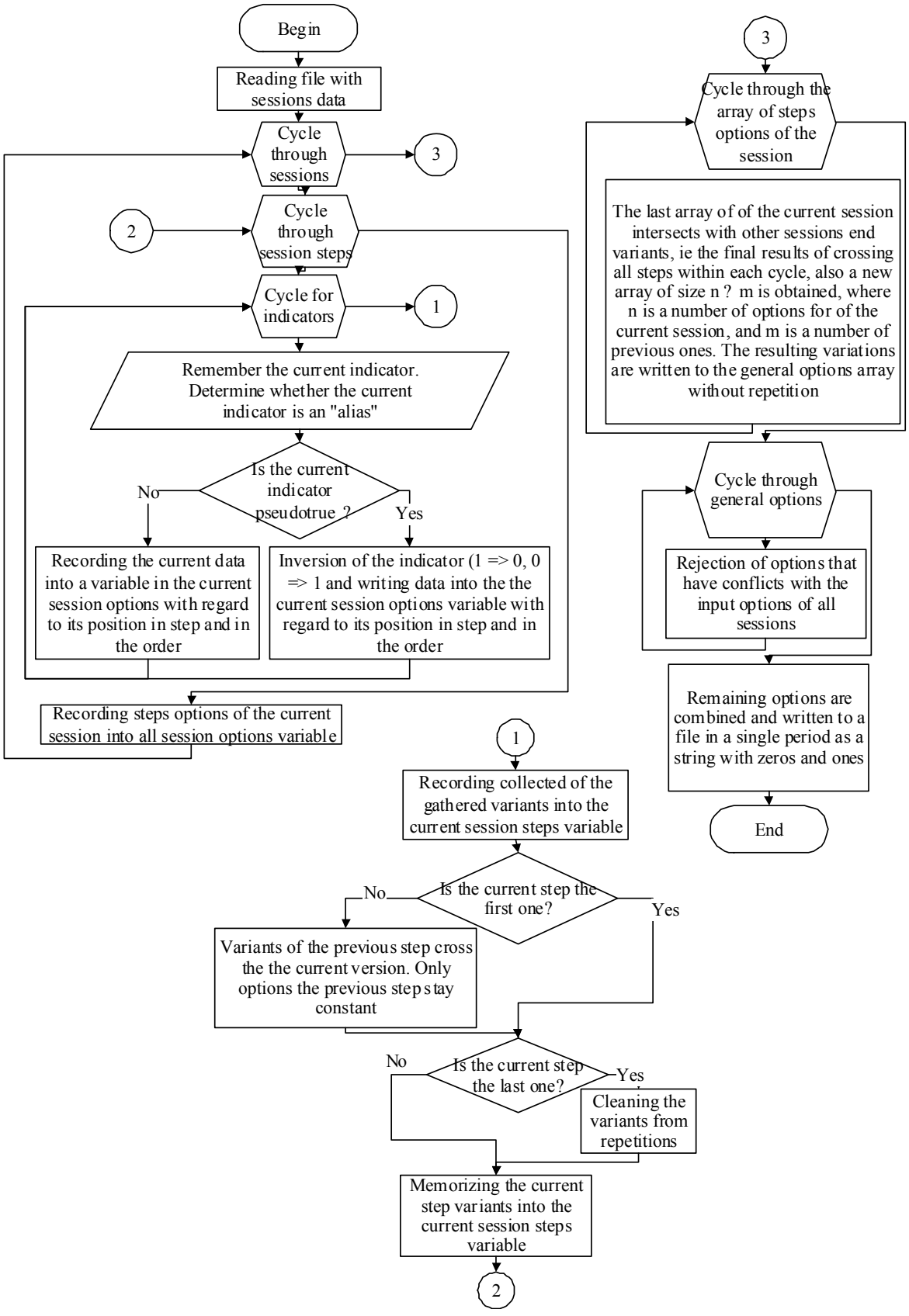

Figure 4 – Plastic PassWindow cards monitoring algorithm

The algorithm itself uses the technique of brute force. It begins by generating all combinations with the result that the numbers are the result that can be placed in the template.

For example, a six-figure result in the pattern of 14-columns provides the following options (among others):

2 – 5 – 7 – 2 – 4 – 3 – – –

2 – 5 – 7 – 2 – 4 – – 3 – –

2 – 5 – 7 – 2 – 4 – – – 3 –
2– – 5– – 7 – 2 – 4 – – 3.

Each combination is estimated by well-known barcode to calculate whether he could imagine the digit in the request or not.

Segments can either be present, if they are necessary to build the solution or not, if they must be absent for it, or may be unknown, if the segment is far from the digit, or imposed on the barcode bit.

After a separate set of combinations for each interception, the algorithm looks for the incompatibility between the combinations. It takes the first combination of the first set, comparing it in turn with each of the combinations of the second set. If it is incompatible with each combination of the second group, the combination is discarded.

Compatibility check continues so that each combination in each set is compared with the combinations of each other set. If the combination is discarded, then each subsequent set needs to be revised. By sorting and analysing sufficient number of interceptions algorithm is able to derive the key pattern with sufficient reliability.

However, this attack requires a significant amount of interceptions by an attacker: 20–30 in case of small patterns, hundreds of templates for large, several thousand in the case of using the method in the animation mode of increased security.

Thus, the PassWindow safety is not so much the complexity of the algorithm needed to solve it, as the systemic extracting enough information from the target difficulties. If PassWindow used correctly, there is a high probability that the necessary information may not be available, even for the most experienced hackers.

Let concider the Fake (weakened) PassWindow barcodes.

An attacker can try to weaken the protection, changing the frame rate of real (intercepted) barcode before delivering weakened (simplified) bar code to the user. This method reduces the entropy of the bar code in order to change details that could facilitate the analysis intercepting of requests / responses. However, clearly the damaged barcode passively alerts the user to attempt an attack, causing his suspicions about the use of computing and communication channels.

However, this attack requires a considerable amount of interceptions by an attacker: from 20 to 30 in case of small templates and hundreds for large ones, several thousand in the case of using the method in the animation mode with advanced security mode [1].

Thus PassWindow security is not so much the complexity of the algorithm required to solve it, but the difficulties in the system problems of sufficient information retrieval from the target. If PassWindow is used correctly, there is a high probability that the required information may not be available even for the most experienced hackers.

The authors offer their algorithm of PassWindow system monitoring, which allows in 3–5 sessions of transmission of OTP passwords to get a unique card barcode of a user that almost leads to destruction of the safety of the banking system.

6 DISCUSSION

Hypothetical attacks on authentication means PassWindow.

Man in the middle and phishing attacks (MITM) involve a third party intercepting communications between a client and server, impersonating each to the respective other and intercepting, recording, and/or altering communications between them [12].

Phishing is a kind of MITM attack that usually involves a fake login screen for well-known online services that reports login details to the attacking third party before seamlessly forwarding the user to their desired destination, unaware that their authentication details have been compromised to be used maliciously later [13].

This attack method is the most effective one. Standard methods for one-time password (OTP) are unable to provide protection because the OTP itself is simply passed to an attacker, together with any other relevant information, such as user name and password.

PassWindow solves this problem by providing a passive check at the transaction level to ensure that the user knows about the authenticity of the transaction, which one performs to enter OTP at the completion of this transaction. Thus, PassWindow protects transactions against fraudulent MITM attacks and provides authentication both ways from the user to the server and the server to the user.

Let concider the Social engineering attacks.

Social engineering involves the customer being convinced to reveal their private details, and in the case of hardware tokens, their OTPs.

A PassWindow key pattern is not easily communicated verbally or by typing, thereby eliminating the most convenient telephone social engineering attacks that are used against electronic hardware tokens, a method that is called «vishing» [14]. These attacks are based on the person who calls the user and impersonating an authorized service representative.

An oral request is made to read a valid authorization code from the authentication device of victim that supposedly allow the caller to identify, for example, «an important confidential information». It is unlikely that an attacker will try to extract the PassWindow key combination from the client this way, as it is difficult to explain in words the visual characteristics of the PassWindow matrix segment.

Man in the browser or hacker infiltration. When an attacker receives reports from the malware installed in the victim's computer and detects that the victim is accessing their financial institution's website, the software alters the form data in the browser such that a different amount of funds are transferred to a different account – usually a 'mule' account. The owner of the mule account then transfers this money to the attacker.

Verification information about the transaction taking place can be encoded into the PassWindow challenge pattern. This can assure the user, for example, that the funds are being transferred to the correct account.

Let concider the Simple theft.

The only way for a PassWindow key pattern to be revealed and duplicated is by directly copying the card in one's immediate possession. This possibility is reduced by the introduction of a tint that can be printed over the pattern, hindering attempts at photography and photocopying.

However, because PassWindow should be used as the second factor in the authentication strategy, mere knowledge of the key pattern is insufficient for fraudulent authentication without also knowing the victim's username and password.

Shoulder surfing. While probably the most mundane of the 'hacking methods', PassWindow is secure against 'shoulder surfing' – surreptitiously watching the user enter their transaction details. Because the key/challenge solution

is a one-time password, the shoulder surfer cannot benefit from knowing it.

Again, a tint printed over the key pattern on the card renders the pattern itself invisible to anyone but the user.

Direct attack on a PassWindows authentication server. An attacker can try to directly attack a PassWindows authentication server, to disrupt the integrity of the PassWindow authentication procedure. The PassWindow authentication server uses very simple and limited communication protocol, and the entire authentication processing is performed on the server. Its functionality is limited to the creation of the barcode image data and receiving short access codes and user IDs, and eventually making a response (yes / no) to the authentication request. In addition, different authentication strategies run queries speed and response duration. This basic digital communications with the authentication server give a small opportunity for an attacker to directly occupy the server in any effective manner, which may lead to a successful access.

Let concider the Analytic attack on the secret key.

An attacker can try to bring a printed the PassWindow key combination of a user through the analytical (e.g. statistical or algebraic) attack. This can be done using a complex program «attack of the man in the middle» or malicious programs installed locally on the basis of monitoring that will allow to intercept PassWindow barcodes and appropriate user responses. With the time, as the attacker accumulates these pairs of request / response, one can potentially get some idea about the PassWindow key template through the analysis of the captured data.

CONCLUSIONS

In this paper, the theoretical generalization of major the increase principles of integrity and authenticity of data packets in security banking transactions protocols based on authentication methods of the two-factor authentication.

Scientific novelty lies in the fact that, for the first time proposed mathematical tools and program implementation of the PassWindow system monitoring allows to get a unique barcode of the user's card for 3–5 OTP passwords transmission sessions, which almost leads to destruction of the banking system safety.

ACKNOWLEDGEMENTS

Work was executed within the concept of the National Informatization Program, approved by the Law of Ukraine «On the Concept of National Informatization Program» dated 4 February 1998 № 75/98-VR.

Concept (Principles of Public Policy) of the National Security of Ukraine, adopted by the Supreme Council of Ukraine on 16 January 1997 № 3/97-VR.

Tactical and technical task for research work: – № 36B113 «Development of methods for improving efficiency of transmission and protection of information in telecommunication systems».

REFERENCES

1. Evaluation of hypothetical attacks against PassWindow [Electronic resource] / S. O'Neil // PassWindow – 2009. – Access mode: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
2. Двухфакторная Аутентификация [Электронный ресурс], *Aladdin,* 2014, Режим доступа: http://www.aladdin-rd.ru/solutions/authentication.
3. Настройка двухфакторной аутентификации [Электронный ресурс], *Citrix,* 2012, Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru.
4. Семь методов двухфакторной аутентификации [Электронный ресурс], *ITC.ua*, 2007, Режим доступа: http://www.infosecurityrussia.ru/news/29947.
5. Man In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication [Electronic resource] / E. Chickowski // Information week – 2010. – Access mode: http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495.
6. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication [Electronic resource] / E. Barkan, E. Biham, N. Keller // ACM digital library. – 2008. – Access mode: http://dl.acm.org/citation.cfm?id=1356689.
7. $45k stolen in phone porting scam [Electronic resource] / Brett Winterford // ITnews – 2011. – Access mode: http://www.itnews.com.au/News/282310,45k-stolen-in-phone-porting-scam.aspx/0.
8. Zeus Banking Trojan Hits Android Phones [Electronic resource] / M. J. Schwartz // Information week. – 2011. – Access mode: http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909.
9. Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth [Electronic resource] / [C. Zeitz, T. Scheidat, J. Dittmann; at all.] // Proceedings of SPIE. – 2008. – Access mode: http://spie.org/Publications/Proceedings/Paper/10.1117/12.767632.
10. Trojan Writers Target UK Banks With Botnets [Electronic resource] // TechWorld. – 2010. – Access mode: http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets.
11. Belgian court found fraud in Internet banking [Electronic resource] / Het Belang Van Limburg // PassWindow – 2010. – Access mode: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
12. Network Forensic Analysis of SSL MITM Attacks [Electronic resource] // NETRESEC Network Security Police Service – 2011. – Access mode: http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks.
13. Internet Banking Targeted Phishing Attack [Electronic resource] // Metropolitan Police Service – 2005. – Access mode: http://www.webcitation.org/5ndG8erWg.
14. Spike in phone phishing attacks [Electronic resource] / Brian Krebs // KrebsOnSecurity – 2010. – Access mode: http://krebsonsecurity.com/2010/06/a-spike-in-phone-phishing-attacks.

Article was submitted 07.11.2014.
After revision 21.11.2014.

Евсеев С. П.[1], Томашевский Б. П.[2]

[1]Канд. техн. наук, доцент кафедры информационных систем Харьковского национального экономического университета им. С. Кузнеца, Харьков, Украина

[2]Канд. техн. наук, ведущий научный сотрудник, старший научный сотрудник научно-исследовательского отдела ракетных войск и артиллерии научного центра сухопутных войск, Харьков, Украина

ИССЛЕДОВАНИЕ УГРОЗ МЕТОДОВ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

В статье рассматриваются основные методы построения системы двухфакторной аутентификации на основе использования криптографических механизмов обеспечения криптостойкости, формируемых аутентификаторов, оценивается риск различных методов онлайн-атак против различных систем двухфакторной аутентификации, а также рассматривается система PassWindow, обеспечивающая двухфакторную аутентификацию на уникальной способности части матриц передавать информацию таким образом, что она расшифровывается только при наложении физического шаблона знаков предполагаемого получателя и шаблона штрих-кода, получаемых через

электронно-сетевые устройства пользователей, стойкость к анализу обеспечивается уникальностью формирования шаблона штрих-кода карточки в виде уникальных статистических изображений, последовательности символов или в виде более расширено анимационной версии.

Объектом исследования является процесс повышения целостности и аутентичности пакетов данных в протоколах безопасности банковских транзакций на основе методов двухфакторной аутентификации. Предметом исследования являются методы и алгоритмы контроля целостности и аутентичности пакетов данных в протоколах безопасности банковских транзакций на основе методов двухфакторной аутентификации.

Целью работы является повышение целостности и аутентичности пакетов данных в протоколах безопасности банковских транзакций, оценка угроз на методы двухфакторной аутентификации. Проводится сравнительный анализ различных систем двухфакторной аутентификации с системой PassWindow в сфере противостояния различным интернет-сценариям атак. Предлагается эффективный практический метод мониторинга системы двухфакторной аутентификации PassWindow при ее применении в банковских системах.

Ключевые слова: двухфакторная аутентификация, онлайн-атаки, социальная инженерия.

Евсеев С. П.[1], Томашевский Б. П.[2]

[1]Канд. техн. наук, доцент кафедри інформаційних систем Харківського національного економічного університету ім. С. Кузнеця, Харків, Україна

[2]Канд. техн. наук, провідний науковий співробітник, старший науковий співробітник науково-дослідного відділу ракетних військ та артилерії наукового центру сухопутних військ, Харків, Україна

ДОСЛІДЖЕННЯ ЗАГРОЗ МЕТОДІВ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

У статті розглядаються основні методи побудови системи двофакторної аутентифікації на основі використання криптографічних механізмів забезпечення криптостійкості, аутентифікаторів, які формуються, оцінюється ризик різних методів онлайн-атак проти різних систем двофакторної аутентифікації, а також розглядається система PassWindow, що забезпечує двофакторну аутентифікацію на унікальній здатності частини матриць передавати інформацію таким чином, що вона розшифровується тільки при накладенні фізичного шаблону знаків передбачуваного одержувача і шаблону штрих-коду, одержуваних через електронно-мережеві пристрої користувачів, стійкість до аналізу забезпечується унікальністю формування шаблону штрих-коду картки у вигляді унікальних статистичних зображень, послідовності символів або у вигляді більш розширено анімаційної версії.

Об'єктом дослідження є процес підвищення цілісності та автентичності пакетів даних у протоколах безпеки банківських транзакцій на основі методів двофакторної аутентифікації. Предметом дослідження є методи та алгоритми контролю цілісності та автентичності пакетів даних у протоколах безпеки банківських транзакцій на основі методів двофакторної аутентифікації.

Метою роботи є підвищення цілісності та автентичності пакетів даних у протоколах безпеки банківських транзакцій, оцінка загроз на методи двофакторної аутентифікації. Проводиться порівняльний аналіз різних систем двофакторної аутентифікації з системою PassWindow у сфері протистояння різним інтернет-сценаріями атак. Пропонується ефективний практичний метод моніторингу системи двофакторної аутентифікації PassWindow при її застосуванні в банківських системах.

Ключові слова: двофакторна аутентифікація, онлайн-атаки, соціальна інженерія.

REFERENCES

1. Sean O'Neil Evaluation of hypothetical attacks against PassWindow [Electronic resource], *PassWindow*, 2009, Access mode: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
2. Dvuxfaktornaya Autentifikaciya [Electronic resource] // Aladdin – 2014. – Access mode: http://www.aladdin-rd.ru/solutions/authentication.
3. Nastrojka dvuxfaktornoj autentifikacii [Electronic resource] // Citrix – 2012. – Access mode: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru.
4. Sem' metodov dvuxfaktornoj autentifikacii [Electronic resource] // ITC.ua – 2007. – Access mode: http://www.infosecurityrussia.ru/news/29947.
5. Chickowski, Ericka Man In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication [Electronic resource], *Information week*, 2010, Access mode: http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495.
6. Elad Barkan, Eli Biham, Nathan Keller Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication [Electronic resource], *ACM digital library*, 2008, Access mode: http://dl.acm.org/citation.cfm?id=1356689.
7. Brett Winterford $45k stolen in phone porting scam [Electronic resource], *Itnews*, 2011, Access mode: http://www.itnews.com.au/News/282310,45k-stolen-in-phone-porting-scam.aspx/0.
8. Schwartz, Mathew J. Zeus Banking Trojan Hits Android Phones [Electronic resource], *Information week*, 2011, Access mode: http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909.
9. Christian Zeitz; Tobias Scheidat; Jana Dittmann; Claus Vielhauer; Elisardo González Agulla; Enrique Otero Muras; Carmen Garc a Mateo; José L. Alba Castro Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth [Electronic resource], *Proceedings of SPIE*, 2008, Access mode: http://spie.org/Publications/Proceedings/Paper/10.1117/12.767632.
10. TechWorld Trojan Writers Target UK Banks With Botnets [Electronic resource], 2010, Access mode: http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets.
11. Het Belang Van Limburg Belgian court found fraud in Internet banking [Electronic resource], *PassWindow*, 2010, Access mode, http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
12. Network Forensic Analysis of SSL MITM Attacks [Electronic resource], *NETRESEC Network Security Police Service*, 2011, Access mode: http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks.
13. Internet Banking Targeted Phishing Attack [Electronic resource], *Metropolitan Police Service,* 2005, Access mode: http://www.webcitation.org/5ndG8erWg.
14. Brian Krebs Spike in phone phishing attacks [Electronic resource], *KrebsOnSecurity*, 2010, Access mode: http://krebsonsecurity.com/2010/06/a-spike-in-phone-phishing-attacks.