УДК 004.056.523:004.732 DOI: 10.31673/2412-9070.2023.053537

N. M. AUSHEVA[1], D.S., assoc. professor;
Y. V. MELNYK[2], D.S., assoc. professor;
S. I. OTROKH[1], D.S., assoc. professor;
I. S. MORDAS[1], student,
[1] National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv
[2] State University «Kyiv Aviation Institute», Kyiv

SYSTEM OF TWO-FACTOR AUTHENTICATION OF THE USER OF THE CORPORATE ENVIRONMENT USING A QR CODE

In today's world, technologies are developing at a rapid pace. It is very difficult to imagine a sphere of human life where digital data is not used, for example, banking operations, distance learning, utility payments, online messaging have become commonplace for us. However, on the other hand, the question arose of how to ensure the reliability and confidentiality of this data. One of the methods was authentication when entering the system, that is, entering a login and password to identify the user. To date, this method is not reliable and quite vulnerable, because most users have started using the same passwords for login, or simply ignore their reliability and use rather primitive ones. As a result of such actions, more and more confidential user data is at risk of being acquired by unauthorized criminals.

The idea to develop a two-factor authentication system using a QR code arose as a result of the urgency of this problem and the imperfection of existing software products. The basis will be the generation of a unique code that will be available only for a short period of time, which will be enough for the user to enter the system. This technology will allow dynamically changing the set of numbers required for authentication. If an attacker takes possession of it, he will not be able to use it, because it will change in the system in a fairly quick period of time.

The article discusses the implementation of the two-factor authentication algorithm using a QR code, which has a simple appearance, but can store a large amount of data. Also, regardless of how much information the QR code contains, the data is displayed immediately after reading it. This provides an increased level of protection when the user enters the system and prevents unauthorized access to confidential data by cybercriminals.

An approach using TOTP (Time-based One-time password) is also proposed, which will generate a one-time code based on a secret key. The main feature is the use of time as one of the parameters to generate a dynamic 6-digit password required for logging into the system. Also, its generation will be carried out automatically every 30 seconds, thus creating conditions for making its theft and unauthorized use impossible.

Keywords: QR code; barcode; TOTP algorithm; dynamic password generation; data scanning.

Introduction

In today's world, there is a rapid development of technologies, which has led to an increase in the amount of information that people use in everyday life. Today's realities require the creation of software products that are compact, easy to use and visually pleasing to the user. The main purpose of such applications is to find and provide the necessary information in the fastest way and in the appropriate format.

One of the widely used methods of presenting data are QR codes, which stands for «Quick Response». Such codes are two-dimensional black and white symbols of a square shape, in which data is encoded horizontally and vertically, which can be read, for example, using a mobile phone. Today, they are used in various environments of human life: in trade, production, entertainment, and in scientific institutions.

It is worth paying attention to the process of user identification to the application, during which you need to enter a login and password to check the appropriateness of access to certain information in the system. However, this method does not provide maximum data protection, because when using the same or unreliable passwords, which may contain personal data, for different social networks and e-mails, the risk of data leakage from cybercriminals increases.

Two-factor authentication using a QR code can solve this problem and provide increased protection when entering the system. After all, in addition to entering the basic login and password, the system will expect a special code that will be unique for each system user and dynamically generated every 30 seconds. And access to which can be obtained only after scanning the QR code, which will be unique and will appear only during the initial registration to the system.

The purpose of this work is to implement a system of two-factor identification of the corporate environment using a QR code. The use of such software will guarantee increased protection during authorization and will prevent unauthorized access to resources by offenders.

The main part

The QR code was developed and presented for the first time in 1994 by the Japanese company Denso-Wave. The main goal of creation was to simplify the scanning of barcodes and increase the amount of information that could be encrypted. A year after the start of development, the first version was presented, which could store up to 7,000 Chinese characters and scanning was ten times faster than traditional codes.

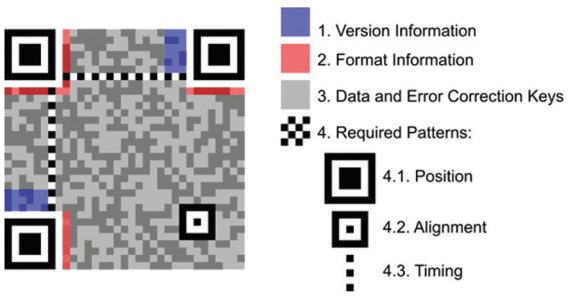
A unique feature of this development was the method of reading the code. Previously, this process took place only in one direction - from top to bottom, which led to the storage of a limited amount of free information. While the QR code was read from top to bottom and from right to left, it is already two directions, which significantly reduced the scanning time and increased the amount of data that can be encrypted.

Thus, the technical characteristics of passable QR codes today are:

- numbers — 7089 characters;
- code — 295 bytes;
- hieroglyphs — 1817.

The QR code is based on an encrypted sequence of data, which is stored in binary format in the form of a matrix. Each cell of the matrix is assigned a value depending on the color: white or black. The special device recognizes the code with the help of three main square marks, which are placed in the corners and indicate the direction of reading. The next step is to scan and analyze each square and present it in the form of a grid with the corresponding values.

The figure shows the structure of the QR code.



The structure of the QR code

One of the elements that ensures reading even on an uneven surface is the synchronization lines. A QR code contains a version marker that lets you understand its format: binary, numeric, alphanumeric, and kanji for Japanese characters.

There are also special Reed-Solomon error correction blocks, which are special combinations that correct the QR during reading. As a result of such actions, even damaged up to 30% code will be read correctly.

The use of two-factor authentication creates a double level of protection and allows you to distinguish between an attacker and a verified user. Entering the system using a QR code works on the basis of Time-based One-time Password Algorithm (TOTP). During registration by QR scanning, you need to get a secret key that will generate a one-time password with a numerical period of 30 seconds.

In the process of researching this technology, it was decided to create a two-factor authentication system using a QR code. After all, the speed of reading, volume of information and ease of use will help solve one of the urgent problems with identification. The usual method of verifying the user using a login and password has lost its reliability and has become quite vulnerable in the modern world. It is worth paying attention that almost every person has several social networks or e-mails for which you need to use unique and unique passwords to gain access, but there is such a tendency that users do not follow these rules.

Algorithm of the program. The two-factor authentication system using a QR code is based on the TOTP (*Time-based One-Time Password*) algorithm, which provides a one-time time-based password for logging into the system.

It is worth noting that, unlike other authentication methods, a certain application on a smartphone is required to generate a unique code. Thus, the logic of this algorithm will be implemented on the server and user side.

The sequence of actions performed by the program to ensure authentication:

1. The server generates a secret key;
2. This key is encrypted using a QR code;
3. The mobile application reads the QR code and generates a one-time password based on the received data;
4. The generated password changes dynamically with a certain time interval.

Let's consider in more detail the code generation algorithm, which in turn uses the outdated HOTP (*One-time password based on HMAC*) methodology as a basis. This algorithm creates an HMAC hash (a method based on SHA-1), which combines a secret key and a counter. As a result of such actions, we get a string 20 bytes long, which is later truncated to the form of a one-time password.

The main difference between HOTP, which generates a counter-based hash, and TOTP is the use of a time parameter as a unique identifier for code generation. It is worth noting that to eliminate misunderstandings with different time zones, a Unix time stamp is used, which in turn is counted in seconds.

The principle of operation of the program can be described using formulas:

$$T = \frac{CurrentTime - T_0}{X}, \quad (1)$$

$$HOTP(K,T) = Truncate(HMAC - SHA - 256\,(K,T), \quad (2)$$

$$TOTP = HOTP(K,T), \quad (3)$$

де T — discrete time value; *CurrentTime* — current time in seconds, from the beginning of the epoch measurement; T_0 — starting time; X — the length of the time period (30 seconds); K — secret key; $HMAC-SHA-256$ — hash generation function based on a secret key and time in the form of 20 bytes; *Truncate* — method of reducing to 4 bytes.

Also, when implementing this algorithm, you can use various hash functions, such as HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512, depending on specific requirements.

The generated key must be entered into the mobile application, where the dynamic code for authentication will be displayed directly, for this we will use the QR code.

So, the following sequence of actions takes place: the mobile application reads the secret key from the QR code and the time value at the moment, with the help of the TOTP algorithm, the password is generated. When the user enters this code into the system during authentication, similar things happen on the server side in order to generate his dynamic password and compare it with what was received.

Intelij Idea was used as a development environment, which provides a wide range of possibilities for the implementation of this system. The high-level Java programming language was used to write the software, which provides all the necessary tools for writing code, connecting auxiliary external systems and accessing interaction with the database.

The TOTP algorithm is a modern cryptographic method for authentication. It is quite resistant to cyberattacks, but it is worth considering ways to hack this technology. One of which is the interception of login and password using traffic listening. To prevent such a case, it is worth reducing the validity period of the one-time password, so that in case of possession of it, the offender does not have time to use it.

Conclusions

Having studied the technical characteristics and the principle of operation of QR codes, it is possible to propose its use for two-factor authentication, because it is easy to read, print, fast, safe and can encrypt a large amount of information.

The implemented TOTP algorithm is a reliable way to increase the security level of confidential data protection and prevent cyber-attacks on accounts during authentication. After all, to successfully enter the system, you need to know the secret key and the exact time.

Thus, by combining the capabilities provided by the QR code and the TOTP algorithm, we can create a reliable system with the help of which the user can safely perform two-factor authentication.

References

1. ***Boyles A.*** *The Complete Guide to QR Codes Kindle Edition. QR-Codes.com, 2012. 35 p.*

2. ***Huaguo J.*** *Study and Application of Encoding and Decoding Algorithms for Colored Two-dimensional Code on Mobile Terminals. Hangzhou: Zhejiang University of Technology, 2009. 17 p.*

3. ***Time*** *based One Time Password [Electronic resource]. URL:*

https://www.hypr.com/security-encyclopedia/time-based-time-password-totp-otp

4. ***Winter M.*** *Scan me: Everybody's Guide to the Magical World of QR Codes. Westsong Publishing, 2011. 144 p.*

5. ***Hopkins D.*** *QR Codes in Education: QR Codes ... A great way to pass information from on source to another. Westsong Publishing, 2013. 108 p.*

Н. М. Аушева, Ю. В. Мельник, С. І. Отрох, І. С. Мордас

СИСТЕМА ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА КОРПОРАТИВНОГО СЕРЕДОВИЩА З ВИКОРИСТАННЯМ QR-КОДУ

У сучасному світі технології розвиваються стрімкими темпами. Дуже складно уявити сферу людського життя, де б не застосовувалися цифрові дані. Зокрема, банківські операції, навчання в дистанційному форматі, оплата комунальних послуг, онлайн-обмін повідомленнями стали для нас звичними речами. Водночас постало питання, як забезпечити надійність і конфіденційність цих даних. Одним із методів була автентифікація під час входу в систему, тобто введення логіна і пароля для ідентифікування користувача. Сьогодні такий метод є ненадійним і доволі вразливим, адже більшість користувачів почали застосовувати одні й ті самі паролі для входу, або просто ігнорують їх надійність і використовують доволі примітивні. Як наслідок таких дій все більше і більше конфіденційних даних користувачів перебувають під загрозою заволодіння несанкціонованими правопорушниками.

Ідея розробити систему двофакторної автентифікації за допомогою QR-коду виникла в результаті актуальності цієї проблеми і недосконалості вже наявних програмних продуктів. За основу братиметься генерація унікального коду, котрий буде доступний лише невеликий проміжок часу, якого буде досить, щоб користувач увійшов до системи. Така технологія дасть змогу динамічно змінювати набір цифр, потрібний для автентифікації. У разі, якщо зловмисник заволодіє кодом, то він не зможе ним скористатися, адже код зміниться в системі за доволі швидкий проміжок часу.

У статті розглянуто реалізацію алгоритму роботи двофакторної автентифікації за допомогою QR-коду, який має простий вигляд, проте може зберігати великий обсяг даних. Також незалежно від того, скільки інформації містить QR-код, відображення даних відбувається відразу після його зчитання. Це забезпечує підвищений рівень захисту під час входження користувача до системи й унеможливлює несанкціонований доступ до конфіденційних даних із боку кіберзлочинців.

Також запропоновано підхід із використанням TOTP (Time-based One-time password), який генеруватиме одноразовий код на основі секретного ключа. Основною особливістю є використання часу як одного з параметрів для створення динамічного шестизначного пароля, потрібного для входу в систему. Також його генерація буде здійснюватися автоматично кожні 30 с, унеможливлюючи його викрадення і несанкціоноване використання.

Ключові слова: QR-код; штрих-код; алгоритм TOTP; динамічна генерація пароля; сканування даних.