The practice of using one-time passwords in modern corporate information systems

V Landyshev[1,*], *T* Blinovskaya[1], *D* Krakhmalev[2]

[1]Don State Technical University, 1 Gagarina sq., Rostov-on-Don, 344003, Russia
[2]University under the Government of the Russian Federation, 49, Liningradsky Prospekt, Moscow, 125993, Russia

Abstract. One-time password (OTP) systems, or one-time passwords, are an authentication method in which the user is provided with a password that is active only for one login session or transaction in an information system. Currently, the systems are not implemented in their pure form, but are one of the components in multi-factor authentication systems. Despite its widespread use in the financial sector, a one-time password does not guarantee secure login authentication.

1 Introduction to authentication problems in corporate systems

Currently, the human factor continues to be one of the fundamental threats in the modern information system model.

As a rule, the user's password is most sensitive to attacks, and as practice shows, a user with administrative rights, i.e. an administrator of an information system, website, or other resource.

One of the objective challenges for the modern corporate information space is the organization of secure user authentication both inside and outside the information security perimeter of the corporate computer network.

Sniffing, brute force, social engineering, and the use of malware such as keyloggers are not a complete list of ways in which a user's password can be compromised.

The traditional mechanism for ensuring password strength in an organization is the organization's password policy, which involves a number of organizational and technical measures designed to strengthen password protection. Traditionally, these methods include applying requirements for complex password complexity, applying requirements for password uniqueness, determining the password lifetime, and so on.

Unfortunately, as experience shows, these policies are not always effective and often fail to be implemented not only when authenticating with user rights, but also when accessing with privileged rights.

One of the ways to increase the strength of a password is to shorten its life. In essence, the process is similar to the technology of using a classic cipher block, in which a new encoding sequence is used for each encryption transaction. This technology is called OTP (

* Corresponding author: vlandyshev@donstu.ru

One Time Password) and is described in RFC 2289 .OTP (One Time Password) technology allows the user to use only one permanent password to log in to the information system [1].

2 OTP technology implementation principles

An OTP password-based authentication system uses a secret passphrase to generate a sequence of one-time (one-time) passwords. With this system, the user's passphrase must never cross the network at any time, such as during authentication or when changing passphrases. Thus, it is not vulnerable to repeated attacks. Additional security is provided by the property that no secret information should be stored in any system, including the protected server.

The OTP system protects against external passive attacks on the authentication subsystem. It does not prevent a network eavesdropper from gaining access to private information and does not provide protection from either "social engineering" or active attacks.

Currently, use in its pure form has not found commercial and application, but is a component of many multi-factor authentication systems.

When a user account is created in OTP authentication protocols, the account is tied to the user by owning some information related to the user, such as a mobile phone number or email address. On login, an OTP is generated for the user, who must return it correctly. Usually, an alternative channel for sending a one-time password is used, such as SMS, e-mail notification, using a specialized mobile application or a hardware token.

In fact, Android and IOS apps often use SMS OTP authentication, where the server generates a pseudo-random one-time password and sends it via SMS to the mobile phone number in the user profile. This pseudo-random value is only transmitted between the server and the user who owns the mobile phone. The user then sends the resulting value to the server for authentication. Naturally, strengthening the authentication process is required for applications that actively use confidential user information, for example, mobile applications of banks, business systems, etc.

In addition to the application, systems of hardware tokens of the U2F (Universal 2nd Factor) standard, created by the FIDO Alliance, are implemented in practice.

Hardware U2F tokens are essentially the information security standard in large information systems. First of all, because from the user's point of view, their use is not difficult. To get started, you need to connect the U2F token to your device and register it in the authentication service.

Subsequently, if you need to confirm the entrance to this service, you will need to connect the U2F token to the device from which you are logging in, and press the button on the token (in some devices, enter the PIN or put your finger on the scanner) at this stage, the authentication process in the system ends. One of the advantages of these systems is the ability to authenticate in services that support this standard.

The main algorithms for generating a one-time password are HOTP (HMAC-Based One-Time Password Algorithm), a secure authentication algorithm using a One Time Password (OTP) and TOTP (Time-based One-Time Password Algorithm, RFC 6238), an OATH algorithm for generating one-time passwords for secure authentication, which is an improvement on HOTP (HMAC-Based One-Time Password Algorithm). An algorithm of combinations of one-time passwords based on HMAC (HOTP) incrementing counter (C) and secret key (K) to generate a one-time password. The generated OTP value according to the HOTP algorithm is defined as

$$value = HOTP(K,C),$$

where HOTP is a function:

$$HOTP(K,C) = Truncate(HMACH_H (K,C)),$$

where H is a cryptographic hash function and the output from the HMACH hash function is truncated to a user-friendly size. A short HOTP value is convenient but vulnerable to brute force attacks.To address this issue, RFC 4426 recommends two steps:

1) the maximum number of possible attempts for a login session must be set in advance;

2) each unsuccessful attempt must introduce an additional delay before allowing a retry. RFC 4426 also suggests that with these safeguards, the HOTP value should be at least six digits long [2].

Time-based one-time password. The One Time Password (TOTP) algorithm is an extension of the HOTP algorithm that uses elapsed time increments instead of an event counter. The one-time password for each login session must remain valid for a period of time (determined by a fixed time step). Based on RFC 6238, the OTP value generated by the TOTP algorithm is defined as:

$$value = HOTP(K,C_T)$$

where K is the secret key and C_T is an integer counting the number of time steps completed between the start counter time T_0 and the current Unix time. Given the T_x time step in seconds, C_T is calculated as:

$$C_T =(\text{current Unix time} - T_0)/T_x$$

Due to network latency, the number of time steps (C_T) calculated by clients and servers may differ and therefore result in different TOTP values. This problem can be resolved by setting the OTP T_x time step to an acceptable size. The OTPs generated at any time within the time step will be the same and will allow the user to log in successfully.

However, the algorithm assumes the ability to accept one-time passwords from previous or subsequent time steps. For example, if an OTP is generated near the end of a timestep, the user can calculate the counter based on the subsequent timestep due to latency. To accommodate this, the server can receive OTPs computed at +/- 1 time steps from its current time step. However, a larger time step makes the OTP TOTP authentication protocol more vulnerable, because it gives an attacker more time to guess the one-time password value.

To balance the security and usability of this authentication scheme, RFC 6238 recommends setting the time step size to 30 seconds. In addition, the server must ensure that sufficient time has elapsed between the generations of sequential TOTP values so that the number of time steps (C_T) has changed [2].

3 Implementation of attacks on OTP systems using social engineering methods

In practice, security technologies where the second factor of authentication is widespread in the financial sector. Despite the fact that multifactor authentication technologies should increase the authenticity of user authentication in the information system, in fact, attackers deceiving the OTP system password received full access to the system, the attack scheme is shown in Figure 1 [4].

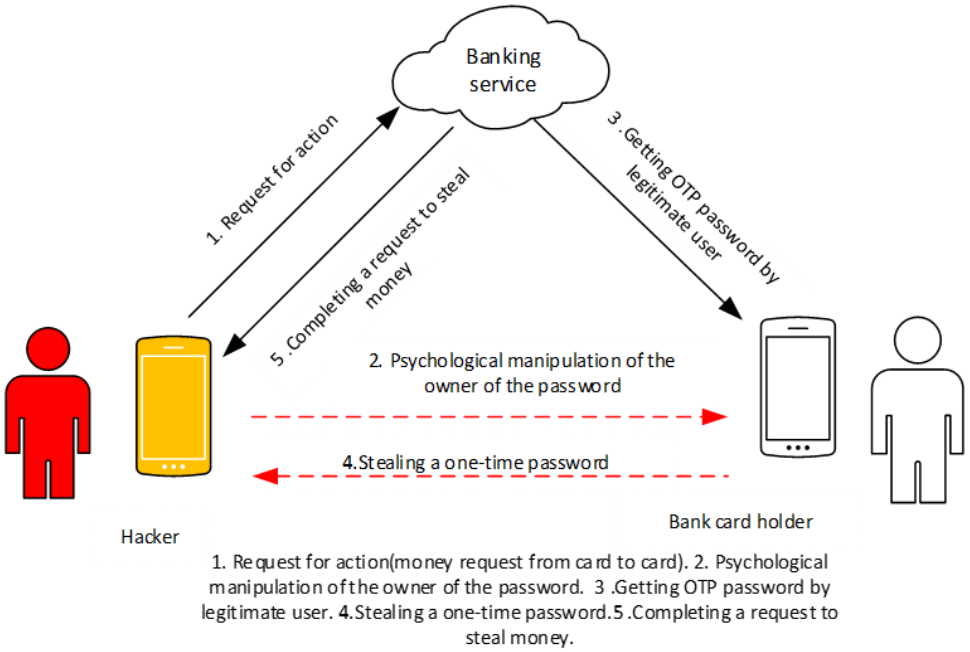

Fig. 1. The attack scheme.

Fraudsters use the substitution of their own numbers for the official numbers of banks in order to contact bank clients on behalf of a credit institution and deceive money through their personal accounts or simply from cards. Social engineering became the most widespread method of stealing money from bank clients in Russia in 2018: it accounted for 97% of all cases of theft.

In June-August 2019, the Central Bank of Russia sent information to telecom operators about more than 2.5 thousand telephone numbers from which calls to banking customers were received. The substitution of numbers was detected by operators in 198 cases in response to a message from the Central Bank of Russia [5].

4 Conclusions

1. At present, OTP systems in their pure form, with rare exceptions, have left the market, but at the same time they are widely used as a second method of authentication in multi-factor authentication systems. Currently, many systems use OTP as a secondary authentication method.
2. The OTP system significantly increases the strength of the password protection system, but practically does not protect against sniffing and social engineering methods. Currently, social engineering remains the main threat to multi-factor authentication systems.
3. The use of OTP systems in a corporate environment is currently one of the promising areas, but is constrained by its relative complexity and high cost when used in large corporate systems. The use of corporate systems of one-time passwords implemented by cloud services technology is promising.

References

1. RFC 2289 One-Time Password System https://tools.ietf.org/html/rfc2289
2. RFC 6238: Time-Based One-Time Password Algorithm https://tools.ietf.org/html/rfc6238
3. RFC 4426 Generalized Multi-Protocol Label Switching (GMPLS) https://tools.ietf.org/html/rfc4426
4. Hossein Siadatia, Toan Nguyena, Payas Guptaa,Markus Jakobssonb, Nasir Memon Mind your SMSes: Mitigating social engineering in second factor authentication Hossein Computers & Security Volume 65, March 2017, Pages 14-28
5. Computer Attack Monitoring and Response Center Report in the credit and financial sphere of the Department of Information security of the Bank of Russia 1.09.2018 - 31.08.2019
https://cbr.ru/Content/Document/File/84354/FINCERT_report_20191010.PDF