Mechanics Transport Communications

Academic journal http://www.mtc-aj.com

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
volume 19, issue 1, 2021
article № 2065

METHOD FOR PROVIDING TWO-FACTOR AUTHENTICATION IN OPERATING SYSTEMS WORKING WITH AUTHENTICATION SERVICES WITH CENTRALIZED ACCOUNT DATABASES IN TELECOMMUNICATION NETWORKS

Bohdan Rezanov[1], Galina Cherneva[2], Maksym Bartosh[1]
brezanov@gmail.com, cherneva@vtu.bg, s_semenov@ukr.net

[1]National Technical University "Kharkiv Polytechnic Institute",
Kharkiv, 2, Kyrpychova str., UKRAINE
[2]Todor Kableshkov University of Transport,
1574 Sofia, 158 Geo Milev Str., THE REPUBLIC OF BULGARIA

Key words: *two-factor authentication, Active directory, LDAP, MFA, operation system, telecommunication network*

Abstract**:** *During the research, method for providing two-factor authentication in operating systems working with authentication services with centralized account databases in telecommunication networks*

The work is dedicated to the development of a method for integrating two-factor authentication into operating systems by integrating the second factor into a centralized account database.

The work described scheme of an authentication process by using an additional component, the high-level scheme of interaction of system modules that implements the proposed method, sequence diagram of interaction of modules during user registration, authentication process using the proposed method.

Method is based on injecting OTP directly into the authentication service with a centralized account database.

The developed system consists of 9 interconnected modules, in which 7 relate directly to the system and 2 additional blocks (user and services).

In the proposed method, the authentication process has been improved by integrating the second factor into an authentication service with a centralized account database. This improvement made it possible to achieve universality, shorten the authentication time, and achieve the inexpediency of compromising the first factor.

The proposed method lacks an additional segment (service for checking the second factor).

INTRODUCTION

At the moment, there are many solutions to ensure security in telecommunication, computer systems and services. Among them, there are both satisfying the requirements that the world community puts forward to ensure security (integrity, confidentiality, availability, authenticity), and not satisfying.

One of the issues that the scientific community decides in the field of security is to ensure authenticity, the basis of which is authentication.

There are 3 authentication factors known today. The first is the knowledge (password), the second is the possession (token, smart card, phone) and the third is inherent (fingerprint, fingerprint, face, voice, iris recognition).

Studies have shown [1] that at the moment there are many different mechanisms, means and methods of authentication. The primary authentication method is single factor authentication. Single-factor authentication using an ID and

password has been found to be vulnerable to malware attacks, replay attacks, offline brute force attacks, key logger Trojans, dictionary attacks and shoulder surfing[2].

The solution is to use multiple authentication factors, such as the use of OTP (One Time Passwords) in addition to the knowledge.

However, a number of operating systems (Windows, Linux, MacOs) do not have the ability to use two-factor authentication mechanisms by default.

Modern scientists are developing new and improving old methods of authentication.

Many modern scientists are working on the current problem, including Wei-Yuan Lee, D Dasgupta, A Roy, A Nag and commercial organizations such as DUO, Okta, Microsoft.

Thus, it is relevant to develop a way to integrate two-factor authentication into operating systems using an authentication service with a centralized accounts database.

THE MAIN PART

Wei-Yuan Lee, in his work “Multi-Factor Authentication System and a Logon Method of a Windows Operating System” [3], offers a way to integrate two-factor authentication by installing a third-party component (Credential provider) into the Windows operating system. As well as the DUO company presented a similar technology to the public [4].

Let's take the Microsoft Windows authentication process based on the above method.

The authentication process is as follows:

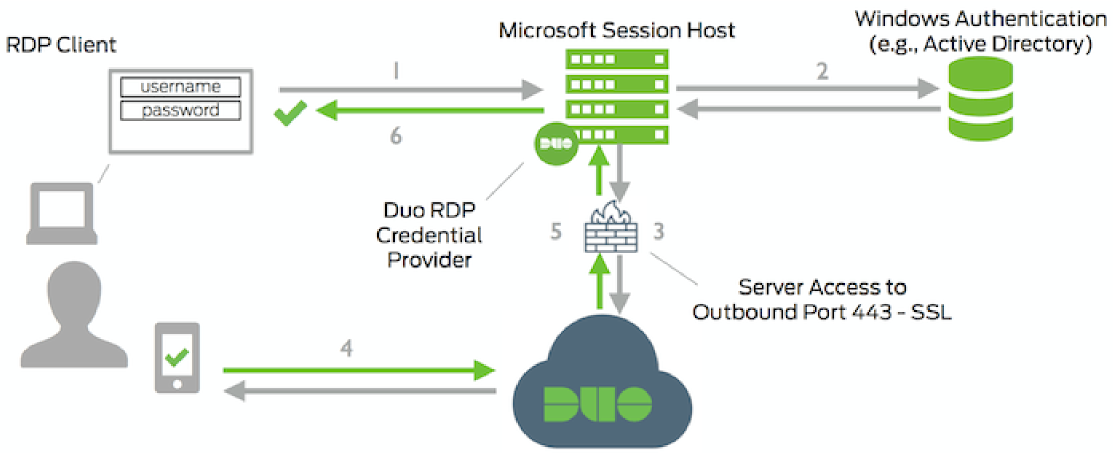

Fig. 1 Scheme of an authentication process by using an additional component

1. User enters username and password.
2. Primary authentication in the authentication service (Active Directory).
3. Request for entering OTP (second factor).
4. User enter OTP.
5. Response from the second factor verification service.
6. Target system allows the user to logon.

The presented method has several disadvantages. Let's consider some of them.

The versatility of the way. The presented method is not universal. Since operating systems such as Windows, Linux, MacOS have different authentication mechanisms inside, different components of user authentication are needed, different settings at the provider of the second factor.

Authentication time. The proposed method assumes the use of an additional service - the service of verification second factor.

Using the second factor verification service introduces additional steps into the authentication process, thereby increasing the authentication time.

Compromise of a first factor. Using a computer attack allows attackers to steal the password hash from the computer system, compromising the first factor. Thereby an opportunity to enter the system in which the additional component is not installed.

Thus, there is a need to create a universal method for integrating two-factor authentication in different operating systems by improving the above authentication method.

Method for providing two-factor authentication by integrating the second factor into an authentication service with a centralized account database is proposed.

Method is based on injecting OTP directly into the authentication service with a centralized account database and eliminates the disadvantages of the previously described method.

The basis was taken OTP generation algorithm - TOTP [5].

Consider a two-factor authentication process based on developing ways.

1. OTP value generated based on the clock and secret within the authentication device (phone application, OTP token) and developed OTP generation system, which then updates for a given predetermined period in Active Directory based on a predetermined user password and generated OTP.
2. The user activates their authentication device, which displays a generated value (1234567890) based on a hash of the time and secret.
3. User login, password plus the given OTP value is transmitted over the telecommunication network to the authentication server with a centralized database of accounts (Active Directory).
4. The server at this time find a record about the user, his password + OTP, and compares the values received from the user, if the coincidence of the given values, the authentication is considered successful.

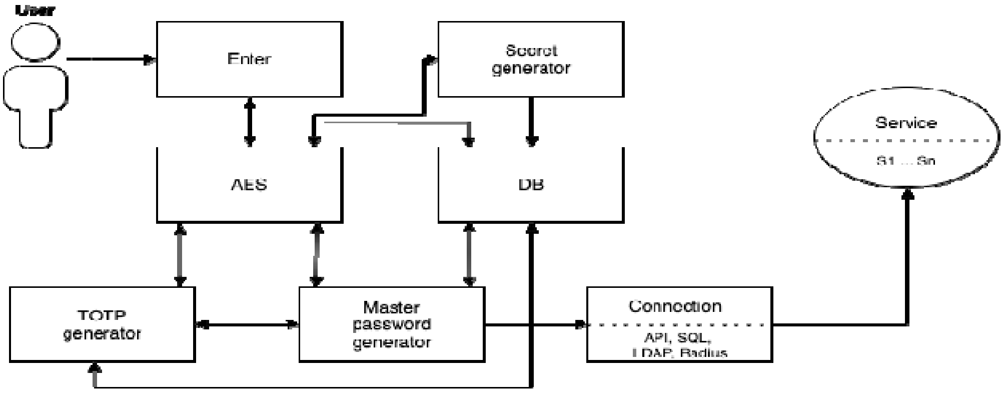

Fig. 2 High-level scheme of interaction of system modules

Description of system modules:

User:

Is a user who interacts with the system.

Module Enter:

This module is a web-application.

Interaction with this module occurs once, during the initial registration of a user in the system.

Interacts with the User, AES and DB modules.

The task of the module is to receive data from the user, encrypt it with the AES module, and store the encrypted data in the database using the DB module.

Module Secret Generator:

This module interacts with the AES and DB modules.

The module's task is:

- generating the secret key (pseudorandom sequence) in BASE32[6], which is used to generate one-time passwords;
- encryption of the generated key when interacting with the AES module;
- storing the encrypted value in the database through interaction with the DB module.

Module TOTP Generator:

module implements the TOTP algorithm.

The module's task is to generate one-time passwords (OTP).

Interacts with AES, DB, Master Password Generator modules.

When accessing this module from the Master Password Generator module, a request is made to the database via the module DB to obtain the encrypted secret key, then the resulting value is decrypted using the AES module. After receiving the encrypted value, generates an OTP based on the TOTP algorithm and returns the generated OTP to the module Master Password Generator.

Module Master Password Generator:

The task of the module is to concatenate the static password (the first factor) and the generated by the module TOTP Generator - OTP (the second factor) with the subsequent transfer of the value to the module Connection.

This module interacts with the AES, DB, TOTP Generator and Connection modules.

The Master Password Generator generates a request to the database via the module DB to obtain an encrypted static password, then the resulting value is decrypted using the AES module. The next step, module refers to the TOTP Generator module that generates the OTP.

After receiving two values, this module concatenates them and sends the final value to the module Connection for further transmission to the target system.

Module AES:

The module's task is to perform data encryption and decryption operations using the Hardware security module [7] using the pkcs # 11 protocol [8].

This module interacts with Enter, TOTP Generator, Secret Generator, Master password generator modules.

Module DB:

The module's task is to establish communication with the SQL database [9] through a secure connection using the TCP [10] + SSL [11] protocol.

This module interacts with Enter, TOTP Generator, Secret Generator, Master password generator modules.

Module Connection:

The module's task is to establish communication with the target authentication system with a centralized database of accounts.

This module interacts with the Master password generator module.

Service:

It is an authentication system with a centralized database of accounts such as Active Directory, OpenLdap, FreeIPA, Freeradius.

Interacts with the Connection module.

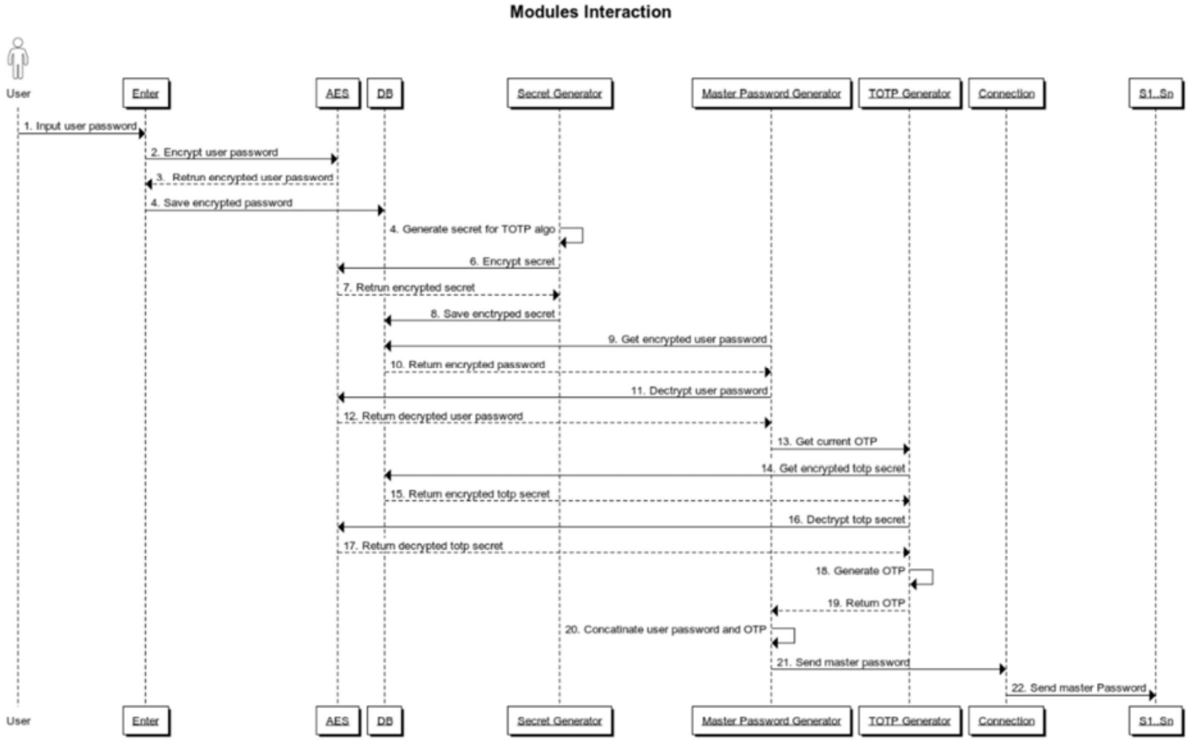
Modules Interaction
User
Enter
AES
DB
Secret Generator
Master Password Generator
TOTP Generator
Connection
S1..Sn
1. Input user password
2. Encrypt user password
3. Retrun encrypted user password
4. Save encrypted password
4. Generate secret for TOTP algo
6. Encrypt secret
7. Retrun encrypted secret
8. Save enctryped secret
9. Get encrypted user password
10. Return encrypted password
11. Dectrypt user password
12. Return decrypted user password
13. Get current OTP
14. Get encrypted totp secret
15. Return encrypted totp secret
16. Dectrypt totp secret
17. Return decrypted totp secret
18. Generate OTP
19. Return OTP
20. Concatinate user password and OTP
21. Send master password
22. Send master Password
User
Enter
AES
DB
Secret Generator
Master Password Generator
TOTP Generator
Connection
S1..Sn

Fig. 3 Sequence diagram of interaction of modules during user registration

Diagram Description:

1. User enters the login and password on the web page, which is sent to Enter module.
2. Enter module sends the received user's password to AES module for encryption.
3. AES module returns an encrypted password.
4. Enter module sends login and received encrypted password to DB module.
5. Secret Generator module generates a secret key for the TOTP algorithm.
6. Secret Generator module sends the secret key to the AES module for encryption.
7. AES module returns the encrypted secret key to the module Secret Generator.
8. Secret Generator module sends the received encrypted secret key to the DB.
9. Master Password Generator module generates a request to the DB to obtain the encrypted user password.
10. DB module returns the encrypted password to the Master Password Generator module.
11. Master Password Generator module sends an encrypted password to the AES module.
12. AES module returns the decrypted user password to the Master Password Generator module.
13. Master Password Generator module forms a request to the TOTP Generator module to get one time password.
14. Generator module generates a request to the DB module to obtain an encrypted secret key.
15. DB module sends an encrypted secret key to the TOTP Generator module.
16. TOTP Generator module sends an encrypted secret key to the AES module.
17. AES module returns the decrypted secret key to the module TOTP Generator module.
18. TOTP Generator module generates one time password.

19. TOTP Generator module returns the generated one time password to the Master Password Generator module.

20. Master Password Generator module concatenates the decrypted user password and one time password, thereby obtaining the master password.

21. Master Password Generator module sends the master password to the Connection module.

22. Connection module sends the received master password to the Sn system.

Consider the authentication process in Figure 4.

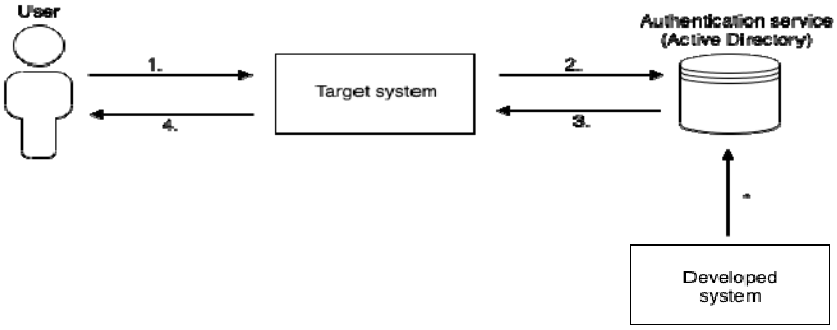

Fig. 4 Authentication process using the proposed method

1. User enters login and password and OTP into the target system
2. The target system authenticates to an authentication service with a centralized account database (Active Directory).
3. The authentication service returns a response to the target system
4. The target system allows the user to log on.

The system being developed implements the proposed method and changes the password in the authentication service with a centralized account database once in a given period of time.

CONCLUSIONS

In the proposed method, the authentication process has been improved by integrating the second factor into an authentication service with a centralized account database, which distinguishes this method from that presented by Wei-Yuan Lee and DUO. This improvement made it possible to achieve universality, shorten the authentication time and achieve the inexpediency of compromising the first factor.

The versatility of the way. The developed method performs manipulations in the authentication service with a centralized account database, which provides versatility when using different operating systems.

Authentication time. The proposed method lacks an additional segment (service for checking the second factor). Thus, the proposed method simplifies the authentication process by eliminating additional steps (3, 4, 5), in the method presented by Wei-Yuan Lee and the DUO company, thereby speeds up the authentication by the time spent on communication and the processing time of the request by the second factor verification service.

The possibility of compromising the first factor. This possibility is present, but it is impractical, since the validity of the password is limited by the validity time of the one-time password (by default, 30 seconds [5]).

Thus, the universality of the method of integrating two-factor authentication in different operating systems was achieved by integrating the second factor into an authentication service with a centralized account database.

REFERENCES:

[1] Methods and systems for multifactor authentication // https://patents.google.com/patent/US7739744B2/en
[2] Jae-Jung Kim, Seng-Phil Hong A Method of Risk Assessment for Multi-Factor Authentication. Journal of Information Processing Systems, Vol.7, No.1, March 2011
[3] Multi-Factor Authentication System and a Logon Method of a Windows Operating System // https://patents.google.com/patent/US20080115208A1/en
[4] Duo Authentication for Windows Logon and RDP // https://duo.com/docs/rdp
[5] TOTP: Time-Based One-Time Password Algorithm // https://tools.ietf.org/html/rfc6238
[6] The Base16, Base32, and Base64 Data Encodings // https://tools.ietf.org/html/rfc4648
[7] Hardware security module // https://en.wikipedia.org/wiki/Hardware_security_module
[8] The PKCS #11 URI Scheme // https://tools.ietf.org/html/rfc7512
[9] SQL // https://en.wikipedia.org/wiki/SQL
[10] Transmission control protocol (TCP) // https://tools.ietf.org/html/rfc793
[11] The Secure Sockets Layer (SSL) Protocol Version 3.0 // https://tools.ietf.org/html/rfc6101

МЕТОД ОБЕСПЕЧЕНИЯ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ОПЕРАЦИОННЫХ СИСТЕМАХ, РАБОТАЮЩИХ С СЕРВИСАМИ АУТЕНТИФИКАЦИИ С ЦЕНТРАЛИЗОВАННЫМИ БАЗАМИ ДАННЫХ УЧЕТНЫХ ЗАПИСЕЙ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Богдан Резанов[1], Галина Чернева [2], Максим Бартош[1]
brezanov@gmail.com, cherneva@vtu.bg, s_semenov@ukr.net

[1]Национальный технический университет «Харьковский политехнический институт», г. Харьков, ул. Кирпичова, 2, УКРАИНА
[2]Висше транспортно училище «Тодор Каблешков» София ул. «Гео Милев» 158

Ключевые слова: *двухфакторная аутентификация, Active Directory, LDAP, MFA, операционная система, телекоммуникационная сеть.*

Аннотация: *В ходе исследования был разработан метод обеспечения двухфакторной аутентификации в операционных системах, работающих с сервисами аутентификации с централизованными базами данных учетных записей в телекоммуникационных сетях.*

Работа посвящена разработке метода интеграции двухфакторной аутентификации в операционные системы путем интеграции второго фактора в централизованную базу учетных записей.

В работе описана схема процесса аутентификации с использованием дополнительного компонента, высокоуровневая схема взаимодействия модулей системы, реализующая предложенный метод, диаграмма последовательности взаимодействия модулей при регистрации пользователя, процесс аутентификации с использованием предложенного метода.

Метод основан на инъекции OTP непосредственно в сервис аутентификации с централизованной базой данных учетных записей.

Разработанная система состоит из 9 взаимосвязанных модулей, из которых 7 относятся непосредственно к системе и 2 дополнительных блока (пользователь и сервис).