THE ANNALS OF "DUNĂREA DE JOS" UNIVERSITY OF GALATI
FASCICLE III, 2022, VOL. 45, NO. 1, ISSN 2344-4738, ISSN-L 1221-454X
ELECTROTECHNICS, ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS
Article DOI: https://doi.org/10.35219/eeaci.2022.1.02

HYBRID METHODS OF AUTHENTICATION IN NETWORK SECURITY

Georgiana Crihan[1], Marian Crăciun[2], Luminița Dumitriu[3]

[1] "Dunărea de Jos" University, Faculty of Automation, Computer Sciences, Electronics and Electrical Engineering, Științei Street no.2, 800210, Galați, Romania (georgian.crihan@ugal.ro)
[2, 3] "Dunărea de Jos" University, Faculty of Automation, Computer Sciences, Electronics and Electrical Engineering, Științei Street no.2, 800210, Galați, Romania (marian.craciun@ugal.ro, luminita.dumitriu@ugal.ro)

Abstract: In this paper, we present a comprehensive taxonomy of the most popular authentication mechanisms, the main threats, vulnerabilities, the possible types of attacks and the security issues that are associated with computer systems. Our main contribution is to analyze the architecture of the current security environment from all aspects and to make a comparative assessment of different authentication methods in order to identify and develop a scalable and reliable mechanism that must deal with multi-level security and strong authentication requirements. We propose hybrid methods of authentication, which combine and integrate biometric technologies with cryptographic asymmetric algorithms, elements that play a vital role in the field of information security and aim to resolve the shortcomings of traditional methods of authentication and enhance the level of security.

Keywords: *Security, information, authentication, biometric technologies, cryptographic algorithms*

1. INTRODUCTION

In the current security environment, where the typology of threats is diversifying due to digitalization in most fields of activity, the mechanisms of identification and authentication represent a significant problem in ensuring network information security, becoming soon a critical element in the operation of software applications and information systems, which will impose the need to quickly develop robust, adaptable, scalable and reliable defense mechanisms to mitigate the negative implications associated with cyber-attacks and privacy issues in different technologies.

Security represents the main concern in terms of ensuring a protected flow of information in a possible aggressive environment and the implementation of this goal can be achieved through the three pillars of the CIA triad - confidentiality, integrity and availability, as stated in (Boonkrong, 2021). The security model based on the CIA triad, often represented as a triangle, involves the interconnection of the three principles in a unitary system to ensure a secure IT infrastructure within an organization.

Confidentiality is the property of information, services or resources of computer systems not being available to unauthorized persons or processes. Data confidentiality can be ensured through the application of cryptographic, symmetrical or asymmetric algorithms and access control lists – ACL.

Integrity is the property of maintaining the accuracy of the information, services or resources of the information systems transmitted, processed or stored and preventing any modification in an unauthorized manner. Data integrity can be achieved by generating values of hash cryptographic functions, using access control lists – ACL, as well as implementing backup procedures and configuring appropriate redundant systems.

Availability is the property of information, services or resources of information systems being accessible only to authorized persons or processes on time, while ensuring that the system has full tolerance and balancing of tasks in the event of a security incident or disaster. To improve the availability of existing data in the system, fault-tolerant technologies can be used, such as simple virtualized or hybrid RAID storage technologies, represented by dedicated hardware devices for protection against downtime and inaccessible data, redundant sites or access control mechanisms.

The main objective of this research is to develop an analysis of the main countermeasures against attack vectors on authentication mechanisms and to identify a hybrid authentication model based on multiple authentication factors, to secure access to computer networks and achieve the confidentiality, integrity and the availability of the information.

2. TAXONOMY OF AUTHENTICATION MECHANISMS

Authentication mechanisms are the rules designated for interaction and verification that the endpoints (laptops, desktops, phones, servers, etc.) or systems use to communicate. The more the user's need to access as many applications as possible increases, the more standards and mechanisms diversify. Selecting the right authentication mechanism is essential to ensure secure operations and compatibility of use.

Authentication mechanisms are developed at various functional levels, such as network level, applications, endpoint, device and at the virtualized level, which is highlighted in the diagram below (Gamundani et al., 2018).

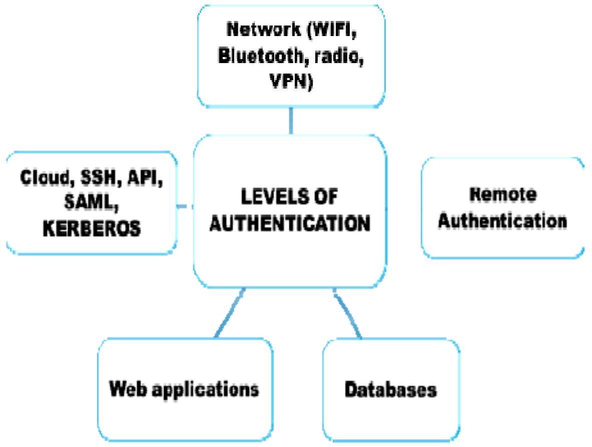

Fig. 1. Taxonomy of authetication levels

According to security experts, the implementation of an authentication process comprises, in principle, one of the three main factors, namely "Something you know", "Something you have", "Something you are" (Boonkrong, 2021).

The first authentication factor "Something you know" is based on the user entering a stored item in the system to prove their identity, a good example of this being a password, a passphrase, a PIN code or the answer to a secret question, used to prove ownership of identity. Password-based authentication schemes, although the most common method of authentication, is no longer considered a very secure method. This is because they are susceptible to many types of attacks, such as password guessing and password dictionary attack. An alternative to confidentiality and enhancing security in using unique passwords are the cryptographic hashes functions MD5, SHA 256, SHA 512, Tiger 128 and the salting techniques (Aumasson et al., 2014), as presented in the table below:

The second authentication factor *"Something you have"* requires the user to have a physical object, such as a digital certificate, digital signature, smart card or an authentication hard/soft token.

Table.1. Implementation of salting and hashing functions

Salting password	**Criptographic hash function SHA 256**	**Criptographic hash function SHA 512**	**Criptographic hash function Tiger 128**
Information	83A36AB3779F4BCBC4B677D9C749F50DEBFBE19FFC33BDFC668B1E592789E680	B3248F21D6B838390D7C3031D11AD2C09EFD2DDB3B3CCF99330A845104850EB3C63C3BF2BBC091F30AC3B34CFCD571F53844DD7FE737E9CA6D99179CFAFDAEA0	807B40B5C37304792E1BAAA24431A0D3
Information + GSevx	18C2DF94091CCAF8D39E5CCF76D05BFB1B001AF77CD4354CFCAA44FCFD9F2B97	E3E034C387B74AAFBECDE87621FF4BB0E7A368EEF1CD8CD0351A36F2FABB5B72E7219615074C3B85F87F298FBB8665C32A2DFE8C28AED8999882A0473DEC50FF	DF7982BE93B4D270156062FDB97D6CE8
Information + MNeo	A4BE84A189DE486922625C6C3F36EEC29482A3A1910B92DA45F95AE71B5DCDD3	C84ABBF5BB7C79AAD1181AFF40E677B199CDE6311D4FE48C130CE2828036A83D72A28DF7EAF505C0459D385C06048D75320354230167C61AE7F96A1EA3022B4B	940CF43FC14D9EE6177EBA0A690C1FDD

The main advantage of using an authentication token, either synchronous or asynchronous, is that the user's password changes each time he logs in. This method is known as a unique time-based password or TOTP for the synchronous symbol and a unique hash-based password or HOTP for the asynchronous symbol, both of which substantially reduce the risk of passwords being guessed by attackers (Mayes and Markantonakis, 2017). This form of human authentication removes the problem of forgetting something you know, but they are vulnerable due to the possibility that they may be lost or stolen, cloned or copied, which creates a significant security breach in a network.

The third factor *"Something you are"* is represented by the biometric authentication that works by comparing the real characteristics of the user with the data stored in a database to determine the veracity of the applicant's features. Biometric elements commonly used for authentication purposes are based on the two main categories, as follows (Li and Jain, 2015):

1. *Physiological biometrics* is the verification of a person's physiological characteristics such as fingerprint, face, palm, hand geometry, ear, retina, iris, brainwave and odour techniques.

2. *Behavioral biometrics* consists of checking a person's behavioral characteristics such as voice, handwritten signature, social media usage pattern, typing pattern (formerly known as keystroke dynamics), heartbeat, and gait pattern (or gait).

However, only the fingerprint, retina and iris are considered truly unique elements of authentication. With the implementation of the concept of digitization in the main fields of activity of society, the typology of biometric authentication methods have diversified, in the sense that new methods have emerged, such as signature dynamics and typing model (formerly known as keystroke dynamics)(Nirmal et al., 2022).

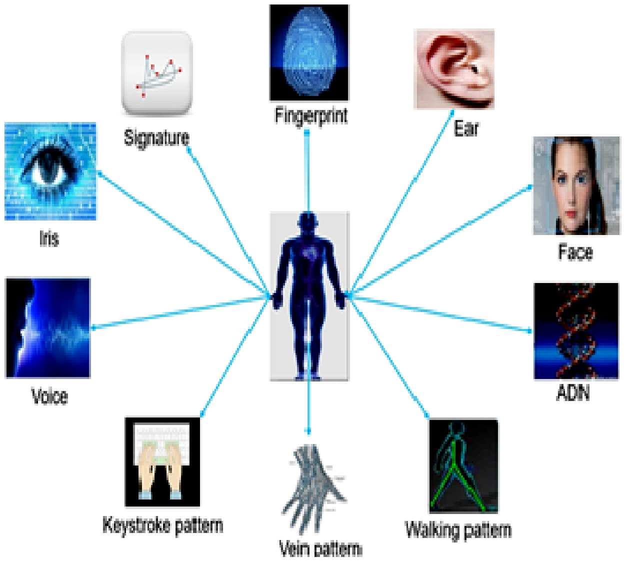

Fig. 2. Taxonomy of biometric authentication mechanisms (Jain et al., 2008)

Although biometric methods have grown exponentially, there are a few concerns about ensuring the security and confidentiality of information conveyed, regarding the vulnerabilities of the biometric databases and the cross-matching process, where the same biometric features are used for authentication in all systems and networks and are exposed to credential theft attack. This implies that if an attacker obtains a person's biometric information, they may try to use that information in a biometric authentication process and other applications or systems, a situation known as cross-matching.

3. ATTACK VECTORS

Analyzing the authentication process from the security point of view, there are three critical points that can make it vulnerable. When the user enters the access credentials, they could be attacked by a script or a potential attacker. Similarly, when access credentials are transmitted over a communications channel: wire, radio, wireless, they could be intercepted by a potential attacker. Finally, when access credentials are compared to database entries, they could be modified to achieve successful penetration.

Taking into account these three critical points, we focus on presenting the main types of attacks on authentication mechanisms, correlate with the affected security objectives and we proposed a series of countermeasures that could be implemented to defend against this attacks and to protect the systems.

Potential threats to authentication	Affected security objectives	Countermeasures
Default passwords	Confidentiality	Use unique authentication password Force users to change their default passwords through security policy settings
Password guessing	Confidentiality	Use passwords with a high level of entropy Avoid the use of previous passwords
Theft of credential access	Confidentiality	Use different authentication passwords for different accounts Apply multi-factor authentication (2FA/MFA) Use of CAPTCHA mechanisms
Dictionary attacks	Integrity	Use of salting defense techniques
Replay attacks	Integrity	Use of OTP (Example: Lamport Schema – one-time password generation scheme) Application of a challenge and response mechanism
Exhaustive searches	Integrity	Use authentication passwords with a high level of entropy Implementation of network security policies Limit the number of attempts in case of user authentication
Man-in-the-Middle	Confidentiality Integrity	Use of asymmetric or symmetric encryption mechanisms Use a Virtual Private Network (VPN)
Impersonation /masquerade/ cloning	Confidentiality	Apply multi-factor authentication (2FA/MFA) Develop and implement security policies
SQL Injection	Integrity	Apply multi-factor authentication (2FA/MFA) Use cryptographic hash functions for passwords Use protection tools such as web firewall

Social engineering	Availability	Raise user awareness Implement security policies in networks Adopt the concept of defense in depth by implementing procedural techniques on security levels
Denial of Services	Availability Non - repudiation	Create access control lists Access based on digital signature
Brute force attacks	Confidentiality	Use unique and complex authentication passwords Block accounts after a limited number of failed authentication attempts Apply multi-factor authentication (2FA/MFA) Use encryption mechanisms
Phishing	Availability	Use unique and complex authentication passwords Using SSL certificates for websites Use a Virtual Private Network (VPN)
Malware	Availability	Implement an "Application Whitelisting" mechanism Log monitoring using the Security Incident and Event Management (SIEM) solution Develop and implement security policies
APT - Advanced Persistent Threat	Availability	Use protection tools such as IDS/IPS, NGFW-Next Generation Firewall Use a Virtual Private Network (VPN)

Fig.3 Measures to counteract attack vectors (Cyber defense mechanisms, 2021)

4. HYBRID METHODS OF AUTHENTICATION

The main objective of authentication mechanisms is to ensure the protection of information against unauthorized access to any computer network or security system. Single-factor authentication proved to be vulnerable to attack vectors, and to prevent these attacks, a mature, high-security authentication scheme is needed to support the dynamic profile of users in various applications. In this respect, the level of protection for the access control mechanism increases exponentially when two or more factors are applied as part of the identity verification process and a hybrid authentication method is adopted.

To implement an efficient hybrid authentication method in a system, it is necessary to have a SWOT analysis, so that a development plan can be elaborated in which to take into account its strengths, eliminate the weaknesses, to exploit effectively the opportunities that have arisen and that allow counteracting the possible threats.

Table. 2. Analysis of authentication methods

STRENGTHS	**WEAKNESSES**
1.Establishing the user identity trying to access a system 2.Ensuring the protection of information against unauthorized access 3.Ensuring control of access to information resources of systems 4.Simplifying the authentication process by adopting innovative mechanisms such as biometrics, cryptographic algorithms, artificial intelligence, One Time Password, compared to classical password-based methods	1. Insufficient development of communications and IT infrastructure 2. Use of unprotected data channels 3. The implementation of hardware / software for additional security is costly in the process of acquisition and maintenance 4. Addiction to hardware and software can cause inactivity due to technical malfunctions 5. Manipulation of the human factor through social engineering techniques 6.Security policies that are not in line with current operational requirements.
OPPORTUNITIES	**THREATS**
1. Reducing the losses caused by security incidents through unauthorized access to information resources 2. Digitization of activities in various fields of activity through the implementation of new information technologies 3.Monitoring and auditing of events in computer systems and networks 4. Educating staff on computer security issues 5.Raising users' awareness of the need to secure online information	1.Diversification and complexity of attack vectors in the current security environment 2. Lack of security updates for operating systems and software applications may cause security breaches 3.Theft of credentials access and unauthorized intrusion into the system 4. The superficiality of the human factor in auditing logs and monitoring network events 5. Natural disasters, human intervention (sabotage, vandalism) and emergencies (fires, explosions) that affect the availability of information systems.

The multi-factor hybrid authentication mechanism can be seen as an extension of two-factor authentication and can increase the level of security for access control mechanisms due to the higher number of factors required to verify a person. As the name suggests, multi-factor hybrid authentication is an authentication process that uses two or more authentication factors which can include the factor - something you know, the factor - something you have, the factor - something you are. It is now considered a de facto standard for any system that requires strong security.

To be able to use a secure authentication scheme to ensure the confidentiality and integrity of information in the authentication process and to counteract various types of attacks, a several cryptographic algorithms can be applied, as presented in fig. 4 (Masdari and Ahmadzadeh, 2016). Also a viable alternative in supplementing security measures within the authentication mechanisms is the implementation of the following relatively new factors: the time factor that authenticates a person based on the assumption that their connection behavior takes place within a well-defined time frame and the location factor that authenticates a person based on their physical location, generated especially by IP address or GPS technology (Halak, 2021).

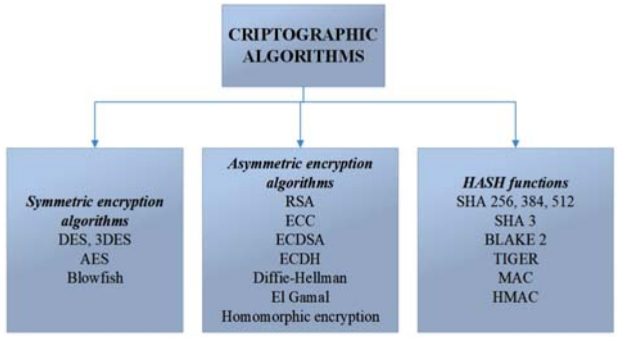

Fig.4 Improving authentication through cryptographic algorithms

In our project, we propose the implementation of a modern type of asymmetric encryption algorithm, such as fully homomorphic encryption algorithm BGV (Brakerski-Gentry-Vaikuntantan), in order to protect biometric templates, used to identify and authenticate a user according to data protection legislation such as the European's Union General Data Protection Regulation (GDPR), which provides strict guidelines for the This encryption algorithm, defined by polynomial rings use a public key for encryption and a private key for decryption and ensure the protection of sensitive data in computational tasks with multiple participants. It allows us to perform different operations on the encrypted data itself without having to decrypt it.

As stated in (Acar et al., 2019), the algorithm of encryption comprises the following operations:

a) Key generation

This probabilistic algorithm takes into consideration two inputs, security parameter λ, a number that represents the security level of the algorithm and auxiliary input α, and outputs a key triple (*pk, sk, ek*), where *pk* is the public key used for encryption, *sk* is the secret key used for decryption and *ek* is the key used for evaluation. While sk should be kept private for sensitive data, *pk* and *ek* can be shared without affecting the encryption algorithm.

The secret key *sk* is generated as a random polynom, whereas the public key *pk* is a pair of polynomials *(pk$_1$, pk$_2$)*, calculated as follows:

$$pk_1 = [-1(a * sk + e)]_q$$
$$pk_2 = a \tag{1}$$

b) Encryption

This algorithm takes as input a message *m* to be encrypted, a public key *pk* and outputs a cipher text *c*, as represented below:

$$c_1 = [pk_1 * u + e_1 + \Delta M]_q$$
$$c_2 = [pk_2 * u + e_2]_q \tag{2}$$

Where Δ is used to scale the message and $\Delta = \frac{q}{t}$

c) *Evaluation*

During this step, the evaluation key *ek* is taken as input and produces an evaluation output. This step is represented by two main homomorphic operations: addition and multiplication. Algebraically, they can be expressed as follows:

$$EvalAdd(c^1, c^2) = ([c_1^1 + c_1^2]_{q1}, [c_2^1 + c_2^2]_{q2}) = (c_1^3, c_2^3) = c^3$$
$$EvalMult(c^1, c^2) = ([c_1^1 * c_1^2]_{q1}, [c_1^1 * c_2^2 + c_2^1 * c_1^2]_{q1}, [c_2^1 * c_2^2]_{q1}) \tag{3}$$

d) Decryption

This deterministic algorithm takes a cipher text to decrypt, a private key *sk* and outputs the plaintext *m*.

$$M = [\frac{t[c_1 + c_2 * sk]_q}{q}]_t \tag{4}$$

According to NIST 800-63B standard and the levels of authentication provided (Grassi et al., 2017), we highlighted the possibilities of designing and implementing the hybrid authentication solution using existing methods depending on the operational requirements of the systems. An imperative requirement, mentioned in the standard below is a cryptographically secure communication channel between the two entities - the user and the service provider to help maintain the confidentiality of user credentials used for authentication and the re-authentication process that must be performed periodically at a regular interval of time regardless of the user's activity.

Now if we look into fig. 5, it is clear that the hybrid methods of authentication, corresponding to the highest level of protection – AAL3 are among the most robust factors of authentication, that improve the security strength. These methods are mainly used in institutions that require strict measures to control physical and logical access, especially in the military domain and governmental institutions where the necessity to assure confidentiality, integrity and availability of information is an essential task.

Authentication method	Level of access according to NIST 800-63B	Attack Vectors	Level of protection
Password	AAL1	Man-in-the-Middle, Phishing, Dictionary attack, Theft of credential access, Replay attack, Social engineering	Low
Pattern-based authentication	AAL1	Man-in-the-Middle, Phishing, Social engineering, SQL Injection	Low
Token OTP	AAL1	Man-in-the-Middle, Criptographic attacks, Compromising cryptographic keys	Low
FIDO security key	AAL2		Medium
Criptographic algorithms/ PKI certificates	AAL2		Medium
Pattern-based authentication + password	AAL2	Man-in-the-Middle, Denial of Services, Malware, SQL Injection, Social engineering, Brute force attacks, Compromising cryptographic keys	Medium
OTP authentication+ biometric methods	AAL2		Medium
FIDO security key + biometric methods	AAL3	Criptographic attacks, Compromising cryptographic keys, APT - Advanced Persistent Threat	High
OTP hardware authentication + password	AAL3		High
Criptographic algorithm + password	AAL3		High
OTP authentication + cryptographic algorithm	AAL3		High

Fig.5 Overview of authentication methods related to assurance levels [12]

It is worth pointing out that biometric recognition and cryptographic algorithms are among the best factors used to provide secure and reliable authentication in the user authentication process.

5. CONCLUSION AND FUTURE WORK

In this research, an assessment of the current security environment is presented, in which the continuous development of attack vectors acquires new valences, that are undetectable and difficult to neutralize, requiring the need to implement additional solutions to secure access to a network in order to ensure the confidentiality, integrity and availability of information.

We propose the implementation of an optimized authentication system that combine two or more authentication factors, such as the use of biometric recognition features and fully homomorphic encryption algorithm BGV (Brakerski-Gentry-Vaikuntantan), two strong factors of authentication with a high level of protection, to reduce the effect of emerging attacks and maximize security.

Thus, one of the future directions of development would be the design, implementation and evaluation of the technical solution of an original hybrid network authentication mechanism by combining biometric methods based on iris and fingerprint with asymmetric encryption algorithms, to improve the overall security and accuracy of user network authentication.

REFERENCES

Acar, A., Aksu, H., Uluagac, A.S., Conti, M., 2019, A Survey on Homomorphic Encryption Schemes: Theory and Implementation, *ACM Computing Surveys*, Vol. 51, No. 4, Article 79, pp. 1–35.

Aumasson, J.-P., Meier, W., Phan, R.C.-W., Henzen, L., 2014, *The hash function BLAKE, information security and cryptography*, Springer Berlin Heidelberg, Berlin

Boonkrong, S., 2021. *Authentication and access control: practical cryptography methods and tools,* Apress, Berkeley, Thailand

Gautam, K. Dinesh, K.S., Nguyen Ha Huy, C.*, Cyber defense mechanisms: security, privacy, and challenges*, CRC Press, 2021

Gamundani, A.M., Phillips, A., Muyingi, H.N., 2018, *An overview of potential authentication threats and attacks on Internet of Things (IoT): a focus on smart home applications*, IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)., IEEE, Halifax, NS, Canada, pp. 50–57

Grassi, P.A., Fenton, J.L., Newton, E.M., Perlner, R.A., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz, N.B., Danker, J.M., Choong, Y.-Y., Greene, K.K., Theofanos, M.F., 2017, *Digital identity guidelines: authentication and lifecycle management,* (No. NIST SP 800-63b), National Institute of Standards and Technology, Gaithersburg, MD

Gupta, B.B., Perez, G.M., Agrawal, D.P., Gupta, D. (Eds.), 2020, *Handbook of computer networks and cyber security: principles and paradigms,* Springer International Publishing

Halak, B. (Ed.), 2021, *Authentication of embedded devices: technologies, protocols and emerging applications*. Springer International Publishing, Springer International Publishing

Jain, A.K., Flynn, P., Ross, A.A. (Eds.), 2008, *Handbook of biometrics*, Springer, New York

Li, S.Z., Jain, A.K. (Eds.), 2015*, Encyclopedia of biometrics,* Springer US, Boston

Masdari, M., Ahmadzadeh, S., 2016, Comprehensive analysis of the authentication methods in wireless body area networks: Authentication methods in wireless body area networks, *Security and communication networks,* Vol. 9, no. 17, pp. 4777–4803

Mayes, K., Markantonakis, K. (Eds.), 2017, S*mart cards, tokens, security and applications*, Springer International Publishing, U.K.

Nirmal, J.R., Kiran, R.B., Hemamalini, V., 2022, *Improvised multi-factor user authentication mechanism using defense in depth strategy with integration of passphrase and keystroke dynamics*, Materials Today: Proceedings 62, pp. 4837–4843.