DOI: http://doi.org/10.25728/cs.2022.3.4

ASSESSMENT OF OPERATOR AUTHENTICATION METHODS IN INDUSTRIAL CONTROL SYSTEMS[1]

V.G. Promyslov[1], K.V. Semenkov[2], N.E. Mengazetdinov[3]

Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia

[1]✉ vp@ipu.ru, [2]✉ semenkovk@ipu.ru , [3]✉ mengazne@mail.ru

Abstract. This paper considers the authentication of operators in instrumentation and control (I&C) systems for industrial facilities. The main emphasis is on such systems for critical facilities, on an example of nuclear power plants (NPPs). Authentication methods known for public information systems (password, token, and biometrics) are surveyed, and their applicability in typical working conditions of an I&C system operator is analyzed. The analysis includes experimental testing of password and biometric authentication methods and an expert assessment of their advantages and disadvantages for I&C systems. According to the testing results, all the methods under consideration have somewhat worse values of the false rejection rate (FRR) compared with the known characteristics from available sources. The best results are shown by biometric identification by the face geometry. However, the percentage of FRR for this method is significant, which can affect the availability of the control function for a legitimate operator. As concluded, a promising approach for industrial control systems is to implement multi-factor authentication: token or password protection for blocking authentication jointly with biometric authentication by the face geometry with a non-blocking security policy.

Keywords: authentication, biometrics, token, password, industrial control system, I&C, operator.

INTRODUCTION

Modern industrial enterprises, including hazardous ones (e.g., nuclear power plants (NPPs), transport and chemical industry enterprises, etc.) depend on digital automated control systems. The control loop of such systems often includes a human operator, who exerts an impact on the controlled facility and its control system through the computers within an instrumentation and control (I&C) system.

In I&C systems, authentication arises when allowing a trusted operator to control an industrial facility (particularly when granting some action rights to the operator). In information technology, this procedure is commonly referred to as authorization. Authentication can be defined as "actions to verify the genuine character of an access subject and (or) access object as well as verify that the access identifier and authentication information presented belongs to the access subject and (or) access object." [1].

The authenticating subject performs verification by matching some personal identifier (e.g., a shared secret) negotiated in advance during user registration. This can be done to create trusted communications between parties or grant access rights to communication and computing resources of the system during authorization.

Unauthorized operator actions can violate the basic information security properties (integrity, availability, and confidentiality) and, moreover, cause economic damage or harm to human health. An additional problem is to trace control decisions on the facility, i.e., ensure the non-repudiation of previously performed actions. In general, these problems force using more formal authentication methods even for routine operations in I&C systems.

The authentication of operators in I&C systems for critical facilities has peculiarities associated with the

[1] This work (Sections 2.3–2.5) was supported in part by the Russian Foundation for Basic Research, project no. 19-29-06044.

controlled facility and information security policy [2]. They distinguish operator authentication in I&C systems from user authentication in public information systems. The main peculiarities are as follows:

- A demilitarized zone to access the facility reduces the threat from an external intruder in personnel authentication. However, it does not eliminate the threat posed by an internal intruder: a person without operator authority but admitted to the zone may attempt to access operator control functions.
- The priority of accessibility over other information security properties applies strong requirements to the duration of the authentication process and the probability of first-kind errors (the percentage of the false rejection rate, FRR).
- Stressful situations in the operator's work (e.g., an industrial accident) may cause the person to forget obvious things, and his functional and external characteristics may change (trembling hands, another voice timbre, perspiration, etc.).
- Authentication complication may occur due to some changes in the environment. Such complication neither destroys the facility nor immediately violates functions of the I&C system and the facility; but it causes inconvenience to the operator (e.g., partial failure of the lighting system, smoke, activation of the firefighting system, earthquake, etc.).

Like for conventional information systems, authentication problems for I&C systems include operator (user) authentication on the computer (digital device) and computer authentication. For public information systems, computer authentication is well developed [3, 4]. In I&C systems with controllers and industrial computers, protocols with weak authentication mechanisms or even without any authentication are often used. However, reliable computer-to-computer authentication in I&C systems is a problem of particular implementations rather than of scientific study.

User authentication protocols are much less secure than computer-to-computer authentication protocols because they deal with people and their limited capabilities and weaknesses [5]. In information security, people are often the weakest element in protection.

In this paper, we select and validate authentication methods and protocols with application to operator authentication in I&C systems. We analyze the main user authentication methods and protocols and experimentally test them considering the peculiarities of industrial facilities and information security policies. As an example of I&C systems, we choose the upper-unit control system for NPPs that was developed at the Trapeznikov Institute of Control Sciences RAS [6].

The experimental studies below proceed from the assumption that the operator's working conditions at the facility and the exposure of people and equipment to physical fields are close to the normal office environment. This assumption may be violated for some industrial facilities, but such factors go beyond the scope of the paper.

1. AUTHENTICATION METHODS AND PROTOCOLS IN INDUSTRIAL CONTROL SYSTEMS

We consider the main user authentication methods and compare their effectiveness with application to I&C systems.

User authentication methods can be divided into classes based on three questions [7]:

– What do you know?

– What do you have?

– Who are you?

Often the three authentication methods are associated with their characteristic representatives: password, token, and biometric trait. Therefore, when describing each of them, we will refer to their particular implementations. In all cases, the object of authentication is a person.

1.1. Password authentication methods

A password is a secret word known to the user and possibly to the computer on which the user undergoes authentication. This word is related to the key by which authentication occurs. In theory, password authentication can be very strong. For example, in the case of the extended encryption standard [8], the maximum key length is 256 bits, and it would take an intruder over 10^{76} attempts on average to guess the key (too long now and in the foreseeable future). If the password and the authentication key are directly related, a password of comparable length is needed to ensure high reliability of the key, which is too much for a human to remember. In practice, this key is stored, e.g., in a file protected by a shorter password. The main vulnerability of password protection is that a memorable password can be guessed or found by an intruder [5, 9], whereas a long, random, and changeable password is difficult to remember. (Therefore, it can be written down and stored in plaintext.) According to [10, 11], about 20% of users apply no more than five thousand passwords out of all possible combinations. Consequently, the search space for hacking a system is reduced, and an intruder can often focus on these five thousand combinations.

The drawbacks of password authentication can be avoided by choosing other classes of methods in which a person becomes not the subject but object of authentication. These are token-based and biometric methods.

1.2. Authentication methods using tokens

A token is a physical device that performs or assists authentication. The term also refers to software tokens issued to the user after successful authentication as the key to access services. Tokens can be passive or active (e.g., providing one-time access codes or changing synchronously with the host master, etc.). Token security is ensured by various protection means, such as a token case or special hardware that disables the token when compromised or if the number of failed authentication attempts exceeds a given threshold.

In general, a token can be considered a secret similar to a password, except that it is machine-generated or machine-stored, so it can be longer, more random, and possibly change over time.

1.3. Biometric methods

For a person as a user, biometrics is the most convenient and easy way to authenticate: it extends natural ways of establishing identity.

Biometrics, or biometric personal data, is some measurable individual characteristic of the human body that can be used for user authentication. The standard [1] defines biometric personal data as information characterizing the physiological and biological traits of a person to establish his or her identity.

Biometrics is intended to link the authenticator (trait) and the owner of the authentication trait inseparably. In the case of passwords and tokens, this cannot be done in principle because both can be borrowed or stolen. Such an inseparable linkage between the authentication trait and the trait holder would ensure non-repudiation. (With this property, there is such evidence of given actions that the parties involved cannot subsequently reject the transaction as unauthorized or claim that they did not perform those actions.) However, biometric traits, like passwords, can be copied or forged at some cost and used to gain unauthorized access. In general, biometrics at the current technological level does not guarantee non-repudiation.

Biometric authentication data are usually typified into physical and behavioral. The physical type includes biometrics based on stable body traits (fingerprints, face, iris, hand shape, etc.). The behavioral type includes skills acquired through training, such as handwriting signature, keyboarding dynamics, and gait. Being the product of learned behavior, voice is usually typified as behavioral biometrics [12–14].

Biometric authentication, like other methods, may cause errors [15], but the user's attitude to errors varies for different authentication methods. The user may forget or incorrectly enter a password and may lose a token. Such situations are uncomfortable, but the user understands his or her fault. In the case of biometric authentication errors, the user is not at fault and cannot fix the problem independently.

A biometric error can occur for different reasons:

– a dirty scanner,

– poor lighting,

– the system initially remembered the wrong template for comparison,

– the system poorly adapts to changes in the environment (cold, rain, sun glare, dryness, etc.) or to natural changes in the user's biometric traits (hairstyle, beard, cut finger, etc.).

A recent example of biometrics problems is the need to wear masks due to the pandemic.

Detailed requirements for biometric authentication methods were presented in regulatory documents, e.g., the standard [16].

1.4. Authentication protocols and their application in I&C systems

For the user authentication problem, we consider the most general authentication protocol [17]. It establishes the exchange rules to ensure authentication based on bilaterally negotiated secret information.

For public information systems, widespread variants of the authentication protocol are challenge-response protocols [18]. They underlie authentication protocols in Unix with PAM modules [19] and MS Windows [20] and can be used to authenticate I&C system operators based on these operating systems. According to our experience, this protocol has limited use for password authentication due to availability requirements and operator's scenarios when performing critical functions of the system. Nevertheless, the protocol can be applied, e.g., to access the reprogramming function of a digital device.

In real systems, authentication protocols often combine different authentication methods [21] to achieve a high level of protection and its echeloning (multifactor authentication). In this case, the logical AND algorithm is implemented: all authentication methods must be successfully passed to complete. Currently, the vast majority of multifactor authentication approaches involve the "physical token–password" pair [22, 23]. The password and biometric identifier are rarely combined: biometrics is usually chosen for convenience to avoid remembering the password.

Three-factor authentication has not found wide application, although such implementation may be needed for accessing functions with a high level of protection. Table 1 summarizes the main advantages and disadvantages of some multifactor authentication methods. Also, an expert assessment of their suitability for operator authentication in I&C systems is presented on a qualitative scale (bad–satisfactory–good).

Basic authentication protocols are easily modified for multifactor authentication. However, for implementing a security policy with high availability requirements, typical for I&C systems, introducing an additional transaction and complexity in the protocol may cause adverse effects.

For I&C systems and other objects with availability priority, multifactor authentication can be implemented according to the logical OR scenario. In this case, authentication is considered complete if at least one of the multifactor authentication methods is successfully passed.

2. AUTHENTICATION METHODS: ANALYSIS AND COMPARISON

2.1. Principles of comparison

We compare the three main authentication methods by their applicability for I&C systems using the following features: strength, advantages (convenience) and drawbacks, and the quality of identification. The comparative analysis below is mostly qualitative and largely rests on practical (expert) experience, which may have a subjective nature. The set of indicators is taken from the paper [7].

Table 2 summarizes the main attributes of the three authentication methods.

Table 1

Comparison of multifactor user authentication methods for stronger protection in I&C systems

A combination of authentication methods	Advantages	Drawbacks	Example	Assessed applicability for I&C systems
"What do you know?" + "What do you have?"	Losing a token does not immediately compromise it: the token is protected by a password	The user must have a token and remember the password	Bank card + PIN	Satisfactory
"What do you have?" + "Who are you?"	Losing a token does not immediately compromise it: the token is protected by the owner's uniqueness	The user must have a token. May lead to false authentication rejection due to imperfect biometric methods	Pass with chip and photo	Good
"What do you know?" + "Who are you?"	User ID spoofing (using a double) will not result in false authentication	May lead to false authentication rejection due to imperfect biometric methods	Password + fingerprint sensor on the computer	Satisfactory
"What do you know?" + "What do you have?" + "Who are you?"	All three methods work sequentially	The user must have a token and remember the password. May lead to false authentication rejection due to imperfect biometric methods	Authentication for accessing a critical facility, including a chipped badge with a photo at the entrance, a biometric fingerprint scanner for accessing the room, and a password for computer access	Bad

Table 2

Three basic user authentication methods and their attributes

Authentication methods	What do you know?	What do you have?	Who are you?
Implementation	Password	Token	Biometrics
Authentication basis	Knowing the secret	Owning the proper object	Having traits of the subject
Protection type	Keeping the secret	Physical security	Uniqueness of the subject
Examples of vulnerabilities	Can be peeked or guessed	Can be lost or stolen	Can be forged; difficult to change when compromised

2.2 Practical entropy of the key

Comparing the strength of different authentication methods is not an easy task: the protocol key may have different relationships to the initial data depending on the particular implementation of an authentication method. For example, in password authentication, a key may simply be a stored copy of a password, its hash code, or validation values that depend on passwords but cannot be directly used by an intruder to authenticate. In other authentication methods, some value from a token or biometric device may be used instead of a password.

Therefore, to assess the strength of authentication methods, we adopt an entropy-based measure of the key that can be directly obtained from the initial data (a password, information stored in a token, or biometric data). According to the studies of leading IT companies with a large volume of personal data (Yahoo and Google) [5], the entropy of the key based on passwords is 10–20 bits. As noted, using hash codes reduces the entropy of the key closer to the left limit (10 bits) since the hash code is optimized to provide fast performance at the cost of lower strength of the key. Although, e.g., implementations of *Secure Hash Algorithm* 1 (SHA1) [24] are configurable and can be very strong.

Early studies [5] demonstrated that biometric and password protection methods have approximately the same entropy of the key and, consequently, the same strength. However, according to more recent results, biometrics ensures a degree of protection 2–3 three times better than password authentication [25].

To our knowledge, strength was not examined for password operator authentication methods in I&C systems. However, it seems reasonable to take the strength of passwords closer to the lower limit (simple passwords). The security policy of an industrial facility can and must contain password strength requirements and a password management procedure: a too complex (strong) password is impossible to use due to system availability requirements and stressful situations in the operator's work.

The key obtained from the data and contained in the token can have a very large entropy when using algorithms similar to computer-to-computer authentication. For example, the entropy of the key reached 128 bits in [26]. However, it is necessary to consider the probability of token theft, which can be significant, especially under malicious intent.

2.3. The quality of identification: main indices

Traditionally two indices are used to assess the quality of identification: *the False Rejection Rate* (FRR) and *the False Acceptance Rate* (FAR).

The first rate is the probability of denying access to an authorized person. The second rate is the probability of making a false authentication. The better the system is, the lower the FRR value will be under the same FAR values. FAR makes sense only for biometric authentication: for other authentication methods, its value reflects human capabilities (typing and memorizing the password) or the reliability of hardware implementation.

Any authentication method has some share of errors due to hardware failures (e.g., a token reader or keypad). As practice shows, this share is negligible. The quality of biometric authentication is the most unstable characteristic since it depends heavily on the person. Table 3 contains typical errors for different biometric authentication methods available in the literature. Typical errors demonstrate only a trend: the comparison of different biometric authentication implementations and algorithms is beyond the scope of this paper.

Table 3

Typical biometric authentication errors

Type of biometrics	FAR	FRR	Sample size [27]	Source
Fingerprint recognition	10^{-3}	10^{-2}	$5 \cdot 10^6$	[27]
Facial recognition	0.058		$12 \cdot 10^6$	[27]
Retinal recognition	0.059		$500 \cdot 10^3$	[27]

We conducted additional testing to investigate the practical aspects of the applicability of commercially available biometric authentication devices for I&C system operators. During the testing, we simulated some typical working conditions of the I&C system operator. The results are presented in subsection 3.4.

2.4. The applicability of authentication methods for I&C system operators: Practical testing

We tested password authentication and some implementations of biometric authentication methods in typical working scenarios for I&C system operators at an industrial facility. Token-based authentication was not tested: its properties are determined by the capabilities inherent in the design and manufacture of a token, and they are supposed stable during operation.

Table 4 shows the commercial devices used and the type of biometric authentication available on the device. At the time of writing the paper, these devices were officially supplied to the Russian Federation without license restrictions. For testing biometric authentication methods, we chose devices and algorithms available to the mass consumer and used for authentication in mobile devices. For password authentication tests, typical PC keyboards used at the workplaces of I&C system operators were used. According to our experience, mass products are mainly adopted when implementing technical security measures for industrial systems.

Table 4

Devices used in testing

Device	Authentication type
HONOR 10. Android ver. 10	Fingerprint recognition; facial recognition
MI 5S Plus. Android ver. 8. MIUI Global ver. 10.2	Fingerprint recognition
PC with a membrane keyboard	Password protection

At least 50 tests were conducted for each method. Each test involved a group of two testers: on the command of one tester, the other (operator) attempted to authenticate using an authentication method.

During testing, the testers in the group periodically exchanged their roles. In each test, two measurements were performed: the time to authenticate and the number of attempts to do it. The testing was conducted both in normal working conditions and under complication hindering authentication; see Table 5.

Table 5

Types of complication during testing

Complication no.	Description
1	Warmed hands
2	Pouch on the sensor
3	Thin-layer water on the finger
4	Cooled finger
5	Facial mask
6	Changed angle between the camera and the face
7	Changed lighting
10	Password entered while standing
11	Password entered with gloves on
12	Password entered "blindly"
13	Password entered during physical complication (one tester nudged the other)

For password authentication methods, the password was changed after every ten tests according to the selected complexity level.

The testing results are shown in Table 6.

Table 6

Testing of authentication methods

Test (Working conditions)	Result	
	Maximum, minimum, and average time, s	The maximum number of attempts for successful authentication
Simple password (5 characters; dictionary word-based; normal conditions)	2.63; 1.82; 2.1	1
Simple password (5 characters; dictionary word-based; complication 8)	6.34; 2.1; 2.3	2
Simple password (5 characters; dictionary word-based; complication 9)	9.29; 1.68; 4.2	3
Simple password (5 characters; dictionary word-based; complication 10)	12.64; 2.37; 5.62	4
Simple password (5 characters; dictionary word-based; complication 11)	20.33; 2;06; 6.12	6
Complex password (at least 9 characters; capital and small letters and numbers; normal conditions)	24.5; 5.33; 9.1	3
Complex password (at least 9 characters; capital and small letters and numbers; complication 10)	11.59; 5.98; 6.6	1
Complex password (at least 9 characters; capital and small letters and numbers; complication 11)	49.03; 9.1; 12;6	3
Complex password (at least 9 characters; capital and small letters and numbers; complication 12)	95.31; 7.8; 23.4	11
Complex password (at least 9 characters; capital and small letters and numbers; complication 13)	46.39; 8.1; 24.3	4
Fingerprint (normal conditions)	3.92; 0.99; 1.44	2
Fingerprint (complication 1)	1.23; 1.09; 1.2	1
Fingerprint (complication 2)	2.69; 1.09; 1.82	3
Fingerprint (complication 3)	9.48; 1.05; 3.61	6
Fingerprint (complication 4)	3.59; .2.1; 1.7	3
Face geometry (normal conditions)	2.87; 1.85; 1.91	1
Face geometry (complication 5)	4.23; 1.7; 2.64	2
Face geometry (complication 6)	5.42; 1.64; 3.26	2
Face geometry (complication 7)	2.09; 0.99; 1.2	1

For the password method, we obtained a relatively high ($\sim 10^{-1}$) probability of denying access for an authorized person under complication. The FRR grows with increasing password complexity. Due to a high probability of errors when entering a password (especially a complex one) under complication, the operator has to enter the password twice and more for successful authentication. (In tests, this value reached 11 times.) In this case, authentication time increases by an order of magnitude, with a typical value of about two or three seconds for a simple password and about five seconds for a complex password.

Such delays may be critical for I&C systems. This can be a reason to abandon password protection in favor of tokens, biometrics, or organizational and physical authentication measures and their combinations.

Among the biometric authentication methods, the best testing results were demonstrated by facial identification. For biometric authentication methods, additional testing was conducted to determine the possibility of false authentication. None of the biometric methods allowed false authentication within the means available to the average user ($\text{FAR} = 0$). However, biometric authentication for I&C system operators is not free of second-kind errors, and these results do contradict the typical values in the previous section. The reasons can be the limited sample size and the fact that bypassing the protection systems requires knowledge of the implementation features of the particular algorithms for comparing the biometric template and, possibly, special equipment.

The FRR values for biometrics obtained in practical conditions exceed the typical ones by approximately an order of magnitude. The main reason is the presence of complication. These results should be considered when using biometric authentication methods for I&C system operators.

2.5. Authentication methods in I&C systems: Analysis of applicability

Let us analyze the main problems associated with applying each authentication method in typical working conditions of I&C system operators.

- Knowledge-based authenticators ("What do you know?") include secret information (password), which is unknown and can be roughly defined as "hidden from most people." The disadvantage is that each time secrets are used for authentication, they become less and less secret. In addition, "most people" often means "most honest people": for an intruder applying some effort (e.g., social engineering means), such information is no longer secret. I&C systems are characterized by a high level of trust between users established during personnel selection and production activities (people do common work for a long time). Therefore, an intruder penetrating an isolated team has an easier task of obtaining knowledge (particularly passwords) from other team members.
- Object authenticators ("What do you have?") are material objects (e.g., a token). Such authenticators have the same main drawback as their predecessors (physical keys). If the key is lost, anyone who finds it can bypass the protection system. In this sense, the weaknesses of object authenticators are similar to password protection: an intruder can use a lost or stolen token. As mentioned, I&C system users trust each other. In contrast to password protection, if a physical object is lost, the owner will know about it the first time he accesses it and will take measures to neutralize the threat as quickly as possible.
- Identity-based authenticators ("Who are you?") are related to one person: they are unique. This class includes all biometric authentication methods (fingerprints, eye and iris scans, voice prints or signatures). Biometric authentication has a relatively high degree of protection against copying and tampering and obviously cannot be lost [28].

Summarizing the aforesaid, we conclude that there are no ideal authentication methods: they have "inherent" drawbacks. Table 7 shows the characteristic vulnerabilities of different authentication methods with application to I&C systems. Clearly, the opportunities for attacks on the authentication system of an I&C system are unequal within a given security policy. If an enterprise has an effective intrusion detection system, and there are officials responsible for computer security, brute force attacks will be easy to detect, and appropriate measures will be taken. At the same time, attacks involving the theft of a token or password (especially the latter) are very likely, given the high degree of trust usually established between I&C system users. As we believe, I&C systems should have non-blocking protection against many attacks attempting to bypass the authentication procedure. Non-blocking protection methods are primarily intended to draw the security officer's attention to an abnormal situation, who will take appropriate measures in response to a security event.

Table 7

Compromised security properties in different authentication methods

Compromised security property	Authentication method	Example of an attack	Typical protection methods
Irrefutability	Password, token	Lost or stolen token	Personal liability of the user for loss (administrative protection measure)
	Biometrics	Fake	Multifactor authentication
Detecting compromise	Password, biometrics	Forgery, theft	Informing the user about the use of the authenticator (*last login*)
	Token		Detecting a loss by the user
User spoofing during initial identification	Password	Passing data to an unauthorized person. Default password	Personal appearance of the user. Password management policy
	Token	Passing a token to an unauthorized person	Personal appearance of the user
	Biometrics	Replacing user biometric data	

Table 7 (continued).

Compromised security property	Authentication method	Example of an attack	Typical protection methods
Data leakage when updating the identifier	Password	Passing data to an unauthorized person. Default password	Password management policy. Multifactor authentication
	Token	Passing a token to an unauthorized person	Personal appearance of the user and return of the token if it is broken but not lost
	Biometrics	Replacing user biometric data when compromised	Personal information management policy
Denial of service	Password, token, biometrics	Multiple unsuccessful attempts to block access	Non-blocking security policy with security officer notification
False authentication	Password, token, biometrics	Attack with message retransmission	The challenge-response protocol
	Password	Brute force attack	Blocking security policy under a given number of failed authentication attempts

2.6. Authentication methods for I&C systems: Qualitative analysis and comparison

Various indicators can be proposed to compare authentication methods. We consider three high-level indicators traditionally used to compare such methods [5]:

– usability,
– the ease of deployment,
– security.

For each set of high-level indicators, we choose a set of lower-level indicators. The values of all indicators in the set are assessed using the ranking scale: "good" (2), "satisfactory" (1), and "bad" (0). The value of a high-level indicator is calculated as the sum of individual indicators in the set.

Consider indicators of usability (Table 8) and the ease of deployment (Table 9Table). In turn, Table 10 presents indicators of security: what types of attacks the authentication method can prevent.

Table 8

Different authentication methods with application to I&C systems: indicators of usability

Indicator	Password	Token	Biometrics
Ease of interaction with the authentication scheme for the user	Satisfactory	Good	Satisfactory
Easy to learn: users not familiar with the method can understand and master it without much trouble	Good	Good	Satisfactory
Infrequent errors: the task to authenticate is usually completed successfully when performed by a legitimate and honest user	Satisfactory. Users are usually successful but with a weak password	Good	Satisfactory
Scalability for users: Using a scheme for hundreds of accounts does not increase the burden on the user	Bad. People often reuse passwords or create a simple uniqueness scheme for each website involving a basic password	Satisfactory. The problem of choosing one token from the set of available tokens is not always trivial	Good
Easy recovery from compromise	Good. The advantage of passwords is that they are easy to reset	Satisfactory	Bad
The need to have something at hand	Good	Bad	Good
Score:	8	8	7

Table 9

Different authentication methods with application to I&C systems: indicators of the ease of deployment

Indicator	Password	Token	Biometrics
Easy implementation of the authentication method in real systems	Good	Good	Satisfactory
Compatibility with the authentication server	Good. Authentication servers are originally designed for password-based authentication methods	Good. From the server's point of view, the key obtained from the token is indistinguishable from that obtained from the password	Satisfactory. It may be necessary to implement the protection of biometric information if stipulated by law
Compatibility with the client computer	Good. Authentication clients are originally designed for password-based authentication methods	Satisfactory. Requires support from special devices	Satisfactory. Requires support from special devices
Availability. Restrictions on use depending on the individual	Good	Good	Bad The availability of the method may vary depending on health conditions and injuries. Certain biometric authentication methods may be unavailable for people with disabilities. For I&C system operators, this may be relevant in the case of temporary personnel without proper medical selection (unlike regular operators)
Upgrade option	Satisfactory	Good (Given administrative support)	Bad. Biometrics change very slowly (voice, face) or not at all (fingerprints)
Score:	9	9	3

Table 10

Different authentication methods with application to I&C systems: indicators of security

Indicator	Password	Token	Biometrics
Resistance to observation	Bad. An attacker can impersonate a user after observing his or her authentication several times (say, 10–20). Attacks include shoulder surfing, video recording of the keyboard, recording keystroke sounds, TV images of the keyboard, etc.	Good	Good
Resistance to social engineering methods	Good. An acquaintance (or an experienced hacker) cannot impersonate a user via personal data knowledge (date of birth, names of relatives, etc.).	Good	Good
Resistance to simple guesswork	Satisfactory. Depends on password length	Good	Good
Resistance to internal attacks by actors within the computer system	Satisfactory. Depends on password length	Good	Satisfactory. Biometric methods, like passwords, have low entropy and length of the key
Score:	4	8	7

The total scores of the authentication methods over the three groups of indicators are given in Table 11. According to the analysis results, token-based authentication can be the most balanced method when used independently.

Table 11

The total scores of authentication methods over three groups of indicators

	Password	Token	Biometrics
Total score:	21	25	17

CONCLUSIONS. DISCUSSION OF THE RESULTS

As emphasized, this paper has considered the peculiarities of known authentication methods with application to I&C system operators.

The accumulated experience of using authentication methods for public information systems has been studied. According to the survey of available sources, the degrees of protection provided nowadays by each method are comparable. Note a general problem: an inconvenient authenticator is either not used or used improperly, which can cause vulnerability. In practice, if I&C system operators need to remember multiple passwords to access different workstations or perform different operations, they will choose simple passwords or passwords linked by simple logic. The enterprise security policy may impose certain requirements on passwords (e.g., length, special characters, etc.) to increase entropy. However, as we believe, such password requirements rarely increase the entropy of the key. A competent intruder can consider password restrictions imposed by the security policy when compiling the hash code tables to hack the system. Alternatively, he or she can simply spy a password: the operator will write down a complex password and carry it.

According to the experimental evidence, there is a high percentage of first-kind errors (incorrectly typed passwords) under complication, even for a fairly simple password. Therefore, when determining a password protection security policy, the effect of first-kind errors on the system availability must be considered, which automatically restricts the frequency of password changing and its complexity.

In practice, biometric authentication methods have shown first-kind errors several times worse than the theoretical ones ($\le 10^{-2}$), in typical working conditions and under operator's complication. Based on the testing results, the most promising biometric method is facial recognition. However, even this method has a high error rate, so it should not be combined with a blocking security policy. We propose using multifactor authentication where biometrics is combined with a password or a token. In the case of multifactor authentication, note that biometric and password protection have approximately the same entropy of the key. For passwords, the entropy is restricted by human memory capabilities; for biometrics, by the current hardware implementation of biometric scanners and sensors.

Using a token eliminates the problem of remembering passwords, but the user must have a physical carrier with him or her. Sometimes, this approach is inconvenient because the token can be stolen, copied, or lost.

Finally, we arrive at the following conclusion. For the authentication of I&C system operators, it is possible to build a protection system using different methods and their combinations. As a rule, I&C system operators work in the room with controlled physical access. Therefore, within the controlled security area, it is possible to establish a token-based access procedure with additional video monitoring by the security service. As we believe, a promising approach for industrial control systems is to implement multi-factor authentication: token or password protection for blocking authentication jointly with biometric authentication by the face geometry with a non-blocking security policy.

REFERENCES

1. *GOST* (State Standard) *R 58833-2020: Information Protection. Identification and Authentication. General Provisions*, 2020.
2. Iskhakov, S.Yu., Shelupanov, A.A., and Iskhakov, A.Yu., Engineering of Imitation Model of a Complex Network of Security Systems, *Proceedings of TUSR University*, 2014, vol. 32, no. 2, pp. 82–86. (In Russian.)
3. Dierks, T. and Rescorla, E., The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, 2006.
4. Conte de Leon, D., Makrakis, G.M., and Kolias, C., Cybersecurity, in *Resilient Control Architectures and Power Systems*, Rieger, C., Boring, R., Johnson, B., and McJunkin, T., Eds., IEEE, 2022, pp. 89–111. DOI: 10.1002/9781119660446.ch7.
5. Hu, G., *On Password Strength: A Survey and Analysis*, Springer International Publishing, 2018. DOI: 10.1007/978-3-319-62048-0_12.
6. Mengazetdinov, N.E., Poletykin, A.G., Promyslov, V.G., et al., *Kompleks rabot po sozdaniyu pervoi upravlyayushchei sistemy verkhnego blochnogo urovnya ASU TP DLYA AES «BUSHER» na osnove otechestvennykh tekhnologii* (Works on Creating the First Upper-Unit Control System of the I&C System for Busher NPP Based on Domestic Technologies), Moscow: Trapeznikov Institute of Control Sciences RAS, 2013. (In Russian.)
7. O'Gorman, L., Comparing Passwords, Tokens, and Biometrics for User Authentication, *Proceedings of the IEEE*, 2003, vol. 91, no. 12, pp. 2021–2040. DOI: 10.1109/JPROC.2003.819611.

8. Dworkin, M., Barker, E., Nechvatal, J., et al., *Advanced Encryption Standard* (*AES*), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, 2001. DOI: 10.6028/NIST.FIPS.197.
9. Jobusch, D.L. and Oldehoeft, A.E., A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 1, *Computers & Security*, 1989, vol. 8, iss. 7, pp. 587–604. DOI: 10.1016/0167-4048(89)90051-5.
10. The 200 Worst Passwords of 2021 Are Here and Oh My God. https://gizmodo.com/the-200-worst-passwords-of-2021-are-here-and-oh-my-god-1848073946 (Accessed March 7, 2022.)
11. Most Common Passwords of 2021. https://nordpass.com/most-common-passwords-list/ (Accessed March 7, 2022.)
12. Köhler, D., Klieme, E., Kreuseler, M., et al., Assessment of Remote Biometric Authentication Systems: Another Take on the Quest to Replace Passwords, *2021 IEEE 5th International Conference on Cryptography, Security and Privacy* (*CSP*), 2021, pp. 22–31. DOI: 10.1109/CSP51677.2021.9357504.
13. Alanezi, N.A., Alharbi, N.H., Alharthi, Z.S., and Alhazmi, O.H., POSTER: A Brief Overview of Biometrics in Cybersecurity: A Comparative Analysis, *2020 First International Conference of Smart Systems and Emerging Technologies* (*SMARTTECH*), 2020, pp. 257–258. DOI: 10.1109/SMART-TECH49988.2020.00067.
14. Antonova, V.M., Balakin, K.A., Grechishkina, N.A., and Kuznetsov, N.A., Development of an Authentication System Using Voice Verification, *Information Processes*, 2020, vol. 20, no. 1, pp. 10–21. (In Russian.)
15. Machine Learning Masters the Fingerprint to Fool Biometric Systems: https://engineering.nyu.edu/news/machine-learning-masters-fingerprint-fool-biometric-systems (Accessed July 12, 2022.)
16. *GOST* (State Standard) *R 52633.0-2006*: *Requirements for High-Security Biometric Authentication Means*, 2006.
17. Mao, W., *Modern Cryptography: Theory and Practice*, Prentice Hall, 2003.
18. Burrows, M., Abadi, M., and Needham, R.M., A Logic for Authentication, *DEC System Research Center Technical Report* no. 39, 1989.
19. Krawczyk, H., Bellare, M., and Canetti, R., HMAC: Keyed-Hashing for Message Authentication, *RFC 2104*, 1997.
20. Algorithms for Challenge/Response Authentication. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/4d1a2cb0-0951-462a-8582-121fd1afe28e (Accessed March 7, 2022.)
21. Iskhakov, A.Yu., Two-Factor Authentication System Based on QR-Codes, *IT Security (Russia)*, 2014, vol. 21, no. 3, pp. 97–101. (In Russian.)
22. Giri, D., Sherratt, R.S., Maitra, T., and Amin, R., Efficient Biometric and Password Based Mutual Authentication for Consumer USB Mass Storage Devices, *IEEE Transactions on Consumer Electronics*, 2015, vol. 61, no. 4, pp. 491–499. DOI: 10.1109/TCE.2015.7389804.
23. Razaque, K.K., Myrzabekovna, S.Y., Magbatkyzy, M., et al., Secure Password-Driven Fingerprint Biometrics Authentication, *2020 Seventh International Conference on Software Defined Systems* (*SDS*), 2020, pp. 95–99. DOI: 10.1109/SDS49854.2020.9143881.
24. Eastlake, D. and Jones, P., US Secure Hash Algorithm 1 (SHA1), *RFC 3174*, 2001.
25. Dinca, L. and Hancke, G., User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks, *Entropy*, 2017, vol. 19, no. 2. DOI: 10.3390/e19020070.
26. Fouque, P.-A., Pointcheval, D., and Zimmer, S., HMAC Is a Randomness Extractor and Applications to TLS, *Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security* (*ASIACCS'08*), Tokyo, Japan, 2008, pp. 21–32.
27. Jain, A.K., Deb, D., and Engelsma, J.J., Biometrics: Trust, but Verify, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 2021. DOI: 10.1109/TBIOM.2021.3115465.
28. Alsellami, B., Deshmukh, P.D., and Ahmed, Z.A.T., Overview of Biometric Traits, *2021 Third International Conference on Inventive Research in Computing Applications* (*ICIRCA*), 2021, pp. 807–813. DOI: 10.1109/ICIRCA51532.2021.9545069.

This paper was recommended for publication by A. O. Kalashnikov, a member of the Editorial Board.

Received May 6, 2022, and revised June 30, 2022.
Accepted July 11, 2022

Author information

Promyslov, Vitaly Georgievich. Cand. Sci. (Phys.–Math.), Trapeznikov Institute of Control Sciences, Moscow, Russia
✉ vp@ipu.ru

Semenkov, Kirill Valer'evich. Cand. Sci. (Phys.–Math.), Trapeznikov Institute of Control Sciences, Moscow, Russia
✉ semenkovk@ipu.ru

Mengazetdinov, Nadyr Enverovich. Senior Researcher, Trapeznikov Institute of Control Sciences, Moscow, Russia
✉ mengazne@mail.ru

Cite this paper

Promyslov, V.G., Semenkov, K.V., and Mengazetdinov, N.E., Assessment of Operator Authentication Methods in Industrial Control Systems. *Control Sciences* **3,** 34–45 (2022). http://doi.org/10.25728/cs.2022.3.4

Translated into English by *Alexander Yu. Mazurov*,
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com