Universal Description of Access Control Systems

Karel Burda

Brno University of Technology, Brno, Czech Republic

Abstract
Access control systems are used to control the access of people to assets. In practice, assets are either tangible (e.g. goods, cash, etc.) or data. In order to handle tangible assets, a person must physically access the space in which the assets are located (e.g. a room or a building). Access control systems for this case have been known since antiquity and are based either on mechanical locks or on certificates. In the middle of the 20th century, systems based on electromagnetic phenomena appeared. In the second half of the same century, the need to control access to data also arose. And since data can also be accessed via a computer network, it was necessary to control not only the access of persons to areas with data storage, but also to control the electronic communication of persons with these storage facilities. The different types of the above systems have developed separately and more or less independently. This paper provides an overview of the current status of different types of systems, showing that these systems are converging technologically based on the use of electronics, computing and computer communication. Furthermore, the terminology and architecture of these systems is expanded in the article to allow a unified description of these systems. The article also describes the most common types of access control system configurations.

Keywords:
Access control system, access control system architecture, access control system configuration, identity verification.

1. Introduction

Access control is a method of asset protection that has been around since ancient times. It is based on the fact that access to assets (e.g. into a building or to data) is granted only to selected persons. These persons will be referred to as users in the following. Access control systems have gradually been developed to put the access control method into practice. Mechanical access control systems, i.e. systems based on mechanical locks, appeared first. Only the person who was able to unlock the lock was allowed to enter the asset space. A little later, what we will call certificate-based systems were developed. Originally, these were non-technical systems where access control to assets was carried out by designated persons such as security guards, border guards, etc. These persons control the physical passage to the assets (e.g., a theatre auditorium or a border crossing), and through this passage they allow access to the assets only to those persons who have the necessary certificate (e.g., a theatre ticket or a passport).

Manuscript received August 5, 2024
Manuscript revised August 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.8.5

In the second half of the 20th century, access control systems were further expanded to include electrical systems, i.e. access control systems based on electromagnetic phenomena. All of the above systems are based on restricting access of persons to physical spaces with assets (typically rooms, buildings, or premises). However, with the emergence of computer networks in the late 20th century, it became possible for a user in one physical space (e.g. an office) to work with data stored in another physical space (e.g. a server room). And because data are assets, this fact forced the creation of a fundamentally new type of system. This type of access control systems is not based on restricting the entry of persons into a physical space, but on restricting the electronic communication of persons with data devices.

All of the above access control systems have evolved independently and so their terminology is different. As far as mechanical and certificate systems are concerned, there are no standards that define them as systems at all. In North America, electrical access control systems are referred to as “entry control system” ([1], p. 187) or “physical access control system” - PACS ([2], p. 56). In Europe, the name “electronic access control systems” is standardised for this type of system [3]. Information technology standards (e.g., [4], p. 9) and information processing systems standards (e.g., [5]) can be applied to access control systems to data, where the term “access control” is commonly used. The same term is defined in the Internet Security Concepts Standard ([6], p. 11). However, the term “access control” conveys a security method and not a system, and so in what follows we will use the generic term “access control system”.

The previous paragraph shows that the terminology of the different types of access control systems is neither complete nor uniform. On the other hand, all the systems described have the same purpose (i.e. to control access to assets) and at the same time there is their technological convergence (see below). It is therefore appropriate to first establish a common terminology for these systems. In this paper, the following classification of access control systems will be used.

- For the system for controlling access of persons to objects (e.g. rooms), the term “object access control system” will be used. This class of systems will include the following three types.

  - A system where access control is based on mechanical locks will be called a “mechanical access control system”.
  - A system where access control is based on paper, electronic or other certificates will be referred to as a “certificate-based access control system”.
  - A system where access control is based on the use of electromagnetic phenomena (electric locks, magnetic cards, etc.) shall be called an “electrical access control system”.
- The term “data access control system” shall be used for a system for controlling access to data by persons.

With regard to the above classification, it should be noted that it is based on the historical development of access control systems and does not currently define these systems so precisely. This is because technological developments are blurring the boundaries between different types of systems. For example, contemporary electrical systems use computer networking techniques for communication, data access control systems use electronic certificates, mechanical locks are fitted with electronic accessories, etc.

For a more in-depth description of access control systems, additional terms now need to be defined.

- Entity: a person or device. An example of a device type entity is an autonomous vehicle or a computer. In this paper, however, the problem of access control will be explained using concepts tied to the notion of a person. This is because, for example, the term “requestor” is more concise and illustrative compared to the term “requesting entity”.
- Identity: in the original sense of the word, the correspondence of the attributes of the person being assessed (e.g. his/her surname, eye color, etc.) with the attributes that are certified by a particular authority (e.g. in the person's passport). Nowadays, however, identity is usually understood not as a match, but only as the aforementioned set of certified attributes of the user (e.g., [6]). In access control systems, the identity of a user is usually an identifier (typically a text string).
- Assets: anything that is valuable. Assets can be either tangible (e.g., goods, cash, documents, etc.) or intangible (e.g., data, service, reputation, etc.).
- User: an entity that has rights to manipulate assets, called access to assets.
- Access control: a security method based on the fact that only selected entities, i.e. users, have access to protected assets.
- Access list: a list of users and their access rights. For example, a user with identifier *X* is only allowed to enter room *M* on weekdays between 08:00 and 18:00.
- Access control system: a system that allows users to access assets according to the information in the access list.
- Authority: the person who creates the access list.
- Authorization: the act whereby an authority grants access rights to a person, i.e. grants them user status. For the purposes of the access control system, each user is further assigned a unique designation (i.e. identity), whereby a user with identity *X* will be referred to as user *X* in the following. Next, the user's proof factor and verification factor are negotiated with the user. Using a proof factor (e.g., password), the entity proves to the system that it is user *X*, and using a verification factor (e.g., password hash), the system verifies that the requester has the correct proof factor.
- Certificate: a document confirming a fact. Certificates in access control systems are issued by an authority. Most often, it is a verification certificate that contains the identity of the user and its verification factor. In practice, an authorizing certificate can also be encountered. This specifies the rights that have been granted to the certificate holder. For example, a ticket gives its holder the right to watch a theatre performance from seat *Y*. If the identity of the holder is also stated in this type of certificate, but without a verification factor, then the identity of the holder can be proven within another verification system trusted by the authority (e.g. using an ID card).
- Verification list: a list of user identities and their verification factors. This list may also exist in a distributed form, whereby the authority issues a verification certificate to each user at authorization, stating the identity of that user and their verification factor.
- Requestor: an entity that requests access to assets from an access control system.

2. History

The first access control systems have been documented as early as 6,000 years ago ([7], p. 32). They were based on the principle of a mechanical lock, whereby access to a house or chest required a proof factor in the form of a key. Figure 1 shows a model of a lock from ancient Egypt. The key (bottom right) had uniquely positioned pins, which could then be used to lift up the locking rollers in the holes of the deadbolt body. The picture shows that if the key is lifted all the way up in the lock, the ends of the pins and the ends of the rollers will be flush with the top surface of the deadbolt. A shear line is created (shown in purple in the picture) and the deadbolt can be extended by pulling the key to the right.

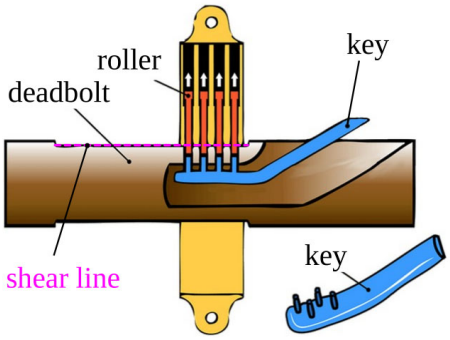

Fig. 1: Ancient Egyptian lock [8].

In antiquity, the first city and state formations began to take shape, with the creation of crossing points on their borders. To cross the border, a person often had to possess the required document [9]. For example, Figure 2 shows a photograph of a papyrus from 722 AD with a person's permission to exit. The documents required to cross the border later evolved into the passport, which today allows its owner to prove his or her identity.

Fig. 2: Ancient Arab exit permit [10].

Access control systems that were based on proof factors in the form of mechanical keys or written documents dominated until the 20th century. The first electrical access control systems appeared in the 1950s. In them, authorized users used a specified type of card as a proof factor and used it to unlock the electric lock of the door they wanted to pass through [11]. Figure 3 on the left shows an example of such a door lock. The types of access cards have gradually changed for security reasons. At first punch cards were used, then magnetic and Wiegand cards, and still later wireless chip cards ([12], p. 108).

In the early 1960s, keyboards also began to be used [11]. In this case, the proof factor was the user's knowledge of the secret number combination entered on the keypad at the door (see Figure 3, right). The 1980s saw a significant proliferation of computers, and here too there was a need to control access - specifically to data, with passwords being the most commonly used as the proof factor.

Fig. 3: A door lock where the proof factor is a card [13] (left) and a door keypad where the proof factor is a numeric code [14] (right).

And in the late 1990s, data access control systems and electrical access control systems [15] also started to use biometrics as proof factors. For example, Figure 4 on the left shows a computer in the form of a smartphone, with the user's facial biometrics used as a proof factor. The figure on the right is then a swipe fingerprint reader on a laptop - in this case the proving factor is the user's fingerprint.

Fig. 4: For example, a face [16] (left) or a fingerprint (right) can be a biometric proof factor [17].

This brings us to the present. The general architecture of access control systems will now be explained.

3. Architecture

The access control system is highlighted by the red box in Figure 5. From the figure, it is clear that the access control system is practically a barrier that is located between the requesters and the assets. And only users can access the assets through this barrier. The behaviour of the system is set and possibly evaluated by the authority.

The system generally consists of four basic elements, which we will call controller C, verifier V, organizer O and gateway G. The purpose of each element is as follows.

- Organizer: the element by which the behavior of the system is set and, where appropriate, by which the authority obtains an overview of the activities of

requesters and other elements of the system. The behavior of the system is mainly set by defining an access list.

- Verifier: element that establishes the identity of applicants or the authenticity of certificates. It communicates its findings to the controller. The verification factors are either obtained by the verifier from its verification list or presented by the requester in its verification certificate.
- Controller: the element that controls the gateway. It usually creates instructions for the gateway based on the verifier's findings and on the information in its access list.
- Gateway: an element that allows user access to assets as instructed by the controller.

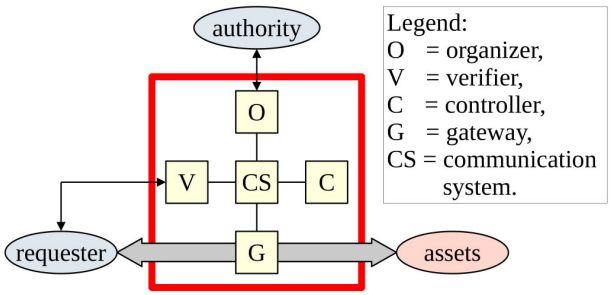

Fig. 5: General architecture of an access control system.

System elements can be devices as well as persons, and multiple elements with the same role can be present in the same system. And if the system elements are geographically dispersed, they communicate with each other through the communication system CS.

Before describing the actual operation of the access control system, it is necessary to clarify a few terms related to verification. The identity of requesters, or the authenticity of certificates, is verified through a verification process. As part of the verification process, the requester allows the verifier to find out the necessary information about his proof factor or certificate. This is done, for example, by taking a fingerprint or by attaching the passport to a reader. The verifier tests the obtained information against the selected verification factor. If the identity of the requester is sought and the aforementioned test is positive for the verification factor of user *X*, the requester is declared as user *X*. If the authenticity of the certificate is verified and the mentioned test is positive for the authentication factor of authority *X*, then the output of the verifier is that the certificate is genuine and issued by authority *X* (e.g. the passport is genuine and issued by the relevant US authority).

In what follows, we will focus on systems that control access based on the identity of persons, and so we will limit further discussion of verification to the issue of verifying the identity of requesters. In some access control systems, a requester first presents itself, i.e., either announces its identity or presents its verification certificate. If the requester announces its identity, the verifier looks up the verification factor in its verification list based on that identity. It then uses this in the subsequent verification test. In the second case, i.e. the requester has submitted a verification certificate, the verifier first verifies the authenticity of the certificate (e.g. by means of a digital signature) and if it is authentic, the verification factor from this certificate is used in the verification test. In both of these cases, if the verification test is successful, the verifier passes the determined identity to the controller. The described process of verifying the presented identity is called authentication.

In other systems, the procedure is that the requester does not present himself and merely allows the verifier to find out the necessary information about his proof factor. The verifier then determines the identity of the requester through verification tests, where it successively tests the verification factors of different identities until either the verification test is positive or all verification factors are tested. If the test is positive for the verification factor of user *X*, the requester is declared to be user *X*. There is no suitable term introduced for the described method of identity determination. While the term identification is sometimes used, this term is generally viewed much more broadly. Therefore, we introduce the term determination for the identification method described above. The term “determination” in the context of identification expresses the fact that the verifier considers all possible identities and determines one of them to be correct.

Then the concepts related to identification can be defined and arranged as follows.

- Presentation: indication of identity by the requester. The requester either announces his identity (usually using a keyboard) or presents a verification certificate stating his identity and the verification factor. The verification certificate may be either in paper form (e.g. passport) or in electronic form (e.g. public key certificate).
- Authentication: verification of the identity of the requester. The requester first presents himself and then allows the verifier to find out the necessary information about his proof factor. The verification test is performed using the verification factor of the presented identity. If the presentation is made in the form of an announcement by the requester, the verifier shall have a verification list. If the presentation is in the form of a verification certificate, the verifier only needs a verification factor designed to authenticate certificates.
- Determination: finding the identity of the requester. The requester does not present himself and only allows the verifier to find out the necessary information about his proof factor. The information obtained is successively tested using verification factors of different identities until either the verification test is positive or all

identities are tested. In this case, the verifier must have a complete verification list.
- Identification: any form of establishing the identity of a requester. It is a generic term that encompasses presentation, authentication and determination.

From the above it is clear that the presentation is an unreliable way of establishing the identity of the requester, as without identity verification, the requester can impersonate anyone. There are two ways to establish identity in a trustworthy manner. Either the requester first makes a presentation and then authentication takes place, or a determination is made. The first method is mainly used in data access control systems, because in this case requesters are by default provided with a means to present themselves (usually a keyboard).

On the other hand, in electrical access control systems, determination is usually carried out, since the possible presentation of the requestor (e.g., by typing his/her identifier on a keypad at the entrance to the building) would take a disproportionately long time. In a typical building access scenario where, for example, hundreds of people per hour need to pass through a single gateway (typically employees arriving at the building in the morning), this delay would be unacceptable. Therefore, the requester simply allows the verifier to determine the necessary information about its proof factor, and the verifier sequentially tests who has a verification factor that matches the proof factor used - this establishes the identity of the requester. Contemporary verifiers are very fast. For example, a fingerprint verifier [18] can scan four fingers of one person's hand and compare them with the verification factors of 100,000 users within 1 second. The throughput of one such pass is then 60 users per minute.

In this context, it is worth noting that determination is also used in police search systems. The difference is that wanted persons do not provide search systems with information about a proof factor (e.g., facial appearance or smartphone identification number) voluntarily. CCTV footage from public places or smartphone login data to base stations are tested against verification lists, which can then identify the locations of wanted persons.

Now we can finally move on to a description of how the access control system works. Before the system can be put into operation, the authority must first store the access list in the controller via the organizer. This list describes the rights of each user to the assets. Next, the authority must import the verification list into the verifier. If authentication is performed using verification certificates, this list contains only one factor that is used to authenticate the certificates. Otherwise, the list contains the identities and authentication factors of all users. Both lists can be additionally updated by the organizer while the system is running (e.g. when a new employee is hired).

The access to the assets itself is as follows. The verifier, either by authentication or determination, determines the identity of the user and passes this to the controller. The controller uses the access list to determine the user's rights and passes these to the gateway. The gateway then allows the user to access the assets in accordance with the list of rights sent by the controller. The gateway can record the user's activities, then pass them to the controller and the controller to the organizer. The authority can then analyze those records.

The certificate that the requester presents to the verifier may contain the requester's rights in addition to the requester's identity and verification factor. In this situation, although the verifier does not need the access list, the authority cannot then operationally change the rights of the person (typically revoke his access rights). The solution is the so-called blacklist, which is a list of persons whose access rights have been revoked. This list is updated by the authority in the controller as needed, and if the requester is on the list, he or she cannot access the assets despite a valid certificate.

4. Configurations

The architecture of the access control systems in Figure 5 is generic. In practice, however, individual devices in the system may play the role of one of the basic elements (e.g., a gateway) as well as the role of several basic elements (usually a controller and a verifier). If a given device fulfils more than one role, this will be indicated by a list of abbreviations of the respective roles separated by a "+" symbol. So, for example, a device that performs the role of both controller C and verifier V will be denoted by (C+V). If we talk about the whole system, we will list all elements symbolically. For example, the enumeration [O, (C+V), n×G] expresses a system with an organizer O, a central device (C+V) and n gateways G.

4.1 Mechanical systems

First, the typical configuration of mechanical access control systems will be explained. The assets are typically located in a room behind a door that is equipped with a lock, usually with a cylinder (see Figure 6). The user has been given a proof factor, which is a key, by an authority (e.g. a hotel receptionist). He inserts this into the cylinder, which puts the key pins and driver pins in the position shown in the figure. In this position, the key pins and driver pins touch each other on the circumference of the plug, which can now be rotated. The cam that unlatches and extends the deadbolt (not shown) rotates with the plug. This allows the door to be opened and the assets to be accessed. In the example described, the plug is the verifier V and the lengths of the key pins are the verification factor.

The controller C is a rotating cam that can be rotated after successful verification. The controller, by its rotation, ejects the deadbolt which here acts as gateway G. All the elements mentioned (i.e. controller, verifier and gateway) form a single device, i.e. it is a device of type (C+V+G).

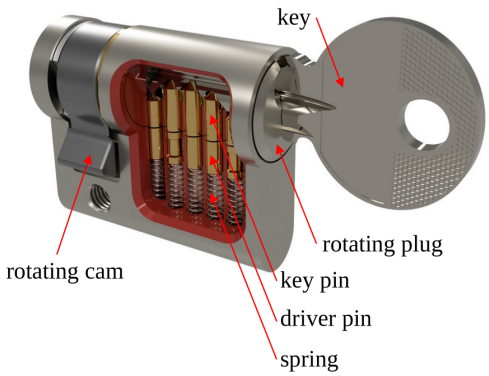

Fig. 6: Cylinder [19].

In the case of a mechanical lock, it is often the case that the key to the lock exists in multiple copies and is thus available to multiple users. In such a case, it is then impossible to determine which of the users opened the lock. The same applies to master key system locks. This type of lock can be unlocked with different keys, but again it is not possible to know when and which user unlocked the lock. Also, with locks, all users have the same right, which is the right to enter the asset room. The lock access list can then be characterized as an implicit list (i.e., it does not exist in explicit form) with a single entry. This entry states that any user (in this case a person with the correct key) has the right to enter the asset room. The verification list is also implicit and, for example, in the case of a cylinder, is determined by the length of the key pins.

The role of the organizer O in systems with mechanical locks is usually performed by the authority itself. The explicit access list (i.e., who has the key to what room) is kept for the administrative use of the authority only and is not exported to any lock. A set of spare cylinders is also included with the organizer. From a system point of view, the verifiers of these cylinders contain various verification lists and then if a key is lost or, for example, a dismissed employee fails to return the key, the existing cylinder is replaced by another. This replacement can be viewed as an export of the new verification list to the corresponding lock. Figure 7a shows a general configuration of a mechanical access control system for a single door. There can be n such doors, and so the configuration of a classical mechanical system can be written symbolically as [O, n×(C+V+G)]. This notation expresses that the system consists of an organizer O and n devices of type (C+V+G), i.e. n locks. The red marked link between the organizer O and the lock expresses the possibility of cylinder replacement, i.e. the possibility of off-line changing the verification list.

Fig. 7: Mechanical and electromechanical access control systems. Typical configuration of these systems a), an example of an electromechanical system with smart cards b) [20] and an example of an electromechanical system with keypad c) [21].

Modern mechanical access control systems already incorporate electronics. The gateway G of such an electromechanical system is usually either a deadbolt operated by a cylinder (see Fig. 7b) or a latch bolt in fitting operated by a door handle (Fig. 7c). The possibility to move the deadbolt or the latch bolt is blocked or allowed by the electronics, which thus acts as a verifier V and controller C. Verification of persons is mainly carried out by means of smart cards (in Fig. 7b the reader is under the black cover), although some manufacturers also offer models with verification by means of keypads (Fig. 7c) or fingerprint readers. The configuration of the described system can again be symbolically described as [O, n×(C+V+G)], i.e. the system contains an organizer O and n locks containing a controller C, a verifier V and a gateway G.

For electromechanical systems, the communication of the lock with the organizer O (red line in Figure 7a) is either offline or online. Historically, the older offline communication is usually mediated by a portable programming device. These devices write lists to the controllers or verifiers and in turn read messages from the controllers. More modern online communication is typically handled by a radio network. The advantage of electromechanical locks is that they offer similar capabilities to electrical access control systems while being easily implemented into existing doors. Simply either replace the existing insert or the fitting.

4.2 Certificate-based systems

Another type of systems are certificate-based access control systems. These are originally non-technical systems where individual roles in controlling access to assets are performed by designated persons, such as security guards, border guards, etc. Although there is a noticeable trend towards automation of this type of systems [22], we will explain it using a classical solution.

The persons who perform the different roles of the system (we will call them services) are in control of the physical passage to the assets (e.g., the entrance to the premises or the border crossing), and through this passage they allow access to the assets only to those persons who have the necessary rights.

Originally, a certificate expressed the fact that the holder of the certificate had certain rights (see text related to Figure 2). This type of certificate can still be found today - for example, a theatre ticket gives its holder the right to occupy a specific seat in the auditorium. For a person who performs a service role, this certificate is one specific access list item that is sent to him by the authority through its holder. The service verifies the authenticity of the certificate and, if so, allows the certificate holder to exercise his rights. The disadvantage of the described solution is the fact that a potential attacker can steal the certificate from the user and thus obtain his rights.

Therefore, in contemporary access control systems, the certificate is practically a distributed item of the verification list, i.e. the certificate contains the identity of its holder and the necessary verification factors (e.g. a photo of the holder). The certificate may also contain the user rights of a person. However, the authority usually does not send the user rights in the certificates and distributes them to the pass points in the form of a complete access list. The user rights can thus be changed operatively during the validity period of the certificate. Certificates were originally in paper form and their authenticity was verified using techmetrics, which are unique measurable and non-replicable attributes of a given certificate (e.g. types and placement of holograms on the certificate). Nowadays, certificates are also used in electronic form and their authenticity is usually verified by a digital signature (i.e. a cryptographic key).

The configuration of the certificate-based system depends on the number of people in the service. The operation of the system will be explained here using the case where the service is single-person, so that this person is also the verifier, controller, and gateway. Symbolically, this is an element of type (C+V+G). As a verifier, the service first verifies the authenticity of the certificate. If the certificate is genuine and it states that user *X* is the certificate holder, then the service assumes that user *X* is requesting access. The certificate includes the verification factor of the requester. For example, in the case of ID cards this is usually the requester's photo and in the case of biometric passports the requester's biometrics. The service verifies the identity of the requester and then starts to act as a controller. It has a written or electronic access list from the authority, which it uses to determine the rights of user *X*. The lists are created by the authority using a suitable organizer O and distributed to the individual passages. Finally, the service starts to act as a gateway and, according to the rights established, allows user *X* to access the assets. There can be *n* passes in the system and so the system described above can be expressed symbolically as a system of type [O, *n*×(C+V+G)].

Figure 8 is a photograph illustrating the passage of a person through a passport counter at an airport. The woman on the left is the requester and the man behind the counter is the service that acts as verifier, controller and gateway.

Fig. 8: Example of a certificate-based access control system [23].

It is clear from the picture that the authenticity of the certificate (in this case the passport) has already been verified and the service is now checking the requester's likeness against the passport photo. So, in practice, in this case a double verification is performed. The first verification is the verification of the authenticity of the passport and the second verification is the verification of the identity of the person according to the verification factor in the passport (in this case the passport holder's photograph). In the case of biometric passports, the service may also verify the person by fingerprint. In this case, the fingerprint verification factors are stored in a chip which is an integral part of the passport. If all the verifications carried out are successful, the service will still verify the requester's rights on its computer. The access lists at border controls do not take the form of a list of persons who can enter the territory of the country, but a list of persons who do not have this right or who need to be detained (the aforementioned black list). If the requester is not on one of these lists, the service will allow her to pass around the counter into the given national territory.

4.3 Electric systems

Historically, the third type of system was the electric access control system. They are mostly used for automated control of access to rooms, buildings or premises. Four typical configurations of this type of system for a single door are illustrated in Figure 9. Organizer O is usually a regular computer with a program (e.g., [24]) that allows the creation, update, and export of access and verification lists. It also allows the import of data on user activities and on the actions of system elements and the subsequent analysis of this data. Gateway G is most often an electric

door lock. However, a gateway can also be, for example, an electrically operated door, or it can be a barrier, turnstile, etc.

Figure 9a shows a historically older configuration of the access control system. The device, which is abbreviated (C+V), acts as both a controller C and a V verifier (e.g., [25]). This device is connected to the organizer and thus the access or verification list can be imported into or updated in the controller or verifier. For connection to the organizer (magenta line in the picture), the RS-485 bus is usually used, or in more modern systems, the LAN computer network. The connection via the computer network is usually metallic (Ethernet connection) and sometimes wireless (Wi-Fi connection).

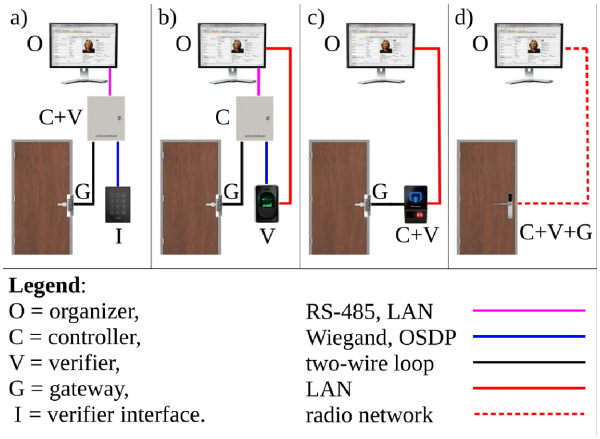

Fig. 9: Typical configurations of electrical access control systems.

Controller C typically controls m = (1 to 4) gateways G via two-wire loops (black line in the picture). Often a door open detector and an outgoing button are also connected to the controller. However, these elements are not essential in principle and so we do not describe them. For safety reasons, the device with the controller is placed inside the object with assets. And since it includes a verifier, an interface I must be installed in front of each gateway, through which the requester can communicate with the verifier. Interface I and gateway G form a pair - by selecting the communication interface I, the requester indicates to the verifier which of the m connected gateways G he wants to pass through. The interface I is either a keyboard or a card reader. The communication between the interface and the verifier (blue line in the figure) is most often done either via a Wiegand connection [26] or, in more modern systems, via the OSDP bus [27]. In general, there can be n devices of type (C+V) in the system, and so the described configuration can be expressed symbolically by the enumeration {O, n×[(C+V), m×(I, G)]}. Thus, in general, there is an organizer O and n devices of type (C+V) in the system, with each device (C+V) connected to m pairs of interfaces I and gateway G.

The deployment of biometric readers forced the configuration as shown in Figure 9b. Verification using biometrics (e.g., fingerprint) requires more computing power and storage capacity compared to existing (C+V) devices. Therefore, biometric reader manufacturers have made the verification interface I (in this case, the biometric sensor) into a complete verifier V. In addition to the sensor, the verifier contains a sufficiently powerful processor to test the biometrics of requesters against a verification list, with the import and update of that list being performed by the organizer O over a computer network (red line in the figure). The remaining interconnections are the same as in Figure 9a. Symboli-cally, the described configuration can be expressed as {O, n×[C, m×(V, G)]}, i.e., there is an organizer of O, n controllers in the system, where each controller C is connected to m pairs of verifier V and gateway G. This configuration was later also used for verifiers that use cryptography to prove identity.

Compared to a biometric verifier, the controller requires much less computational and memory capacity, so the natural evolutionary step was to integrate the controller into the verifier. This resulted in the configuration of Figure 9c, where the biometric reader acts as both verifier and controller (e.g., [28], p. 16). In terms of device inter-connection, this is a much simpler system, but the disadvantage is that the controller controls only one gateway and is also exposed to a higher risk of attack. The described configuration can be symbolically described as {O, n×[(C+V), G]}, i.e., the system consists of an organizer O and n devices containing a controller C and a verifier V, with each of these devices controlling one gateway G.

Due to the miniaturization of components and increasing battery capacity, even more extensive integration can be encountered as shown in Figure 9d. This [O, n×(C+V+G)] type configuration has already been explained for electromechanical systems (see Fig. 7a) and is presented here for completeness. In practice, it is the integration of the controller, verifier, and gateway into a single device that is installed in the door instead of a conventional mechanical lock (e.g., [29], p. 12).

4.4 Data systems

Historically, the youngest systems are data access control systems. The two configurations most commonly encountered in these systems are shown in Figure 10. The figure on the left is the most common configuration of a data access control system, as it is used on virtually any computer network device (computers, servers, routers, etc.). In the example shown, the entire system, i.e., controller C, verifier V, organizer O, and gateway G, is an integral part of the data device. The requestor R accesses assets that are data or data services provided by the given device. The proving factor is most often a password and

possibly biometrics. The described system can be expressed symbolically as (O+C+V+G).

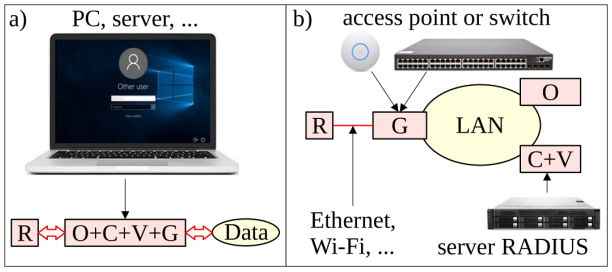

Fig. 10: Typical configurations of data access control systems. On the left is a diagram of the system for data devices, on the right is a diagram of the most common distributed system configuration.

The figure on the right illustrates the most common distributed system layout. In this case, the requester R seeks access to the assets, which are the data and data services provided by the devices on the local network LAN (not shown). Typically, this involves access to server services, access to the Internet, etc. The requester R with its device (typically a computer, smartphone, etc.) is connected to one of the *n* gateways G, which is typically a Wi-Fi access point or an Ethernet access switch. There may be dozens of such gateways in a given LAN. The controller C and verifier V are usually installed on a common server, and the RADIUS protocol [30] is generally used to communicate with all gateways. The access and verification lists are in the form of databases that are populated by the organizer O. The role of the organizer is normally performed by a standard personal computer. A LAN is used to communicate between all elements of the system and a password is often used as a proof factor. The described configuration can be symbolically written in the form [O, (C+V), *n*×G], i.e. the system consists of an organizer O, a device containing both a controller C and a verifier V and *n* gateways G.

In computer networks, it is often the case that the same person is a user in several different data access control systems (different news and shopping sites, different social networks, etc.). However, authorizations in these systems imply different identities and different proof factors for the users, which complicates the users' lives. To address this problem, the concept of common verifier and the concept of shared verifiers have been developed. Both of these concepts are illustrated in Figure 11.

The top figure is used to explain the concept of a common verifier. There are *N* different access control systems consisting of a controller C, an organizer O and a gateway G. In terms of verifying requesters, the authorities of these systems rely on an external common verifier V. An applicant for assets first registers with the administrator of one of the common verifiers V (the so-called identity provider), where it obtains a universal identifier and a proof factor. Then, the interested party is authorized by the individual authorities. If he then applies for access to assets as a requester, the respective controller first requests verification from the verifier V. Depending on the result of the verification, the controller shall grant or deny the requester access to the assets. A well-known protocol for implementing the described concept is the OpenID protocol [31]. The described configuration can be expressed symbolically by the notation [V, *N*×(O, C, G)].

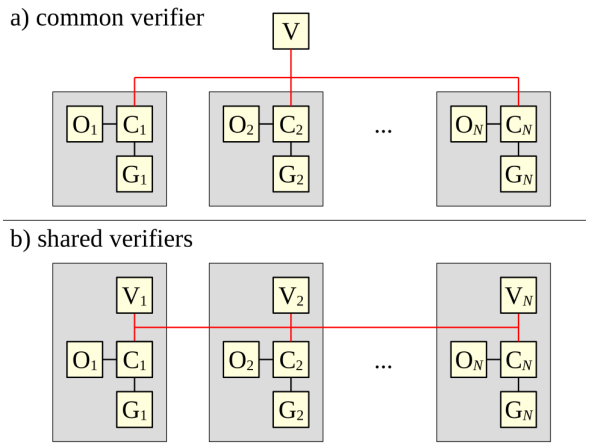

Fig. 11: Concepts of cooperation of access control systems. At the top are *N* systems that use a common verifier V and at the bottom are *N* systems whose controllers trust the verifiers of other systems.

The lower figure illustrates the concept of shared verifiers. In this case, the individual sub-systems are full-blooded, i.e. they have their own verifier. In addition, however, the controllers of these systems accept the outputs of the verifiers of other systems. Symbolically, we can express this configuration as {*N*×[O, C, (V_1, …, V_N), G)]}. A well-known representative of this concept is the eduroam service [32], where staff and students of university A can use the data services of the host university when they visit university B. The controller of university B first facilitates their verification at their home university A and, in case of a positive result, allows them to use the data services provided by university B. The same principle applies to so-called roaming [33], where a user of telephone operator A can use the services of operator B in the area covered by operator B.

5. Conclusion

This paper provides an overview of the current state of existing access control systems. Specifically, it covers mechanical, certificate-based, electrical and data access control systems. For these systems, the terminology and architecture are presented in the paper to allow their unified description. In particular, from a terminological

point of view, new concepts have been introduced, which are presentation and determination. In terms of architecture, the paper shows that all access control systems consist of devices that, in some combination, play the role of four basic elements. These elements are the organizer, controller, verifier and gateway. Depending on the number of these elements in a given system and their degree of integration in the individual devices, there are different configurations of access control systems. The most common ones are listed in the paper.

Overall, the current state of development of the different types of access control systems shows a trend towards their gradual integration. Mechanical locks have been integrated with electrical system devices to create electromechanical systems. Electronic certificates are being introduced into what were originally paper-based certificate systems, and these are also being used in electrical and data access control systems. There is also a trend towards the widespread deployment of computing and the use of digital communication technologies in all object access control systems.

References

[1] GARCIA, M. L. *The design and evaluation of physical protection systems*. 2. Amsterdam: Butterworth-Heinemann, 2008. ISBN 978-0-7506-8352-4.

[2] FERRAIOLO, H. et al. *Guidelines for the Use of PIV Credentials in Facility Access*. Gaithersburg: National Institute of Standards and Technology, 2008.

[3] International Electrotechnical Commission. IEC 60839-11-1, *Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements*. International Electrotechnical Commission, Geneva 2013.

[4] International Electrotechnical Commission. ISO/IEC 10181-3, *Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework*. Geneva, 1998.

[5] ISO. ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*. Geneva, 1989.

[6] SHIREY, R. RFC 4949, Internet Security Glossary, Version 2. Fremont: Internet Engineering Task Force, 2007. Available at: https://datatracker.ietf.org/doc/html/rfc4949.

[7] LE GUET TULLY, F. *Science and the Design of Mechanical and Optical Devices: A Few Case Studies*. In: DE VRIES, M. J.; CROSS, N. and GRANT, D. P. *Design Methodology and Relationships with Science: Introduction.* Eindhoven: Kluwer Academic Publishers, 1993, pp. 29-61. ISBN 978-90-481-4252-1. Available at: https://doi.org/10.1007/978-94-015-8220-9.

[8] *Mechanics of The World's Oldest Lock, From Ancient - Ancient Egyptian Door Lock*. Online. In: Clipartmax. Available at: https://www.clipartmax.com/middle/m2H7i8G6K9H7G6H7_mechanics-of-the-worlds-oldest-lock-from-ancient-ancient-egyptian-door-lock/.

[9] MANGION, N. *The Passport Throughout History - The Evolution of a Document*. Online. In: Investment Migration Insider. IMI. 2020. Available at: https://www.imidaily.com/editors-picks/the-passport-throughout-history-the-evolution-of-a-document/.

[10] AMIN, U. S. M. *Arabic papyrus with an exit permit.* Online. In: Wikipedia. 2019. Available at: https://commons.wikimedia.org/wiki/File:Arabic_papyrus_with_an_exit_permit,_dated_January_24,_722_CE,_pointing_to_the_regulation_of_travel_activities._From_Hermopolis_Magna,_Egypt.jpg.

[11] ENIKEIEFF, O.; WEST, W. and DYE, D. Electronic identification system employing a data bearing identification card (USA). US3221304A. Available at: https://patents.google.com/patent/US3221304A/en.

[12] BOWERS, D. M. *Access control and personal identification systems*. Boston: Butterworth Publishers, 1988. ISBN 0-409-90083-4.

[13] FOWLER, M. ANSI/BHMA A156.25-2023: *Electrified Locking Devices*. In: ANSI. ANSI blog. 2018. Available at: https://blog.ansi.org/ansi-bhma-a156-25-2023-electrified-locking-devices/.

[14] GATE MOTORS. *Let's find the perfect Access Control System Installation companies in your local area*. Gate Motors. Available at: https://libsa.co.za/access-control-system/.

[15] MAGUIRE, M. *The birth of biometric security*. Anthropology Today. 2009, Vol. 25, No. 2, pp. 9-14. ISSN 0268540X.

[16] WHITNEY, L. *How to Set Up and Use Face ID on Your iPhone*. PCmag. 2022. ISSN 2373-2830. Available at: https://www.pcmag.com/how-to/set-up-use-face-id-iphone.

[17] TAYLOR, G. *Flawed Laptop Fingerprint Readers Make Your Windows Password Vulnerable to Hackers*. In: Wonder How To. Available at: https://null-byte.wonderhowto.com/news/flawed-laptop-fingerprint-readers-make-your-windows-password-vulnerable-hackers-0139037/.

[18] IDEMIA. *MorphoWave XP: Contactless fingerprint terminal with extended performance*. Available at: https://www.idemia.com/wp-content/uploads/2022/01/morphowave-xp-idemia-brochure-202201.pdf.

[19] *Half euro lock cylinder* (Wilka). In: GRABCAD. GrabCAD. Available at: https://grabcad.com/library/half-euro-lock-cylinder-wilka-1.

[20] ASSA ABLOY. *Access Control and Net-Ctrl Educate Bett Show on Aperio*. The Locksmith Magazine. 2016. Available at: https://www.locksmithjournal.co.uk/assa-abloy-access-control-net-ctrl-educate-bett-show-aperio.

[21] SALTO. *Product brochure*. SALTO Systems, 2014. Available at: https://www.master-key.pl/files/starter/SALTO-PRODUCT-CATALOGUE-ENG_2015.pdf.

[22] *Automated Border Control*. Secunet Security Networks. Available at: https://www.secunet.com/fileadmin/user_upload/02_Downloads/Produkt-

_und_Serviceseiten_Brosch%C3%BCren_und_Factsheets/easygate/secunet_easygate_Factsheet_EN.pdf.

[23] LOPEZ, M. *Nueva herramienta para ingresar a Estados Unidos más rápido*. Cuba en miami. 2024. Available at: https://www.cubaenmiami.com/nueva-herramienta-para-ingresar-a-estados-unidos-mas-rapido/.

[24] ROSSLARE. *AxTraxPro: The All-purpose Access Control Management Software*. Available at: https://rosslaresecurity.com/wp-content/uploads/2023/12/AxTraxPro-brochure-upd-V009.pdf.

[25] *NetAXS-123: Stand-alone, modular, web-enabled access control system*. Dubai: Honeywell Security Group, 2014. Available at: https://prod-edam.honeywell.com/content/dam/honeywell-edam/hbt/en-us/documents/literature-and-specs/datasheets/HAS-NA123-ME-DS-E%2520pdf.pdf.

[26] SHEPPARD, S. *Wiegand?* Farpointe Data, 2018. Available at: https://www.farpointedata.com/downloads/pr/Understanding_Wiegand.pdf.

[27] SHEPPARD, S. *The Power of an OPEN PROTOCOL*. Security Sales & Integration. 2021, Vol. 43, No. 4, pp. 5. ISSN 1539-0071. Available at: https://www.farpointedata.com/downloads/pr/The_Power_of_an_Open_Protocol.pdf.

[28] IDEMIA. *SIGMA Extreme Series: Quick User Guide*. 2022. Available at: https://biometricdevices.idemia.com/sfc/servlet.shepherd/document/download/0690X00000DpySZQAZ.

[29] *EAccess Product Book*. Solothurn, Schweiz: Glutz. Available at: https://media1-glutz.myassets.ch/A/glutz/82549.

[30] RIGNEY, C. et al., RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*. 2000. Available at: https://datatracker.ietf.org/doc/html/rfc2865.

[31] RECORDON, D. and REED, D. *OpenID 2.0: a platform for user-centric identity management*. DIM '06: Proceedings of the second ACM workshop on Digital identity management. 2006, pp. 11-16.

[32] WIERENGA, K. and FLORIO, L. *Eduroam: past, present and future*. Computational Methods in Science and Technology. 2005, Vol. 11(2), pp. 5. ISSN 1505-0602.

[33] D. He, C. Chen, J. Bu, S. Chan and Y. Zhang. *Security and efficiency in roaming services for wireless networks: challenges, approaches, and prospects*. IEEE Communications Magazine, Vol. 51, No. 2, pp. 142-150, February 2013.

Karel Burda received the M.S. and Ph.D. degrees in Electrical Engineering from the Liptovsky Mikulas Military Academy in 1981 and 1988, respectively. During 1988-2004, he was a lecturer in two military academies. At present, he works at Brno University of Technology. His current research interests include the security of information systems and cryptology.