Access Control in Corporate Systems

Oleg V. Boychenko

V.I. Vernadsky Crimean Federal University, Avenue Academica Vernadsky, 4, 295007, Simferopol, Crimea

Abstract

The work carried out a study on the use of access control systems (MCDS) to ensure permitted access to corporate security. Description of basic, peripheral and additional equipment as part of modern access control systems in the activity of a dynamically developing economic enterprise is given. The main technological capabilities of modern access control systems are described. Directions of the most effective application of access control systems have been determined. Studies have found that MCDS has been widely used in companies where users need to manage and restrict access to information resources with confidentiality characteristics. The fundamental points of the development of innovative access control systems based on machine training and artificial intelligence technologies have been studied. The procedure of preparation of systems for performance of main tasks of determination of the justified necessity of employees on access to information resources of the organization, having signs of confidentiality, is described. It is of paramount importance to use the updated software application as part of access control systems with the provision of continuous monitoring of the unauthorized impact on the automated information system of information resources management of the corporation. The main direction of the development of modern security systems using artificial intelligence systems based on distributed neural networks integrated with blockchain technologies has been determined.

Keywords 1

Access control, security system, security, identification, intellectualization.

1. Introduction

Access control is a set of software and hardware and agency instructions that solve problems of management and administration, visit separate rooms, and operations control the movement of personnel, and spend time in the field. Removing a person from the standard workforce is particularly important for the safety of facilities where the cost of error and sometimes basic needs are very high.

On the other hand, the security officer must be provided with full and accurate information on local developments and have a convenient way of working seamlessly and solving problems. The access control system usually contains ID numbers, card readers, controllers, and ACU [1] servers, and the ID card contains information for user identification.

Along with this, the research shows the prospects for the development of continuous access control management technologies in organizations using information resources that have signs of confidentiality, modern technological machine learning systems (neurotechnologies) in combination (integration) with artificial intelligence systems.

The global market for artificial intelligence (AI) solutions in 2018 amounted to $21.5 billion, in 2024 it will reach $137.5 billion. The global market for neurotechnology solutions in 2018 amounted to $1.3 billion, in 2024 it will increase to $7 billion.

Taking into account the global market for artificial intelligence and neurotechnology in general - taking into account the internal developments of companies - in 2018 amounted to $396 billion, and by 2024 it will increase to $890 billion. Similarly, the size of the global neurotechnology market as a whole in 2018 amounted to $7 billion, by 2024 it will increase to $35 billion.

Proceedings of VI International Scientific and Practical Conference Distance Learning Technologies (DLT–2021), September 20-22, 2021, Yalta, Crimea

EMAIL: bolek61@ mail.ru (A1),
ORCID: 0000-0003-3326-1015 (A1)

The Russian market for AI solutions in 2018 amounted to 2.1 billion rubles, by 2024 it will increase to 160 billion rubles. The Russian market for neurotechnology solutions in 2018 amounted to 100 million rubles, by 2024 it will grow to 8.2 billion rubles.

The Russian AI market as a whole in 2018 amounted to 189 billion rubles, by 2024 it will increase to 907 billion rubles. This indicator includes the revenue of companies in the field of artificial intelligence, the revenue of other IT companies that develop products thanks to AI, and the increase in revenue of companies from various sectors of the economy, which was obtained thanks to artificial intelligence).

Similarly, the Russian neurotechnology market as a whole in 2018 amounted to 45 billion rubles, in 2024 it will grow to 65 billion rubles.

Thus, to detect defects in the equipment of the MCDS system, it is now most advisable to use the development of Boeing using the neural network and machine vision for detection with higher accuracy. In addition, modern computer vision architectures and deep neural network algorithms are being developed to recognize and analyze captured images of aircraft, identify anomalies and initiate early warnings.

2. Technological Aspects of CPD

Each card is assigned a certain level of access, according to which the user is entitled to access that or that door at certain intervals. The card can be used simultaneously as a bypass with a photograph, a credit card, etc. The following types of cards are used in the ACU system:

#Plastic card with magnetic strip Card «Wiegand» is a plastic card with a rectangular loop of hysteresis made of an alloy, which allows assigning each unique code card;

#bar-code card - plastic card with printed bar-code;

#Sensor Contact Cards - Plastic Card with built-in chip and electronic interface.

It should be emphasized that the Smart Card is much better than other types of ID cards in almost all functions (safety level, read technology, noise resistance, mechanical damage, durability, reliability, and bandwidth).

The main advantages of a non-contact smart card are a high level of security, storage of a considerable amount of information, the possibility of programming and reprogramming, the possibility of performing cryptographic operations. Reader applications, as an important element in an ACS system, provide a reading of the information on the map. This information is addressed to the manager who decides on the user's access to the automated system. [2]. It contains information about the operating system's mode configuration, a list of people who are entitled to enter the premises, and their right of access to these premises. Large systems may have multiple controllers.

To enhance the authentication process, a keyboard connected to the administrator is used to dial a personal ID number. SCOD servers are computers that control their associated access controllers. Port data, photos, individual code, and other information about the holder of the user's ID card are entered on the personal «electronic card» so that the personal «electronic card» The user and identification number were appropriate and recorded in the databases. [3]. In the system, each code is linked to information about the rights of the cardholder. Based on a comparison of the information and the circumstances in which the card was entered, the system makes the decision: open the controller or door locks (lock, turnstiles) or turn the room into a protection mode, including emergency signals, etc.

All facts about the presentation of maps and related actions (bypassing, alarm, etc.) are recorded under control and stored on a computer. Information on events related to the presentation of maps can be used in the future for the production of reports on the recording of working time, the allocation of work, etc. Depending on the tasks of the administrative boards, you can choose the appropriate access control and management system. A small access control system prevents access to undesirable people, and staff will determine the exact terms to which they are entitled to access. The more complex system, in addition to limiting access, assigns each employee a unique schedule, saves, and then browses information about the events of the day. Systems can operate autonomously and on a computer.

An integrated access control system allows to solve security and safety issues, automate the work of employees and accounting, to create an automated workstation. The set of workstations performed by complex systems makes it possible to use monitoring systems to perform certain tasks in a company or facility.

Sound hound technology is designed to create the conditions for a flexible and scalable voice intelligence system with voice support and combines both automatic speech recognition (ASR) and natural language understanding (NLU) in one mechanism, which significantly improves speed and accuracy. In addition, the Houndry Platform offers more than 125 domains of mutual understanding, title schedules, and redistribution rights from suppliers.

The implementation of the measures of this roadmap will need 392 billion rubles. until 2024. Including the federal budget, as it is planned to allocate 57 billion rubles for the corresponding purposes, extrabudgetary sources - 335 billion rubles.

Barriers to the development of artificial intelligence in Russia are a low level of AI use in companies; low use of AI technologies in health care; low availability of medical data required for AI; low availability of quality education; Poor quality and accessibility of public services for residents and companies; Low intensity of AI research; Lack of modern AI training programs; insufficient development of domestic high-speed energy-efficient microprocessors that are optimal for AI tasks; insufficient provision of data centers for collective or individual use for the performance of AI tasks; lack of regulatory conditions for access to data and lack of a full-fledged system of regulatory and technical regulation in the field of AI. Because of the above, a gradual transition to new technology platforms with traditional mechanisms for effective management of access control systems in corporations becomes an urgent need.

3. Contactless Access Control Systems

There are now much different control and access control systems. A typical access control system using a MIFARE card as an identification card is MFNet, which is designed to control and allow access of persons or vehicles to the security control area. [4]. The authenticity of the content is verified based on its unique identification information - a contactless Mifare smart card.

The MFCNet system consists of the following elements:

- MIFARE identification letter issued to employees of the company;
- Read the touch screen maps;
- Fastening devices (doors with electrical or electrical locks, oscillations, obstacles);
- Control devices for controlling devices connected to the information system;
- ACS server with server software;
- automated workstation with additional software modules (LAN staff, worktime module, interactive application, etc.).

The MIFARE smart card is designed to define administrative tasks using large internal memory as well as a hierarchical access key system for the information stored on the card and to provide security against unauthorized access. The smart card can store information related to the access group, access level, time, specific route or access point for a one-time and a temporary passage, validity period, and user ID, etc. in the memory.

Sensor screen readers use information from MIFARE cards to read and are produced in various implementations to ensure maximum ergonomics and reliability. The disconnector (ZU) is intended for the immediate closure of the protective zone. ACS MFNet supports a wide variety of SPs electromechanical and electrical locks, turnstiles, obstacles. The system can include a full-function FPR controller 3.02 specialized version 3.02 C FPR controller with additional devices for handling with sides and obstacles and a shorter ASCs 3.02JI image controller, where it is possible to work with only one reader, which is structurally located directly on the administrator [5].

Server software is designed to install operating mode controllers, access methods used, authorized lists and closed Go cards, as well as reports and other events. The additional modules enhance the capabilities of the basic software, which is grey, and are designed to provide CPD operations, produce specific reports or provide access to CPD data from different assignments. MFNet access control system supports several basic access algorithms. Each access point is configured to use one or more (in any combination) access algorithms that allow logic, i.e., if a card is allowed by at least one algorithm, the controller decides to access.

In addition to accessing any point algorithm, it is possible to include additional conditions that may be related to logic, i.e., if the card does not meet at least one of the additional conditions, access will be denied.

The MFNet CKD system can operate in two settings:

#Interactive (all chat controls are controlled by the system server);

#independently (manual mode).

The MIFARE contactless technology allows device administrators to operate in autonomous mode, but in the same system. This simplifies the implementation of systems of access to business, payment, and accounting in remote facilities and related items.

The MFNet access control system allows you to set different settings. Depending on the amount and actions you need, you can analyze the following typical system settings:

• minimum - a system of one or more controllers operating independently or connected to an unregistered server. Designed for small offices;

• standard is a system of multiple controllers connected to a network and a dedicated server connected to a local network. The ACS MFNet server allows you to connect more workstations and users to collect information simultaneously;

• corporate system - includes many tasks (60) of managing various protective devices (doors, gates, barriers).

This system allows access to pass, entry, entry, and exit as a control location for the access control system. System controllers connect to a server, each of which can have up to 64 controllers. Depending on the reliability and performance requirements, MS SQL Server can be used instead of the MS Access database for such a system. [6]. The MFNet system has all the features of classical access systems, such as:

#Create and edit files in different formats in different regions;

#assign and modify individual and group access settings;

#Maintenance of registration and recording of the number of relationships offered by traffic, violation of access mode.

In addition, the system uses a personnel search module that allows finding anyone employee of the company instantly. MFNet access control system is characterized by the following factors: [7]:

- multi-point access for use in a high capacity system;
- The level of access inhibition refers to a system with a high level of stability.

Today, two card formats are as common as possible on the market: EM Microelectronic-Marin EM4100 cards operating in the range of 125 kHZ, and cards manufactured by NXP Semiconductors and HID operating in the range of 13.56 MHz.

EM-Marin cards are widespread on the Russian market - largely due to the affordable price. The use of cards of this format has one drawback - such cards are easy to fake. Copying is done by writing a known number to a new card with the option of overwriting the number (UID, Unique Identifier). Currently, tools are available on the market to create any duplicate cards operating at 125 kHZ.

It was the fact of the insecurity of cards operating at this frequency that served as the main incentive for the widespread distribution of Mifare cards - especially the Plus and DESFire families, which have maximum protection against hacking.

The main difference in the Mifare card format is the presence of internal memory. Memory access may be restricted by the key. For example, for Mifare DESFire cards, the key length is 32 characters. For this type of card, the AES/3DES encryption algorithm is applied to the key, which eliminates any possibility of accessing the application.

All Mifare cards have a built-in memory structure - EEPROM. In addition, each card has a Unique Identifier (UID). The UID is not a protected area and can be read on any device. In some cases, UIDs are mapped. Until recently, only Mifare UID cards were used for identification in MCDS. But today this method does not provide full protection from hacking. You can purchase cards that allow you to record a well-known UID on a new Mifare card and use it as a duplicate [8].

To do this, cards operating at a frequency of 13.56 MHz are used with the ability to overwrite UID (for example, Mifare ZERO cards issued by companies in China). Therefore, access control systems are increasingly using internal Mifare card memory or, in other words, EEPROM to identify users.

EEPROM (Electrically Erasable Programmable Read-Only Memory) is an electrically erasable permanent memory (ROM). Typically, the EEPROM consists of 16 or 40 sectors, and it is in these sectors that the access identifier is written, which is then used for identification in the MCDS. EEPROM sectors are protected by a key.

Maps in this family represent the initial level of protection. The most common area of application is the use as tickets for public transport or mass events. Ultralight family cards differ in memory size (Ultralight ® Nano: 40 bytes, Ultralight ® C: 144 bytes, Ultralight ® EV1: 384-1024 bytes) and have the ability to prohibit overwriting.

These cards have expanded memory, increased data transfer speed, and the ability to crypto protect. Main applications: access control, payment systems, cards for campuses/ID cards, loyalty program cards. In 2007, staff at University College London, UK, and the University of Nijmegen, the Netherlands, discovered a serious vulnerability of such maps. It is noteworthy that NXP tried in court to stop the publication of articles on the hacking of the Mifare Classic.

For effective implementation of card copy protection measures, the readers of the access control system must support the read mode of identifiers from the protected area. Standard versions of readers do not have this ability [9].

The saved configuration is written to the master map for subsequent data transfer to the system readers. The master card is recorded using the standard desktop reader of the system.

After data transfer, the master card contains the following information:

- Mifare Map Family View;
- the memory section of the card where the identifier for reading is stored;
- access key, which will be used by each reader of the system to access user cards during identification.

The configuration is transferred to all system readers using a master card. The administrator presents a master card to each reader of the system.

After the master card is submitted, readers are programmed to work only with a specific Mifare card family, reading is carried out only from the memory section specified in the configuration, Mifare UID does not read.

The memory section of the access card previously specified in the configuration is populated with the ID number for the employee. Identifiers are written to cards using a check reader. The memory section of the card for recording is automatically selected according to the configuration.

Thus, Mifare is a family of contactless smart cards from NXP Semiconductors.

There are some types of maps of this format, which differ in the degree of information protection and the amount of data stored.

Cards of this format are widely used in transport and banking. In MCDS, their use is justified if it is necessary to obtain the most protected system.

As a rule, the recording and storage of information on the card in MCDS are not used, but the ability to read such cards allows you to use identifiers from other areas, such as social or bank cards.

The system of access control and control (MCDS) is designed for automatic and/or automated restriction of access of persons to a certain territory.

Access is restricted based on unique personal characteristics. The most common way to identify a person in MCDS is to read the codes of an electronic card (electronic key).

MCDS brand TSS1 allows you to identify people on almost any basis, which are provided by modern hardware (smart card readers, biometric readers).

The system of access control and control (MCDS) is designed for automatic and/or automated restriction of access of persons to a certain territory.

In addition to directly limiting access, MCDS solves the following tasks:

Record and modify data on the owners of electronic keys, including with automatic recognition of identity documents.

Monitoring and visualization of the system operation (information about the system users' passes, messages about unauthorized access, etc.) in real-time.

Storing system information in the database.

Generate reports (working hours, violations, alarm events, etc.).

Import and export data.

Organization of visitor access control.

Organization of subscription services.

Generate and print passes.

Special modes (evacuation of staff, dining room, elevators, parking, control of key issuance, etc.).

MCDS in general is a software and hardware complex that includes electronic equipment and software, and which operates using personal computer equipment, operating environments, local networks. The basis of the complex is an intelligent control system, consisting of control electronic units - MCDS controllers, and software that repeatedly expands the capabilities of the system [10].

Control controllers of the TSS brand are compatible with almost all types of readers of unique identifiers (Emarin, HID, Mifare, biometric) and actuators (locks, turnstiles, barriers, gate drives, card receivers).

All TCC brand controllers contain a key base (up to 65000), event memory (up to 150000), and in the state of fully autonomous operation2 perform basic access restriction modes. Special settings allow you to independently process some additional functions.

4. Conclusion

Thus, the company's most popular automatic control system is the MFNet system, which allows the addition of access controls to accounting functions as well as cash expenditures, Payment, and accounting of goods and services during the operation of the system without the need to replace existing maps and equipment.

The additional power of the MFNet system is created by the use of contactless Mifare Mifare smart card technology, which allows working with non-independent applications, creating the potential for functional expansion and modernization of the system even during operation.

Today, EM-Marin cards operating at 125 kHZ are most widely used in MCUD. Such identifiers do not have copy protection, enough tools are available on the market to create any duplicates of this type of card. Using Mifare cards in MCDS systems allows you to exclude the possibility of copying the card. A prerequisite is the recording of identifiers in the crypto-algorithm-protected area of cards and the use of readers (including control readers) that access the internal memory of Mifare cards using the specified crypto-keys. Only then is it possible to initialize the user cards correctly and read the identifiers further.

5. References

[1] A.A. Shelupanova, S.L. Gruzdeva, Y.S. Nahaeva, Theory and practice of access to information resources. The hotline is Telecom, 2009. PP. 552.

[2] GOST R 51241-2008 «Control and access control tools and systems. Classification. General technical requirements. Test methods»

[3] A.V. Badikov, P.V. Bondarev, Access Control and Control Systems. M.: MIFI, 2010. 128 p.

[4] A. M. Abramov, O. Y. Nikulin, A.I. Petrushin, Access control systems. M.: Obereg-RB, 1998. 170 p.

[5] A. K. Starch, Means and systems of control and control of access: A training manual. M.: NYC "Protection" of the Department of Internal Affairs of the Russian Federation, 2003. 200 p.

[6] A. Gince, New technologies in SCUD. Safety systems. M., 2005. PP. 38-44.

[7] V.A. Crow, V.A. Tikhonov, Access Control and Control Systems: Training Manual. M.: Telecom Hotline, 2010.

[8] N.V. Apatova, O.V.Boychenko, O.L. Korolyov, I.V. Gavrikov, T.K. Uzakov, Stability and Sustainability of Crypto tokens in the Digital Economy. Communications in Computer and Information Science this link is disabled, 2020, 1337, стр. 484–496.

[9] O.V. Boychenko, I.V. Gavrikov, Potential Applications of Smart Contract Technology in Corporate Business Processes. Communications in Computer and Information Science this link is disabled, 2019, 1141 CCIS, стр. 612-624.

[10] I. Pilkevych, O. Boychenko, N. Lobanchykova, T.Vakaliuk, S. Semerikov, Method of assessing the influence of personnel competence on institutional information security. CEUR Workshop Proceedingsthis link is disabled, 2021, 2853, стр. 266–275.