Hardware-software complex ensuing information security of automated building management systems

Dmitry Mikhaylov[1], Igor Zhukov[2], Andrey Starikovskiy[3], Alexander Zuykov[4], Anastasia Tolstaya[5], Stanislav Fesenko[6] and Stepan Sivkov[7]

[1,2,3,4,5,6,7] National Research Nuclear University "MEPhI", Moscow, Russia

ABSTRACT

The article is related to the issue of protection of automated building management systems or ABMS. The popularity of ABMS and its rapid development has a negative impact on computer security. With the increasing relevance of such systems the number of malicious tools aimed to obtain unauthorized access to information and building management is also rising. That may lead to privacy violation, equipment malfunction, loss of time in business processes and even endanger people`s life. The paper describes the methods of protection of automated building management systems used in smart houses or buildings, and, in particular, to protection against unauthorized devices and connections to the automated control system using wired or wireless channels. The proposed hardware-software system ensures an adequate level of information security of ABMS. The product improves the reliability of such systems in terms of protection against unauthorized third-party and internal actions as well as against malicious software and hardware.

Keywords: automated building management systems (ABMS), security, protection, hardware-software complex.

1. INTRODUCTION

Currently, the market of technical innovations is facing a new trend: equipment of buildings with different automated building management systems or ABMSs.

ABMS is a complex engineering system covering virtually all spheres of life support in modern buildings or all the steps of production manufacturing. The automated control systems provide control and monitoring of various modules and subsystems of the automated production system and other automated systems at the production site.

Such systems are getting more and more popular worldwide due to the wide range of functions they provide. [1]

ABMS may perform a great diversity of functions, namely:

- lighting control,
- climate control,
- access and security control,
- fire alarms control,
- power supplies,
- alarm system,
- video surveillance,
- heating system,
- manufacturing process control,
- etc.

Additionally, the ABMS can be responsible for access control to a production site (or a building). Some sophisticated automated building management systems can be used for complex engineering objects that have a strategic importance for a country. For example, the ABMSs are used at nuclear (or hydroelectric) power plants, places of mass gathering of people, such as, for example, airports, military bases, train stations, malls, etc.

Nowadays the number of vital systems controlled by automation is increasing. However, such systems are often connected to personal computers based on Windows and UNIX operating systems that can be attacked by malicious software [2]. Moreover, open wiring used to control automated management system makes it possible to connect the system by means of "insert" in communication line.

Moreover, the growing complexity of ABMS increases the number of potentially vulnerable elements of the system. At the same time, such vulnerabilities attract attention of intruders because of the possibility to obtain valuable, often confidential, information and control over vital systems. That may lead to privacy violation, equipment malfunction, and loss of time in business processes.

The reason for this is insufficient level of security. Experts who develop the system often do not pay enough attention to information protection. It is often incorrectly states that viruses for ABMS do not exist as well as there is no evidence of any attacks on industrial control systems.

However, such technologies as HTTP, Bluetooth, Wi-Fi, GSM as well as other protocols of wireless data transmission used by people every day may become a channel for infection of automated management system by viruses. [1], [3], [4]

The potential vulnerability of automated management system is in its novelty and technology peculiarity as it unites different technical solutions. In addition, each new technology is inherently vulnerable.

It is worth mentioning that we are talking about life-support systems, and thus, about human lives. This is the first time in human history when a computer attack could threaten people`s life [2].

The first programs to protect industrial control systems were set up by the world leading countries after the virus Stuxnet attacks on Iran's nuclear facilities took place [5]. However, currently there is no specialized integrated system of automated building protection from hackers as used computer antiviruses cannot provide required safety.

Industrial control systems are usually installed at critical facilities. That means that their safety should be ensured not only by the physical isolation of wires that transmit the control signals, but also by the use of modern means of information security.

Taking into account the attention of the world community to counter terrorism and close monitoring of critical objects (nuclear power plants, thermal power plants) as well as public places (shopping centers, airports, etc.), special priority should be given to possible cyber attacks: shutdown of vital systems, alarm systems, electricity, etc.

Currently, only software means of information protection of ABMSs exist [2]. At the same time, the use of hardware basis will not only reduce the costs and complexity of development but also significantly improve the reliability of digital home security. Software antivirus systems cannot solve the problem of full protection of automated building due to the lack of a hardware component in the complex. The effectiveness of ABMS antivirus software protection is extremely low: the methods that are effective for personal computers are not efficient for automated building management system.

Thus, the current ABMSs are not protected from rising malware and computer virus threats. The conventional systems do not have any means for detecting that any unauthorized devices or systems (i.e., the devices not declared in the original documentation) are connected to a given ABMS. Furthermore, there are no antivirus applications that are adapted for use in the automated building management systems. The conventional antivirus applications are not reliable within ABMSs, since they are mainly designed for different types of threat.

Accordingly, there is a need in the art for an efficient and effective system and method for protection of the automated management systems.

2. SECURITY PROVISION OF AUTOMATED MANAGEMENT SYSTEMS

The developed hardware-software complex gives protection of automated building management system from attacks. The complex is developed specifically for this purpose and it can protect the industrial control systems more effectively than standard antivirus means.

The ABMSs used for controlling separate tasks or industrial objects have a precise structure including special communication protocols and a special device addressing system. A majority of automated building management systems use a “star” and “tree” topology. The ABMSs employ various types and numbers of addresses on the bus. For example, the bus can have group addresses or individual addresses.

Any event that occurs inside an automated system triggers a command sent over a data channel. The command contains the address (or addresses) of a sender-device, the address of a receiver-device, the actual command (i.e., for example, “set a room temperature at 72 degrees F in a particular room” or “turn off an automated control for two hours”), as well as some service data including, for example, an execution priority of a given command.

The proposed hardware-software complex protects ABMS from connection of new (unauthorized) devices by constant monitoring of commands transmitted over system network. At any given moment, a user can obtain data about the commands transmitted over the data channel. If an unauthorized device connects to the line, the protection system notifies the user about unauthorized data transmission and saves all of the relevant data (i.e., time, data, executed command, addresses of sender-devices and addresses of receiver-devices).

Protection of automated management systems is implemented in the following areas:

- protection of the ABMSs that use power lines for data transmission;
- protection of the ABMSs that use data transmission over a twisted-pair;
- protection of the ABMSs that uses On-Board Diagnostics signal protocols (i.e. CAN bus) for data transmission;
- protection of the ABMSs that use radio channels for data transmission.

The protection of the ABMS includes the following features:

- analyzing a system for presence of unauthorized devices or unauthorized connections;
- detection of undocumented (i.e., not declared) devices and suspicious commands from connected devices;
- detection of various types of activities (i.e., wrong packets, unidentified activities, certain types of commands, etc.);
- analyzing different network frequencies for data transmissions;
- maintaining device activity logs;
- performing automated database searches for any parameter or set of parameters;
- implementing graphic analysis of ABMS device activities.

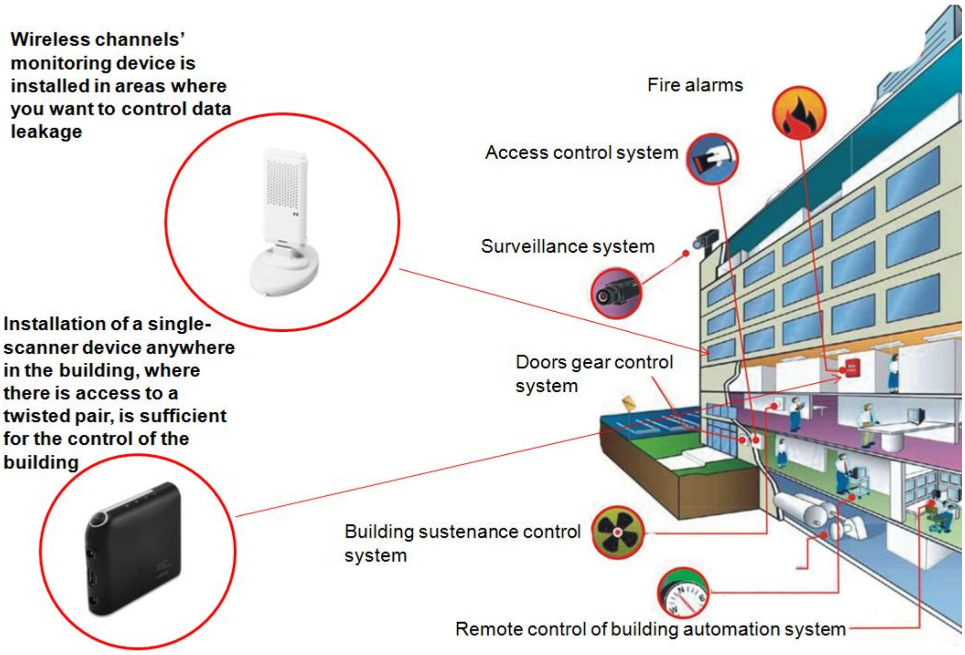
Wireless channels' monitoring device is installed in areas where you want to control data leakage
Fire alarms
Access control system
Surveillance system
Installation of a single-scanner device anywhere in the building, where there is access to a twisted pair, is sufficient for the control of the building
Doors gear control system
Building sustenance control system
Remote control of building automation system

Figure 1 Elements and systems controlled by automated building management systems.

The hardware-software complex ensuring comprehensive protection of automated building management systems from attacks solves the problems of information security, inter alia:

2.1. Signal control passing through the information transmission system based on twisted-pair

The problem is solved by the hardware-software complex development installed in a twisted-pair of industrial control systems. The complex analyzes the signal passing through the twisted-pair and, if necessary, blocks the signal.

The device transmits the information about all suspicious signals to a central server system where this information is collected and comprehensively analyzed. This approach allows quickly detecting and blocking intrusion into automated management system`s network.

2.2. Increasing reliability and security of data transmission through transmission facilities

The problem is solved by the development of the cryptographic data protection device. The device is installed at both ends of automated management system`s data bus. At the entrance of the line the hardware encryption of data is performed and at the output – decryption. Such approach helps to deal with unauthorized intruders of industrial control systems.

2.3. Monitoring and analysis of aberration of the unknown origin occurring in the systems of force lines of industrial control systems connected with attempts of unauthorized third-parties to influence the work of the various electronic components of the automated system

The solution to this problem is a hardware-software tool installed in a force line. By analyzing the incoming signal and a priori information about the system in whole this device filters the signal separating it for useful and random components. After that the signal purified from malicious or accidental impurities is passed through the transmission link.

2.4. Protection of wireless data transmission channels (Wi-Fi, Bluetooth, GSM) widely used in various control mechanisms of intelligent systems of ABMS

The problem is solved by the development of hardware-software complex for activity monitoring of wireless devices in the selected area. The hardware part of the complex is a set of devices installed into the target area and a block of data analysis. The software part is a complex cross-platform software that works with Windows and UNIX operating systems. The software analyzes obtained from the hardware part of the complex data on the subject of unauthorized data transmission.

2.5. Protection of central intelligence industrial control system`s units from malware

Automated building management systems have their own specifications that determine the need to develop appropriate specific antivirus software that is installed on a central server of automated system and protects it from software-based attacks from both internal and external offenders.

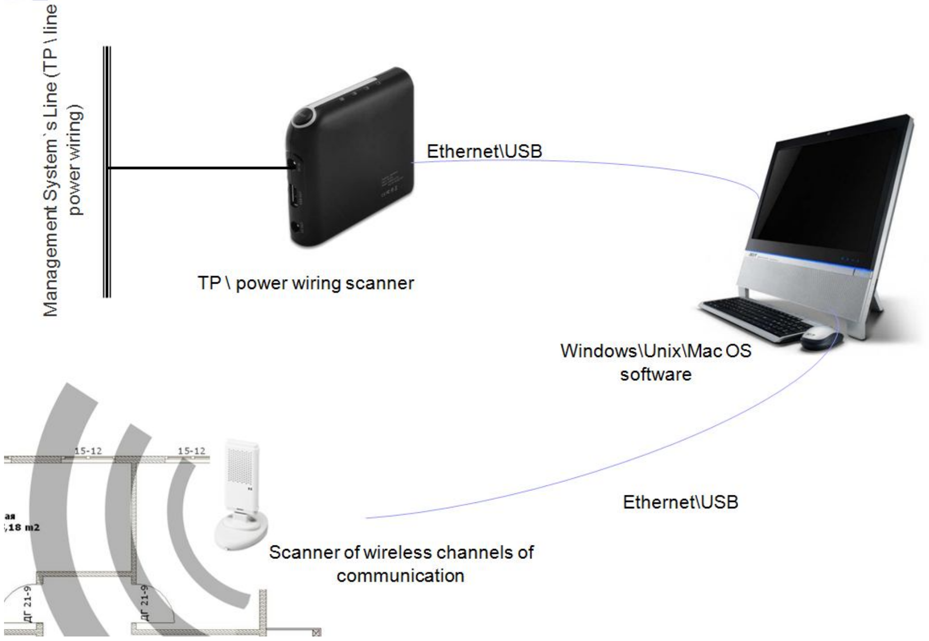
Management System`s Line (TP \ line power wiring)
Ethernet\USB
TP \ power wiring scanner
Windows\Unix\Mac OS software
Ethernet\USB
Scanner of wireless channels of communication
15-12
15-12

Figure 2 The scheme of provision of information protection of automated management system by proposed hardware-software complex.

To perform detection and classification of radio frequency transmission the system comprises antennas, preamplifiers, active filters, reference generators, ADC (analog-to-digital converter), spectrum analyzer, mixers and processor. The signal received by the antenna goes through a high frequency path to recognize its frequency and power. As a result, a narrow frequency channel can be traced to detect transmission of a particular type. Moreover, it is possible to receive radio spectrum activities for a wide range of frequencies.

To protect the automated management systems built on twisted-pair the complex comprising differential amplifiers, active filters, reference generators, ADC, mixers and processors is used. The received signal is checked for all parameters (frequency, amplitude, packet structure, etc.) to identify the compliance with standards. If it conforms to the specifications the received packet is checked for undocumented addresses and unauthorized transmissions. In case of package structural failure or unauthorized connection the operator is notified about the violation.

To protect the automated management systems built on force lines the system comprising passive and active filters, reference generators, ADC, mixers and processors is used. The received signal is checked for all parameters (frequency, amplitude, packet structure, etc.) to identify the compliance with standards. If it conforms to the specifications the received packet is checked for undocumented addresses and unauthorized transmissions. In case of package structural failure or unauthorized connection the operator is notified about the violation.

3. Conclusion

This paper is devoted to description of a new method and system for protection of an automated building management system against unauthorized devices and connections. The system also controls network resources and transmitted data.

The uniqueness of the developed complex is in fact that it uses hardware and software means of protection of automated management systems.

In general, the hardware-software protection of automated building management system solves the following problems:

- protection of automated management systems, built on data transmission over power lines, for example, X10;
- protection of automated management systems, built on data transmission over twisted-pair, for example, KNX, C-Bus, use of Industrial Ethernet;
- protection of automated management systems, built on data transmission over the air, for example, Wi-Fi, Bluetooth.

Work is underway to increase the number of supported protocols and to study new methods of protection.

REFERENCES

[1] Starikovskiy A.V., Zhukov I.Yu., Mikhaylov D.M., Tolstaya A.M., Zhorin F.V., Makarov V.V., Vavrenyuk A.B. Research on vulnerabilities of digital home. Scientific-technical Journal “Special Equipment and Communication” №2, Moscow 2012. Pages 55-57.

[2] Starikovskiy A.V., Zhukov I.Yu., Mikhaylov D.M., Sheptunov A.A., Savchuk A.V., Krimov A.S. Improvement of security of automated building management systems from cyber attacks. Scientific-technical Journal “Special Equipment and Communication” №4, Moscow 2012. Pages 2-5.

[3] Babalova I.F., Shustova L.I., Pronichkin A.S., Aristov M.I., Evseev V.L., Fesenko S.D. Attacks on automated management systems based on vulnerabilities of wireless data transmission channel Wi-Fi. Scientific-technical Journal “Special Equipment and Communication” №4, Moscow 2012. Pages 20-22.

[4] Beltov A.G., Novitskiy A.V., Pronichkin A.S., Krimov A.S. Attacks on automated management systems based on vulnerabilities of digital data transmission devices. Scientific-technical Journal “Special Equipment and Communication” №4, Moscow 2012. Pages 26-28.

[5] Jonathan Fildes. Stuxnet virus targets and spread revealed. BBC News. 2011. URL: http://www.bbc.co.uk/news/technology-12465688.

AUTHORS

Dmitry Mikhaylov, PhD, associate professor of National Research Nuclear University “MEPhI”. Computer Systems and Technologies Department.

Igor Zhukov, Doctor of Engineering Science, Professor. National Research Nuclear University “MEPhI”, Moscow, Russia. Computer Systems and Technologies Department.

Andrey Starikovskiy, teaching assistant of National Research Nuclear University “MEPhI”. Computer Systems and Technologies Department.

Alexander Zuykov, Ph.D. candidate of National Research Nuclear University “MEPhI”. Computer Systems and Technologies Department.

Anastasia Tolstaya, graduate of National Research Nuclear University “MEPhI”. Department of Management and Economics of High Technologies.

Stanislav Fesenko, Ph.D. candidate of National Research Nuclear University “MEPhI”. Computer Systems and Technologies Department.

Stepan Sivkov, Ph.D. candidate of National Research Nuclear University “MEPhI”. Electric Engineering and Electronics Department.