Development of a method for the determination and registration of unauthorized data transmission channels at industrial manufactories

Ilya Kovalev[1,*], *Michael* Babin[1], and *Petr* Nikishechkin[1]

[1]MSTU STANKIN, 127055 Vadkovskiy per. 3a, Moscow, Russia

Abstract. The problem of industrial espionage is very common in the modern world. Existing complex systems are difficult to configure and turnkey solutions are created from integrator firms. In many enterprises, both industrial and civilian, wireless is a less secure area. The proposed solution, which is used as an addition to existing security systems, is able to detect not only created networks with the usual parameters, but also detect hidden data networks and signal unregistered wireless data networks to send information to a special server. The paper presents the architecture of the hardware-software complex, presents the first prototype and conducts test tests.

1 Introduction

One of the components of the competitiveness and technological independence of modern enterprises is an established system of competitive intelligence or industrial espionage. Currently, modern technologies for ensuring security from unauthorized access to information in enterprises are becoming more widespread. In commercial structures, from 3 to 5% of the company's profit is allocated to specialized software and hardware for protection against hacking of server databases (complex firewalls, intelligent penetration detection systems), personnel actions research (DLP - Data Loss Prevention - electronic channel protection systems, which employees of organizations have access to from their work computers), analysis of open and closed markets (in order to determine whether the technology being developed is on sale), etc. For the most part, objects of industrial espionage are financial organizations, trade institutions, and IT companies.

The percentage of competitive intelligence at industrial enterprises in the percentage ratio is only about 8 to 12%, but losses from it at the state level can be colossal and cover all the total losses of the main sectors. All procedures to prevent the use of unauthorized channels of information transfer boil down to a complete ban on the use of third-party equipment (own Wi-Fi routers, 4g modems, etc.) or to jamming certain frequencies. At the same time, if we consider the civilian sector, it is often inappropriate to jam signals in a given situation for a number of reasons: the higher management should still have a

* Corresponding author: binafon88@yandex.ru

communication channel, devices of offices, offices, rooms that are simply located in the neighborhood may be muffled. If we consider industrial enterprises, in certain cases, dimming signals is also not possible, moreover, large areas of the territory also impede this.

2 Information security approach

Currently, in connection with the political and economic situation in the world, the protection of information of industrial enterprises in Russia is one of the most important factors for their safe functioning. According to preliminary data, about 70% of leaks occur through electronic channels accessed by employees of the enterprise from their computers. Typically, these channels and access to them are carefully controlled by security personnel of an industrial enterprise. But there are other communication channels (information transfer through actually deployed Wi-Fi networks, via mobile Internet, etc.) that are difficult to detect (these actions can often be performed only for personal use: watching movies on the Internet, games, etc. etc., but the scale of losses with such an open channel for transmitting information can be significant).

If we consider private enterprises, the detection of unauthorized data transmission channels is also an important task. Network administrators using specialized equipment build maps of Wi-Fi networks, while marking their access points, using the security service they try to identify those who install their routers, Wi-Fi whistles and more. Often in the office network of one company there may be Wi-Fi networks of other companies, therefore, it is not possible to drown out the signal, at the same time, when scaling an office wireless network, you must be able to determine which channels to add to the enterprise network.

Currently, there are various systems that provide protection against various attacks and hacks on the corporate network. Basically, such systems are either their own hardware scanners of Wi-Fi networks with full traffic analysis, or software firewalls that work only with those data packets that are needed at the current time, for example, systems of the WIPS (Wireless Intrusion Prevention System) class. These Wi-Fi intrusion detection systems help detect and block attacks over the air. The first versions of such solutions were used to monitor performance and search for unauthorized access points, but in the next releases they became able to fully block unauthorized devices and detect attacks up to DDoS. Such systems allow you to build a map of Wi-Fi networks, detect attacks (DDoS, MITM, etc.), analyze the passing traffic (the functionality is not present on all systems and is very much inferior to DLP systems that are just tailored for such tasks). The disadvantages of such systems are the impossibility of their work with BT and various other radio channels for data transfer, the very high cost and complexity of the setup, the impossibility of portable placement of analysis devices. The main developers of the solution are Mojo Networks, WatchGuard, etc.

There are also various solutions that allow you to simply block wireless channels, from GSM and Wi-Fi to 4G, but as described above, such options are not always possible to use. The company LLC “CIB” is just providing various engineering services with the possibility of introducing not only blockers, but also offering a solution to protect information.

The main results obtained were summarized in table 1.

Table 1 shows that foreign analogues, firstly, are in a different price category, and secondly, the options they offer are turnkey systems that also need to be controlled and their integration into, for example, domestic industrial enterprises or in network of automated process control system (NAPCS) will be greatly complicated. Most products do not have portable solutions that can be not tied to one room. the developed solution does not offer a complete replacement of powerful information security products, but can act as an auxiliary complex for the detection and registration of non-authorized data transmission channels, taking into account the existing advantages (portability, cross-platform, cost).

Table 1. Analysis of information security systems.

	Dell SecureWorks	Symantec DLP	КИБ SearchInform	Mojo Cognitive WiFi	LLC "CIB"	Developing Solution
Software Production	USA	USA	Russia	USA	USA, Russia	Russia
Hardware Production	USA, China	USA	Russia, China	USA, China	China, USA	Russia, China
Integration into the NAPCS	yes	no	no	no	partially	yes
Portability	no	yes	no	yes	no	yes
Unauthorized Channel Detection	yes	yes	partially	yes	no	yes
Channel Registration	yes	yes	no	yes	no	yes
Crossplatform	partially	partially	no	no	no	yes
Cost	~$70 000	~$110 000	~$35 000	~$12 000	~ $5 000	~$1 500

3 The architecture of the proposed solution

An option is proposed for a hardware-software complex for protection against access to the enterprise's network through unauthorized data transmission channels, which will allow early detection of possible channels of penetration into the information field of enterprises, will make it possible to control the work of personnel and prevent them from using various devices to access the Internet (detection portable Wi-Fi devices, as well as radio frequency information transfer).

The developed hardware-software complex can be implemented in a portable or stationary version

The portable option is placed in a jacket pocket or (if necessary, to increase the radius of coverage of the tracking zone) in a regular backpack or bag. If an unauthorized data channel is detected, a security officer is notified, after returning to the post, all data is automatically uploaded to a stationary server to which the portable solution is connected.

The stationary version is able to process information from portable devices, enter new discovered channels of information transfer to the database. Under certain conditions, it can itself act as a means of detection in the radius of a room or part thereof.

An important factor is not only the identification of the fact of using an unauthorized data transmission channel, but also the identification of maximum information about it (network name, even if it is hidden, signal strength, MAC addressing, etc.) with subsequent processing on the server.

Based on the analysis, a 7-level architectural model of a hardware-software complex was developed for analyzing transmitted traffic and detecting unauthorized channels of information transfer, which includes both hardware and software implementation levels (Fig. 1).

At the lower level, the level of executive devices, there are various devices that can process various signals: radio antennas, Bluetooth modules, Wi-Fi modules, etc. Directly to analyze transmitted packets, it is possible to use basic modules that can listen to the frequencies we need.

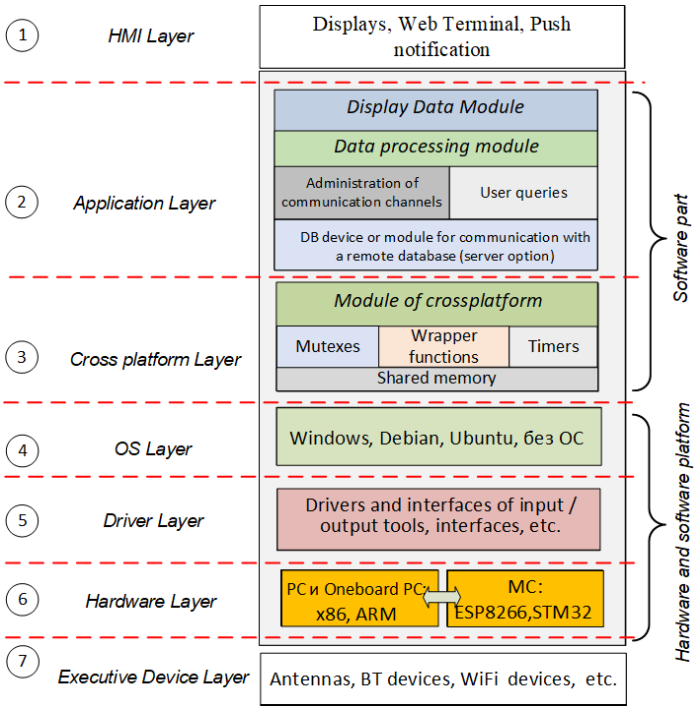

Fig. 1. Architecture of the proposed solution.

The next level is the driver level, which allows you to connect the level of operating systems and the level of the hardware platform with the level of executive devices. In the case of devices without an OS - microcontrollers - special firmware and scripts are used that allow direct access to devices.

Above the level of drivers is the level of operating systems, which can include Windows or Linux (including real-time) for PCs and single-board computers, or not use any OS in the case of using the microcontroller.

The cross-platform implementation of the developed toolkit consists in the use of special wrapper functions, thereby it allows to implement platform-independent functions of timers, mutexes, as well as shared memory. This approach will allow you to use the same code when running on different platforms with minimal modifications.

The application layer includes several modules. The database on the device or the communication module with the remote database allows you to receive information about registered data transfer channels (name, mac addresses, etc.), as well as register new ones. Administration of communication channels allows you to view detailed information about access points (including hidden Wi-Fi and BT) and send special deauthentication packages (if necessary). The data processing module combines the previously listed modules. The terminal level includes various devices to which data is output from the data providing module.

4 Development of a test version of the proposed solution

To test the results, a test program was developed that can run on the Raspberry Pi 3 Model B +, Raspberry Pi0 W, a standard i3 540 PC with Windows and Linux. Support for various platforms is determined by the use of cross-platform architecture, presented above. Domestic Tion Pro 28, Module M, foreign Raspberry Pi 0 W, Orange Pi, ESP8266 are also

considered as target platforms. A variety of software and hardware platforms consists in the number of supported network interfaces, the ability to install additional devices and antennas, power consumption, connecting external screens, etc. Also, a very important factor is the speed and amount of RAM (in the case of battery life, these are important indicators). For the presented boards, performance was evaluated by calculating the number π using various algorithms. The leaders in this calculation are Raspberry Pi 3 and Orange Pi 3, which also support various network interfaces.

The problem with this approach may be the need to natively build the application on each individual device, which can take a fairly long time. In this case, it is good to use the principle of cross-compilation on a powerful stationary PC. After cross-compilation, the software is uploaded to the software and hardware execution platform, where work is already underway to identify unauthorized data transmission channels and their registration. As mentioned above, in the initial stages of development it is planned to use a fully portable solution, where the database of all allowed data transmission channels will be located. Subsequently, it is planned to use a single server, which is a more flexible solution that will allow you to quickly upgrade software and add new registered channels to all devices at once and receive alerts from all devices if unauthorized channels are detected on a single server.

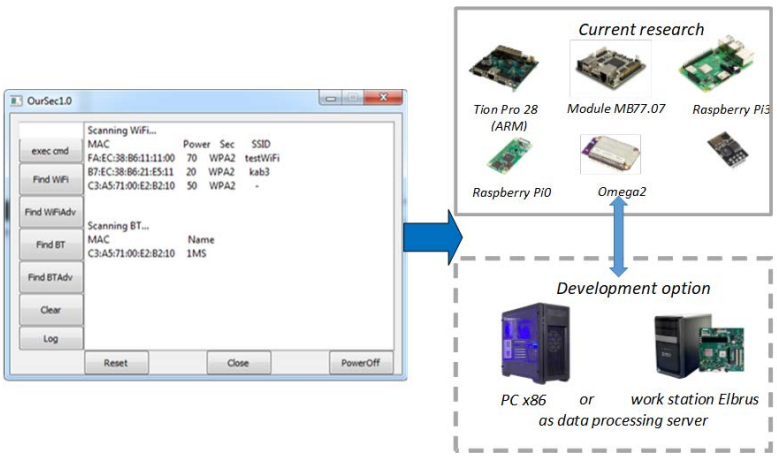

Fig. 2. Development of a test application.

Figure 2 on the left shows the test application window, which is displayed on the TFT screen of a portable device measuring 150x35x80 mm, capable of working from the built-in power source for about 3 hours (the operating time depends on the type of battery used and can be increased, it is also planned to replace the batteries on the go, without portable device shutdown).

On the left are the main keys. Clicking on “Find WiFi” searches for Wi-Fi channels (including hidden ones) and displays information in the work area of the program.

When you click on “FindWiFiAdv”, a deeper analysis of Wi-Fi networks takes place: the channel on which the access point works, mac address of the device, signal strength, devices connected to it, etc.

When you click “Find BT”, BT devices awaiting connection are displayed.

“Find BTAdv” allows you to display not only BT devices, but their mac addresses, signal strength, activity and version of the exchange protocol.

It is also possible to view the message log, restart the main software modules and turn off the device.

On the right, the figure shows the current portable devices under consideration, on which the solution being developed is either already installed or is under development.

5 Test run of a complex for detecting unauthorized data transmission channels

For testing, a number of laboratory stands were developed.

At the first laboratory stand, there are 2 Wi-Fi routers, 1 Wi-Fi whistle, 2 Bluetooth bracelets and the first sample of a hardware-software complex (which is partially described above). The first sample is a portable solution with dimensions of 150x35x80 mm, capable of working from the built-in power source for about 3 hours and having a data display screen.

The second laboratory stand consists of 1 Wi-Fi router, 2 Wi-Fi whistles, a mobile smartphone, a tablet for displaying information and a second hardware and software complex. The second sample is also a portable solution, but with dimensions of 70x20x15 mm, capable of working depending on the selected power source for up to 6 hours.

Figure 3 shows the first version of the stand, which also has a stationary solution that allows you to upload software to portable solutions and analyze in more detail unauthorized data transmission channels.

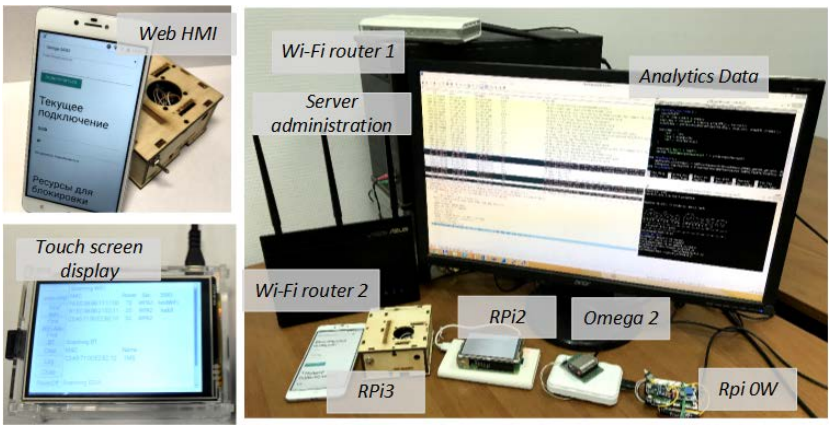

Fig. 3. Laboratory test bench presented solutions.

Using the developed stand, tests were conducted to detect and register unauthorized Wi-Fi and BT data channels. I use BT signals, for example, from a fitness bracelet, it is possible to build a map of a person's movement and understanding whether he has access to the necessary rooms. Several Wi-Fi dots and mini whistles were initialized. For detection, portable devices with and without a touch screen were used. At first it was possible to manually run a network scan. Scanning took about 10 s, after which the found networks (MAC addresses, SSIDs, including for hidden networks, signal strength) were displayed on the screen and those that were not registered as registered in the server database were highlighted. Without screen devices (Omega 2), they scanned the network in a continuous mode: it is possible to transfer data directly to the administration server (if there is a single network) or connect to it after performing a tour around the territory.

6 Conclusion

The proposed approach allows you to create portable devices and stationary devices, combined into a single complex for the detection of unauthorized data transmission channels.

The planned implementation of the principles of cross-platform in the solution will reduce, and in the future, completely eliminate dependence on foreign components and

thereby ensure the technological and information security of domestic enterprises. In the future, it is planned to implement the transition to the domestic element base, including microprocessors (Elbrus 4C) in the development version with the server part of the solution. In the development option of the project, it is planned to develop a method for identifying and registering unauthorized data transmission channels, as well as notification algorithms when they are detected with its practical implementation with minimal delay and reducing network scanning time.

This research was supported by Moscow State University of Technology "STANKIN" and Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (agreement N31-1/03-C18 from 01 August 2018).

References

1. P. Nikishechkin, I. Kovalev, A. Nikich, *An approach to building a cross-platform system for the collection and processing of diagnostic information about working technological equipment for industrial enterprises*, MATEC Web of Conferences, **129**, pp.03012 (2017)
2. R. Nezhmetdinov, P. Nikishechkin, A. Nikich, *Approach to the Construction of Logical Control Systems for Technological Equipment for the Implementation of Industry 4.0 Concept*, In: 2018 International Russian Automation Conference (RusAutoCon), (2018)
3. I. Kovalev, P. Nikishechkin, A. Grigoriev, *Approach to Programmable Controller Building by its Main Modules Synthesizing Based on Requirements Specification for Industrial Automation*, International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), pp.1-4 (2017)
4. P. Kantyshev, V. Petleva, S. Yastrebova, *Hackers turned their eyes to industry*, Electronic version of the newspaper "Vedomosti", https://www.vedomosti.ru/amp/9bdb97c215/technology/articles/2018/01/31/749476-hakeri-promishlennost) (2018)
5. S. Grigoriev, G. Martinov, *An Approach to Creation of Terminal Clients in CNC System*, In: 3rd Russian-Pacific Conference on Computer Technology and Applications. Vladivostok, pp.1-4 (2018)
6. I. Panov, *How to choose a Wireless Intrusion Prevention System (WIPS) to protect your Wi-Fi network from intruders?* Official site of the project NetworkGuru.ru https://networkguru.ru/wireless-intrusion-prevention-system-wips-wifi/ (2019)
7. P. Pletnev, *Supply of protection against commercial / industrial espionage*, Official site of the project LLC « CIB»: https://secret-net.ru/ (2019)
8. V. Chekryzhov, I. Kovalev, A. Grigoriev, *An approach to technological equipment performance information visualization system construction using augmented reality technology*, In: MATEC Web Conf. Volume **224**, 2018. International Conference on Modern Trends in Manufacturing Technologies and Equipment (ICMTMTE 2018), pp.1-7 (2018)
9. G. Martinov, P. Nikishechkin, A. Grigoriev, N. Chervonnova, *Organizing Interaction of Basic Components in the CNC System AxiOMA Control for Integrating New Technologies and Solutions*, Automation and Remote Control, Vol. **80**, No**. 3**, pp. 584–591 (2019)