Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 169 (2020) 183–186

Procedia Computer Science

www.elsevier.com/locate/procedia

Postproceedings of the 10th Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence, BICA*AI 2019 (Tenth Annual Meeting of the BICA Society)

Information security of RFID tags

Dmitry Bagay*

National Research Nuclear University MEPhI, 115409, Russia, Moscow, Kashirskoe shosse, 31, web-domen150796@yandex.ru

Abstract

The development of the Internet of things is the final process of mass integration of computer technologies, technological chains of communication and various sectors of the industrial industry. IS bottlenecks arise because of techniques of eavesdropping, distortion and disclosure of personal information, etc. IoT applications face errors on the application plane - with the use of cloud computing, information processing, protection of confidential information and intellectual property rights.

Keywords: Information Security, Internet of Things, IoT, Industrial Internet of Things, M2M, Cyber Threats, RFID Security

1. Main text

Industrial Internet of things devices are subject to a number of requirements for their information security: it is necessary to ensure the protection of data, the connection of devices to the network must be secure, it is necessary to maintain confidentiality, so that these devices are not subject to cybercriminal attacks, unauthorized access and other network threats.

After you install and configure industrial IOT devices, you need to manage them remotely. The prevailing majority of cameras, sensors, meters, controllers and actuators that are integrated into the M2M network do not have their own

* Dmitry Bagay. Tel.: +7-495-788-56-99
E-mail address: web-domen150796@yandex.ru

10.1016/j.procs.2020.02.133

names, and some do not even have their own traditional user interface. Some of them are designed to work without maintenance and diagnostics for a long time and do not involve human intervention.

For devices that are used in critical systems and infrastructures (medical monitoring systems, building security systems, pipelines) it is necessary to process failures and notifications in real time to ensure uninterrupted maintenance of your site. In addition, these corrective actions must be performed automatically by the devices themselves, depending on security policies, and the data transmitted and received by these devices must be controlled to ensure their manageability, accuracy, and compliance.

Consider the structure and rules of functioning of networks of M2M. Currently, there are 3 choices of connection and the organization of mutual work of the Executive devices.

As the first option, consider the method of organizing external interactions. In this case, the devices in the vast majority of cases connect to the main server, which guarantees secure communication. Devices of this method can be POS terminals, industrial equipment with automatic control of technological operations, Internet terminals, ATMs. Since the location of the devices can be significantly different from each other, the ways of coordination with the Central computer system they also differ significantly: from the GSM mobile communication standard to the Ethernet Protocol. External connections have long been used for encrypted transmission over secure protocols. However, at the same time, the production information network was represented by an intranet, which, due to inaction on the part of the founders of M2M devices, in most cases does not provide any privacy. Quite a long time, this method of network organisation the network has shown a good hand, but with the emergence of Stuxnet and improved technologies targeted attacks, this method of control an automated plant is unsafe and can paralyze the entire enterprise.

At the moment, the issue of a large industrial complex was considered. And what can be said about a more trivial example like a single device that is connected exclusively to a single server? After all, users of such devices have high hopes for data encryption tools that are built into the GSM Protocol.

This problem is caused by the desire to save power devices, since any cryptographic system has its own requirements for power consumption. Alarm buttons, online integrity control, online data transmission over the Internet-all this makes the processor work in a more productive mode, which leads to increased power consumption, the reserves of which are limited in portable devices.

The second variant of the organization of connections of M2M-devices is the use of internal connections that connect the Executive and control device through a physical communication channel. In this version, initially disappear threats associated with an attack on communication channels, but the security issue is not completely closed. Automation for production has been developed for a long time – at a time when developers did not assume that their SOFTWARE can be connected from the outside, often not with good intentions. For this reason, the issue of addressing vulnerabilities in the system that can be used to remotely access their products and use them illegitimately was not given much importance. In addition, programmers on the example of Stuxnet saw that there are high-performance and reliable methods of attacks on internal closed networks without connecting to public access points.

In this case, to ensure the safety of industrial systems, you can use two methods: replace outdated systems with new, more secure systems, or install special additional protection on old systems. It is worth noting that the first method is extremely expensive and not in all situations implement, because there is not always a protected similar system, and the cost of the production system is such that it will be easier to buy a new production plant. The second method seems to be more affordable and really reliable. CheckPoint provides tools such as Anti-DDoS/IPS/IDS to protect the SCADA system from attack.

And the third option of organizing connections M2M-devices-is the introduction of PAN-networks (Personal Area Network), that is, the network structure, acting as a technology and rules for building communications between "smart" devices that can be controlled via a smartphone. The most common embodiment of these technologies – "Smart home". This technology already has formed physical layer standards in the form of IEEE 802.15.4 specification, as well as a set of transport layer standards 6LoWPAN, which uses IPv6 to communicate between devices.

For any type of device interaction, a Protocol for encryption must be developed and a system for mutual authentication of all devices must be thought out, so that it is impossible to view traffic without authorization, duplicate requests and connections, and send control commands. Unfortunately, at the moment there is no single unified Protocol for interaction of M2M devices. How is the development of application protocols of M2M interactions and network protocols (XMPP (Jabber), BITXML, M2MXML and others). The task is complicated by the fact that common standards have not yet been developed, and the introduction of M2M technologies has already begun.

1.1. Security threats in RFID tags

Information security researchers from Australia published a paper describing a method to prevent a reader from reading information from an RFID tag. The method based on the principle of DDoS attacks was used in the work: the radio air is filled with a huge number of signals simulating the signals of RFID tags. In such a situation, the first generation of RFID readers (passive readers) cannot read data from the label due to a collision. There is another threat to RFID tags - it is just their destruction. The most effective way to destroy radio tags is to put them in the microwave for a short time. However, not every item with RFID chip fit in the microwave, so a special RFID device-Zapper was created. The developer of this device decided that the cost of manufacturing should be minimal, so as the basis was chosen camera-soap dish. After improvements to the device, the flash of such a camera could create a strong electromagnetic field that destroys passive RFID tags.

1.2. Cloning RFID tags

Another threat to RFID tags is cloning. The attackers have developed a device proxmark, which easily fit in your pocket and allowed to clone proximity-card imperceptibly for the owner, approaching it at a close distance. This device is constantly being improved and has already received the 3rd generation proxmark3, which has received many new features and the ability to work with the majority of 125 KHz and some 13.56 MHz RFID-tags. Recently, hackers managed to clone even VeriChip, which is positioned as the most reliable way to save user identification data. Cloning an interactive radio tag is already a difficult task, therefore, in the near future, user identification systems with passive RFID tags will become a thing of the past. The main advantage of such interactive systems is the use of encryption to protect information.

1.3. RFID tag encryption issues

There are DST RFID tags that are equipped with 40-bit encryption and are semi-passive. Of course, this encryption is quite easily opened by brute force, but the complexity of determining the key was that the encryption algorithm is unknown to attackers. However, cybercriminals recovered the key using various cryptographic methods. Then they managed to collect a large array that could decrypt 4-5 keys for 1.5 hours. After that, a device that simulates the operation of DST was created.

1.4. Tampering with the contents of memory RFID tags

Information security researcher from Germany Lucas Grunwald demonstrated how information from an electronic passport could be easily transferred to any other RFID-label. Lucas used a previously developed program, RFDump, which allows you to read, edit and write data to RFID tags.

1.5. Attacks via RFID tags

Making changes to the content of the radio tag can allow an attacker to implement different types of attacks on computers running RFID. Databases that are affected by sql-injection can become unprotected places of RFID-systems. In addition, malicious code can also be injected through web interfaces.

1.6. Ensuring information security of RFID tags

In order to reduce the threat of sql-injection attacks, you must perform a full scan of the data that is exposed to sql queries. In addition, there are ORM libraries that are installed between the program and the database. Equally effective is the use of databases that provide capabilities to limit the likelihood of an attack (for example, MySQL and Oracle allow only one request to execute during API calls).

By properly handling scripts, you can prevent malicious client-side scripts. Most of the languages used in web development provide separate functions that allow you to implement proper script processing. PHP language allows you to perform this operation automatically for each line of code, using the symbol "quotes". In addition, if scripting languages are not required, disabling them will avoid any possibility of abuse. When properly processed scripts can also be avoided SSI injection.

Using the Electric Fence and Valgrind tools, you can check the buffer boundaries and thus avoid buffer overflow. You can also use a programming language (such as Java) for this purpose, which also performs buffer boundary validation data.

1.7. Security devices the industrial Internet of things

From the point of view of the architecture of the interaction of devices of the industrial Internet of things, security management requires 3 key components:

1. Each connected device must have its own permanent identifiability. Proper organization of identity management (registration of a device for granting access, its authorization, authentication, management of special services and privileges of a particular device) is the first step to ensure the security of M2M devices. The difficulty is that most of these devices will not use direct connections. Instead, they will be combined into LAN / PAN networks using a common gateway that will provide access to the network through mobile cellular operators. In this case, you must manage the identity not only of each device, but also of the gateway itself. In addition, you must securely manage groups of devices that are connected through the same gateway.
2. The next step to ensure the security of M2M devices is to establish a reliable communication channel for remote control of the device. This channel should protect the integrity of data, ensure the availability of the device, ensure the confidentiality of the transmitted data, provide means of authentication of devices.
3. The third key component is a software environment that will ensure the continued security of applications for industrial IOT devices. Reliable software for M2M devices, signed with a permanent device ID and transmitted to it via a secure communication channel, will provide a secure software environment.

Thus, providing information security at every level of the architecture of interaction of devices of the industrial Internet of things, it is possible to achieve a high degree of security of this technology.

References

[1] Alekseev V. Modules Bluetooth, Wi-Fi and NFC production u-blox connectBlue for the "Internet of things", part 1. Bluetooth-enabled modules // Wireless technologies. 2015. Vol.2. No. 39. P. 27 - 32.

[2] Perera, C. and etc. Context Aware Computing for The Internet of Things: A Survey. Communications Surveys & Tutorials, IEEE, 2014, V.16, Issue 1, P. 414-454.

[3] Goldstein B. S., Curly A. E. post-NGN Communication networks. SPb.: BHV-Petersburg, 2013, P. 160.

[4] Khan R. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, Frontiers of Information Technology (FIT) - 2012 10th International Conference on, 2012. - 257 – 260 p.

[5] Zhi-Kai Zhang. IoT Security: Ongoing Challenges and Research Opportunities, Service-Oriented Computing and Applications (SOCA) - 2014 IEEE 7th International Conference on, 2014. – 1-5 p.

[6] Zhi-Kai Zhang. Emerging Security Threats and Countermeasures in IoT - ASIA CCS '15 Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, 2015. – 1-6 p.

[7] Nefedova M. UPD. DDoS attack on the DNS provider Dyn caused failures in the largest sites. // Hacker Magazine. No. 226, 2017 – 23 p.

[8] Baoquan Z., Zongfeng Z., Mingzheng L., Evaluation on security system of internet of things based on Fuzzy-AHP method, E -Business and E -Government (ICEE). - International Conference on 2011, 2011 – 1-5 p.