B. Turgunov, A. Komilov, D. Abdurasulova, X. Umarov

SECURITY OF A SMART HOME

(Fergana branch Tashkent University of Information Technologies
named after Muhammad al-Khwarizmi)

Actuality: So, what is the smart home? Why, nowadays we have to discuss of problems its security. As it is known, today, the conception of building smart cities, smart house and smart industries are so largely spread. Therefore, it so important and actual question to research of security problems in the smart homes.

A smart home is a system based on the full automation of all housing arrangements. That is, you can easily turn off the light in the corridor with one click on the control panel. But, in order to design a smart house with your own hands, you will have to try. Also you can manage any IoT (Internet of Things) devices in your smart house across wireless connection by use your smartphone.

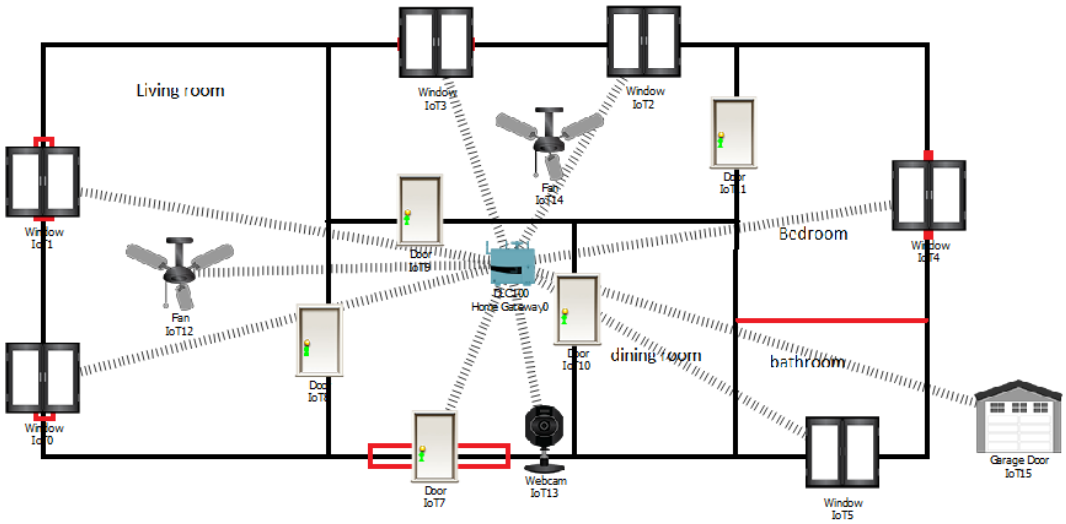

Fig. 1. Wireless connection IoT devices in smart home to home gateway

Your smart home can be connected to local network and your only can manage your IoT devices if you be in your home. But, this type of smart home is not so comfortable by managing remotely. Therefore, usually, the IoT devices of smart home are connected to the internet.

Along with the growth in the number and type of devices connected to the Internet, the risks associated with security and privacy protection are also growing. This is especially true for IoT - the things surrounding us can be used for other purposes and for criminal purposes, their functionality can be changed right up to the failure of the work. While smart objects are becoming more and more intertwined into our lives, making us increasingly dependent on them, the issues of ensuring the security of IoT systems, personal data become more relevant than ever and constitute an important element of our own security and privacy.

The evolution of automated control systems (ACS) has evolved from closed systems with proprietary devices and protocols to a multi-tier architecture with increasing use of standard IT components and, finally, to a new growing trend in the introduction of IoT technologies.

Cost and advanced functionality were the main motivations for moving to a more standard IT architecture and components. This transition had security implications - the system could no longer be regarded as completely isolated, the vulnerabilities of standard components were more pronounced. However, for this generation of control systems, it was possible to provide sufficient isolation from the environment, including physical protection. The number of components was relatively limited, and communication with the external communication infrastructure, in particular the Internet, was not a requirement and either was well controlled or completely absent.

The possibility of introducing miniature sensors and controllers into virtually all components of the physical production process is fraught with benefits that are difficult to refuse. First of all, this is a significant increase in the reliability of the system and the provision of preventive maintenance. The collection of indicators of the status of various components of the system in real time, comparison of data from identical devices, threshold indicators of wear - all this makes it possible to reduce the cost of production and significantly improve its quality.

However, the use of IoT in an automated control system often carries with it serious security problems. First, the entire system becomes more open. The performance and traffic requirements often exceed the capabilities of the corporate VPN, in order to uncover the full potential, in many cases it is necessary to provide communication with external services, etc. Secondly, these problems are exacerbated by the fact that the traditional components of the ACS are not protected by definition, being designed for an assumed completely closed and controlled environment.

In the home automation environment, several factors exacerbate the security problem:

- "Smart home" is an open system. Moreover, despite the development of these platforms, the introduction of IoT in the household is usually done by non-specialists, without long-term planning, leading to the creation of an eclectic system with components and architectures of different manufacturers and the absence of a unified security policy.
- The main emphasis is on the functionality of devices and the system as a whole. Given the desire to minimize the cost of devices, this often leads to insufficient attention to security issues. Ordinary consumers simply can not assess the degree of protection of devices and the risks associated with its use and is forced to close these eyes to these aspects in order to obtain the desired functional result.
- More and more things around us use the Internet to expand their functionality. It is becoming increasingly difficult to acquire a "thing" that would not be connected to the Internet.

- The scale of the implemented IoT devices is significant. Moreover, the uniformity of these devices greatly enhances the effect of detecting a vulnerability in one of them.
- Many sensors collect highly confidential data that provides information about our habits, behaviour, finding, can listen to our conversations and make video recordings. For example, Samsung's SmartTV TV has the ability to be controlled by voice commands. The problem is that for this purpose the TV sends the heard speech to Samsung for analysis on the possible commands.

Threat model

To understand the risks associated with IoT, let's look at the architecture of such a system. As an example, let's take the most general variant of home automation. Vulnerabilities of the system are shown in Fig. 2 in red circles.

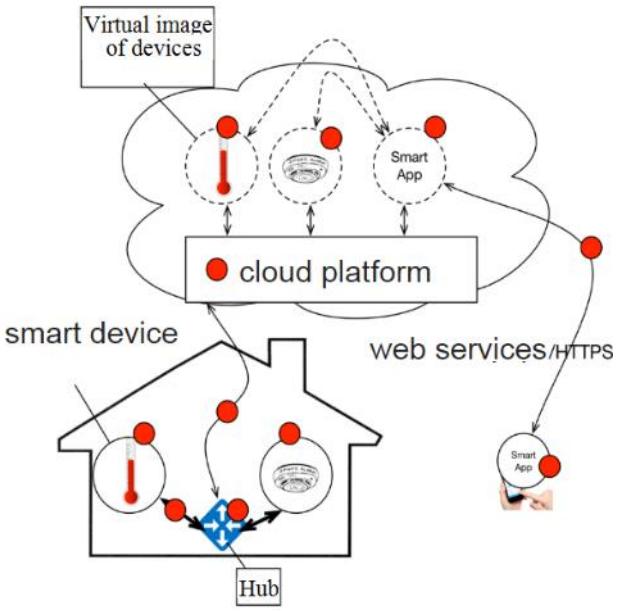

Fig. 2. Vulnerabilities in the IoT home automation ecosystem.

As can be clearly seen from the IoT system threat analysis, the security problem requires a comprehensive solution. There is no magic technology or practice that would reliably protect the entire system. The more open the system, the more players should be involved in solving the problem - from IoT equipment manufacturers, software developers to cloud providers and the owners of smart devices themselves. Moreover, inadequate security of at least one of the elements can significantly weaken the security of the system as a whole.

Taking into account the analysis of threats and vulnerabilities of the system, shown in Fig. 1, we can formulate a number of complex measures aimed at enhancing the security of the system as a whole.

Security of IOT devices

Let's start with the proper IoT devices - from smart locks, thermostats, light bulbs, video cameras, etc. Although, as I have already noted, the possibilities of such systems are very different, you can still formulate some general recommendations:

- A reliable access and authentication system based on cryptography. The requirement for the convenience of connecting devices often takes precedence over safety and uncommon use of standard login / password requirements such as admin / admin, even without the requirement of their changes after the initial initialization of the device on the network. During initialization, the device and its authentication in many cases, play an important role local gateways or cloud platform.
- Cryptographic protection of software (software). A good practice is to use a PKI system for code signing and verifying its authenticity. This functionality is also the basis for a secure software update.
- Software update throughout the life cycle of devices. As you know, there is almost no software without errors. This means that sooner or later the device can find new vulnerabilities. The only way to reduce this risk is the ability to update the software version of the closed-found vulnerabilities. Of course, provided that the software developer responds to detected vulnerabilities creation of the necessary patches and timely releases an updated version of the software. It is extremely important that the update can be carried out automatically, without the participation of the device owner. Critical is the security of the whole process.

This issue is not easy, and its solution is fraught with many pitfalls. A more detailed discussion of the problems and additional guidance in this area can be found in the report of the seminar Internet of Things (IoT) Software Update (IoTSU) organized by the IAB

Conclusion

The significant increase in risks related to security and privacy issues is not related to IoT itself, but to the fact that the digital world and the Internet are increasingly intertwined in our lives. More and more personal and confidential data are stored in the "clouds", we are increasingly dependent on clever useful devices, applications, the Internet. IoT certainly makes the problems discussed above more significant.

System security is not a binary state. The degree of safety is a wide range. How well protected the system also depends on the nature of the threats. All these factors change over time. Let's hope that as the industry becomes more mature, IoT security will be ensured at an adequate level.

References

1. https://www.smarthome.com
2. http://domsdelat.ru
3. http://netping.ru