# Developing models of IoT infrastructures to identify vulnerabilities and analyse threats

# Developing models of IoT infrastructures to identify vulnerabilities and analyse threats

**N A Proshkin[1], E S Basan[1], M A Lapina[2], A G Klepikova[3], V G Lapin[4]**

[1] South Federal University, 2 Chekhov St., Taganrog, 347928, Russia

[2] North-Caucasus Federal University, 1 Pushkin St., Stavropol, 355017, Russia

[3] Belgorod State National Research University, 85 Pobeda St., Belgorod, 308015, Russia

[4] Stavropol regional clinical consulting and diagnostic center, 304 Lenina St., Stavropol, 355000, Russia

E-mail ele-barannik@yandex.ru

**Abstract.** This article describes the developing stands of typical IoT infrastructure Technologies, which are designed to identify vulnerabilities and analyse potential threats. Scenarios of attacks typical for such systems have been developed, and the consequences of implementing attacks have been determined. Attacker can use the developed scenarios, been motivated by different goals. The research is also aimed at increasing the awareness of IoT users and determining the necessity to compliance with the minimum set of requirements relevant articles in literature searches, great care should be taken in constructing both.

## 1. Introduction

In the modern world, there are more and more opportunities for learning, and it becomes easier to find the necessary knowledge. Every person will be able to find any information they are interested in on the Internet [1].

Along with this, in the age of information technology, such a direction as "Cybercrime" is particularly developed. Cybercriminals are people who have made every effort to find the necessary knowledge and tools to use their computer illegitimately and influence information systems.

Today, the range of devices and technologies that can be attributed to the "Internet of things" systems is actively expanding, primarily systems such as: "Smart home", "Smart city", "Smart greenhouses", "Smart farm", "Smart factory", etc., I.e., systems that can consist of sensors, cameras, actuators, in combination with information and telecommunications technologies and control systems [2]. The use of such systems in various spheres of human life gives a positive economic effect and makes additional benefits from various points of view. The direction related to the digitalization of the economy is one of the priorities for the Russian Federation.

All information about the devices listed above and the devices themselves are easily accessible. The use of such systems in various spheres of human life gives a positive economic effect and allows to get additional benefits from various points of view. For example, using the "Smart lighting" provides energy savings of 40%. The "Internet of things" is an information system that consists of various hardware, software and telecommunications components, each of which has threats and vulnerabilities, as a result of which it can be subject of attacks from an intruder, environmental influences, failures and other factors that can lead to malfunction of both the system itself and the object that this system manages. A study by Positive Technologies States: "On average, about 10 vulnerabilities are detected in home network devices (Wi — Fi and 3G routers) every month. According to PositiveTechnologies experts, most developers and suppliers of network devices do not attach proper importance to such concepts as "testing" and "security". Many serious vulnerabilities remain without updates, and if they do come out, users are in no hurry to apply them. For example, 87% of systems tested by Positive Technologies experts had vulnerabilities related to the lack of updates." Dmitry Yaroshevsky, senior solutions architect of the company "Kaspersky Lab", writes: "Deception of sensors, manipulation of data received in the program or shown to the operator, influence directly on the Executive mechanisms-successful attacks on any links in this chain can lead to disastrous consequences. Despite the reality of the threat, many users are negligent about basic cybersecurity rules. So, according to one of the studies, only 50% of the surveyed Russians changed their default passwords on the router, 61% check updates once a year or less often." In many ways, users of such systems are often the culprits of incidents related to the violation of the security of their "Internet of things" system themselves [3].

## 2. Description of Internet of things infrastructure stands

### *A. Automated dairy farm*

The first example of a stand developed for information security analysis is "Automated dairy farm" (hereinafter referred to as "Smart farm"). The "Smart farm" model consists of temperature and carbon monoxide sensors, alarms, lighting, and an Arduino UNO microcontroller. Microcontrollers in such systems are used to control other devices and provide an interface for human interaction with the system. The structure of the remote farm management system, its topology, and physical and technological connections are shown in figure 1.

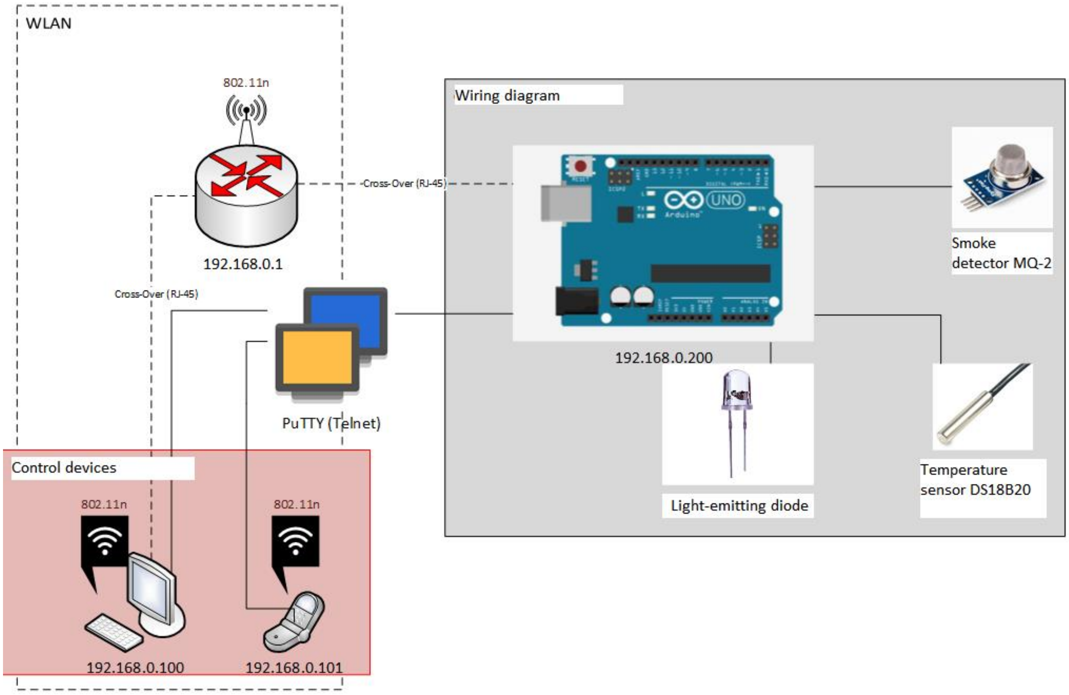

Figure 1. Block diagram of «Automated dairy farm»

The "Smart farm", connected to a wireless router via an Ethernet cable, is managed using control devices (PC or phone) located in the same WLAN (LAN) network with the Arduino UNO microcontroller, using the Telnet remote control protocol.

Analogous to such infrastructures are the systems of the companies "Dairy XL", "Iron Ox", the international agricultural Corporation "Lely" and others [4].

*B. Automated oil pump*

The second stand is "Automated oil pump" (hereinafter referred to as "Oil pump"). The "Oil pump" model consists of a stepper motor for adjusting the pump's swing speed, an Arduino UNO microcontroller, and a smoke generator that simulates the engine's excess power. Control of the "Oil pump" connected to the router via a cross-over cable is performed by control devices (PC or phone), located in the same WLAN (LAN) network with the Arduino UNO microcontroller, over the HTTP Protocol, by connecting to the management interface and supporting the system via the browser address bar. Analogues of such systems are: "AHM7500 series electric pumping oil mainline units" and others [5].

*C. Smart house*

The third stand is "Smart house". It includes several types of wireless communication: radio, Wi-Fi, telephone, temperature, humidity, pressure, carbon monoxide, motion, rain, sound, light controls, Russian microcontrollers Iskra and their Arduino counterparts, servos.

The Smart house connected to the router is managed via a mobile app that displays all the system's functionality.

The type of wireless communication is determined by the analysis and identification of the most secure type of communication.

Comparison of different countries-manufacturers of microcontrollers is related to the need to use domestic technologies.

Analogous to such infrastructures are many systems such as: "Xiaomi", "Yandex", "Rexant", etc.

## 3. Typical attacks on information systems and tools for attacks

*A. DoS Attack*

Denial of Service (DoS) attacks are a type of network attack [5]. A DoS attack causes interruptions in network services for users, devices, or applications.

There are two types of DoS attacks:

- Huge amounts of traffic;
- Packages with incorrect formatting.

The tool for carrying out the attack can be the utility "Netwox 76" under the Linux operating system.

*B. Sniffing*

This type of attack involves traffic tapping using the Wireshark sniffer program, which is used by network administrators to detect network problems, but a cybercriminal can use this program to commit illegal actions.

*C. Spoofing*

Spoofing is an impersonation attack in which attackers exploit a trust relationship between two systems.

Types of attacks using substitution.

- Spoofing the MAC address;
- IP address spoofing;
- ARP substitution.

The tool for carrying out the attack can be the utility "Netwox 40" under the Linux operating system.

*D. Man in the middle (MITM)*

An attacker becomes an intermediary by intercepting messages between devices on the network to steal information. A criminal can also manipulate messages and pass false information between hosts, since the hosts do not know that a message modification has occurred.

The tool for conducting an attack can be the "Netwox" utility under the Linux operating system.

## 4. Vulnerabilities of Internet of things infrastructure

Finding vulnerabilities in copies of the Internet of things systems allows to analyze a similar real system, identify potential vulnerabilities and, accordingly, potential threats.

It must be noted that in real systems, responsible information security specialists provide for all typical attacks on automated systems, thereby reducing the number of potential threats.

In particular, their security measures target network nodes such as routers, switches, and management devices of automated infrastructure.

But IoT Technologies, despite their simplicity, also have a number of vulnerabilities. It is difficult to influence the sensor modules from the outside, you must have access to control the microcontroller, but the wireless communication modules of "Internet of things", practically, do not have protection at all.

In this way, the basic infrastructure of IoT Technologies consists of two levels:

- Network devices;
- «Internet of things».

Therefore, it is advisable to separate vulnerabilities depending on the level of infrastructure components.

### *A. Vulnerabilities at the network device level*

This layer, as mentioned earlier, includes: routers that provide remote connection and data transfer over the network; switches that allow to combine multiple devices into a single local network; and management devices that directly have access to the infrastructure.

This level is characterized by typical vulnerabilities and attacks, so it does not make sense to consider it in detail.

We will take a closer look at vulnerabilities at the Internet of things level

### *B. Vulnerabilities at the Internet of things level*

This level includes microcontrollers, sensors, wireless and wired communication modules.

The sensors are only exposed to electromagnetic interference and do not act as a target. Microcontrollers are vulnerable only when interacting directly with them, that is why, they can be a subject to 0-day attacks. But the software or firmware of microcontrollers cannot be counted without special utilities and direct access to it. Therefore, the attacker does not appraise microcontrollers as a target.

The main target of such systems are wireless communication modules, as well as wired communication modules connected to the router.

Communication modules are as vulnerable as communication tools. They are vulnerable to eavesdropping, signal suppression, radio intelligence, etc. Most vulnerabilities are also related to the fact that IoT Technologies are connected to the Internet.

Let's look at the vulnerabilities of specific stands.

## 5. Vulnerabilities of IOT stands and attacks:

### *A. Vulnerabilities of "Auto farm"*

"Auto farm" is connected to the local network via an Ethernet cable connection between the router and the Ethernet Shield.

The vulnerability of the Telnet remote access Protocol is that data is transmitted over this Protocol without encryption. In this way, you can conduct an attack on the confidentiality of information by using the Wireshark traffic sniffer to intercept packets and read data. The vulnerability of the router is that it does not have protection against sending ICMP packets, so an attacker can scan the network and identify devices inside this network. And also conduct a DoS or DDoS attack on the router, thereby disconnecting the control device from the system.

### *B. Vulnerabilities at the Internet of Things*

This level includes microcontrollers, sensors, wireless and wired communication modules.

Sensors are exposed only to electromagnetic effects and do not act as targets.

Microcontrollers are only vulnerable to direct interaction with them and are susceptible to 0-day attacks. But the software or “firmware” of microcontrollers cannot be read without special utilities and direct access to it. Therefore, the microcontrollers do not see the attacker as a target.

The main goal of such systems are wireless communication modules, as well as wired communication modules connected to the router.

Communication modules are vulnerable as well as communications. They are vulnerable to listening, signal suppression, radio intelligence, etc. Also, most of the vulnerabilities are related to the fact that IoT-Technologies are connected to the Internet.

Consider the vulnerabilities of specific stands.

### *C. Vulnerabilities of the "Oil pump"*

The "oil pump" is connected to the local network via a crossover cable connection between the router and the Ethernet Shield.

The vulnerability of the HTTP Protocol is that information transmitted in packets and headers of this Protocol can be used to get data about the web server or clients.

When connecting the router to an Internet provider, access to the web page for managing the "Oil pump" is not protected in any way, and a VPN is not used, so an attacker can find out the IP address of the system and connect to it from anywhere in the world.

There are also router vulnerabilities related to sending ICMP packets and attacks on system availability.

### *D. Vulnerabilities of the "Smart house»*

The Smart house stand is a stand for analyzing the security of the majority of wireless communications technologies.

Microcontrollers are divided into:

- Central;
- Primary;
- Secondary.;

Primary and Central microcontrollers form a network of topology "Star", where the Central node is the Russian microcontroller Iskra Pro. They are connected to each other by a wired connection and use the UART Protocol for data exchange.

Sensors and communication modules are also wired to each secondary microcontroller and use UART, SPI, or I2C protocols, depending on the hardware of the device. Only the communication modules are connected to primary microcontrollers

Primary and secondary microcontrollers interact with each other via wireless communication. In the future, we will call this interaction "Pair".

Wireless communication modules for each "Pair":

- Radio communication module "nrf24l01" 2.4 GHz;
- "Troyka-module" Wi-fi module based on ESP-12 with 5 GHz ESP8226EX chip;
- GSM SIM800l cellular communication module without Bluetooth and GPS/GLONASS support.

To manage the Smart house infrastructure, a wireless connection to the Central microcontroller is used using the HC-05 Bluetooth module.

Vulnerabilities of the radio communication module are physical insecurity and the ability to listen to the communication channel. An attacker can intercept radio waves using a broadband software-defined radio receiver-transmitter "HackRF", and also, recognizing the frequency, send their data [6].

In this way, the confidentiality of information in the system will be violated without proper encryption of radio traffic.

Also, radio communication is subject of distortion or signal suppression by an attacker, which leads to a violation of the integrity and availability of information in the system.

The vulnerabilities of the Wi-Fi communication standard are similar to those of radio communications. In addition to them, the vulnerability of the "open hotspot" also applies. It appears when the Wi-Fi module does not have a hidden parameter in its configuration, which allows you to conduct a "Denial of Service" attack on the module itself. As well as attacks on vulnerabilities in the WEP and WPA security protocols.

Vulnerabilities of the cellular communication module are associated with the possibility of overflow of the incoming message buffer, as well as with suppression and jamming of cellular communication frequencies [7]. Since the cellular module uses telemetry to work in duplex mode, and there is no white list of numbers that the module can respond to, there is a vulnerability of the depletion of the money balance due to sending telemetry messages.

Vulnerabilities of the Bluetooth module are associated with vulnerabilities of the protocols LMP (Link management Protocol), L2CAP (logical link control and adaptation management Protocol), SDP (Service Discovery Protocol), TCS Binary (telephony control Specification - Binary), TCP and UDP.

This is not the final list of vulnerabilities, but an attacker can use them to attack the infrastructure using IoT Technologies, thereby exposing the entire system to threats.

Next, the scenarios of such attacks, analysis of the corresponding threats and their consequences, conducted at the stands of the Internet of things will be presented.

## 6. Attack Scenarios, threats and consequences

*A. «Auto farm»*

**Scenario 1**: A Cybercriminal learns that there is a milk production plant nearby that has remote access to control, determines the IP address of the router (target) and conducts a Denial of Service attack using the "Netwox 76" utility.

Possible consequences: during a DoS attack: all connected nodes lose connection. If you lose control of a plant, its owner may lose a large number of their assets, dairy products will deteriorate, and the sooner the owner reacts to the attack, the more money they will be able to save to restore the system.

The threat is related to the possibility of violating the availability of the system.

**Scenario 2:** A fired employee, been driven by revenge, connects to the internal network using old authentication data (or using a Brute force attack), and, already having access to the system, starts sending incorrect commands, overflow the incoming command buffer, and destabilize the enterprise. The operator who manages the plant by receiving and sending data, will receive distorted information or not receive it at all, and will not be able to send their commands.

Possible consequences: failure to take timely measures on the part of the owner will ensure the loss of his assets.

The threat is related to the possibility of violating the integrity and availability of the system.

*B. «Oil pump»*

**Scenario 1**: Infrastructure Operators use remote access to regulate engine power and limit its maximum value. An attacker using the «Netwox» utility arranges a DoS attack or, after infecting a large number of devices with viruses, makes a "Bot network" and arranges a DDoS attack at the moment when operators began to increase the engine power. When performing this attack, the connection is broken, so it is not possible to reduce the engine power remotely, it gradually approaches the limit and the engine breaks.

Possible consequences: Loss of assets.

The threat is related to the possibility of violating the availability of the system.

**Scenario 2**: An Attacker connected to the network by matching the password to the router using a Brute force attack. Using the «Wireshark» sniffer he captured packets with the HTTP Protocol, analyzed them, and found out the IP address of the system [8]. Since the infrastructure had a password system only at the router level, the attacker gained access to the system, increasing the power of the engine, thereby incapacitating it.

Possible consequences: Loss of assets.

The threat is related to the possibility of violating the system's privacy.

*C. «Smart house»*

**Scenario 1**: an attacker fraudulently entered the target's home by impersonating as a new neighbor. After establishing contact with the victim, he found out that the house is controlled with a phone, using Bluetooth. Knowing that the range of Bluetooth communication is not large, an attacker will take advantage of a vulnerability in the protocols of this wireless communication and perform a "Bluesnarfing" attack to steal data. Then, he can conduct a "Bluejacking" attack to send false alerts to the victim's phone and false commands to the system.

Possible consequences: an attacker will not be able to manage the Smart house remotely, but in a small radius from the house, if the owner is not in it, he will be able to set false infrastructure commands.

The threat is related to the possibility of violating the system's privacy, however, considering the fact, that the interaction distance is limited, this model is irrelevant.

**Scenario 2**: The Cybercriminal found out that the Smart house is controlled by sending common SMS. After learning the number of the Smart home, he will try to figure out its location using GPS [8]. If this attack fails, because the module cannot use this function, the attacker may start sending a large number of SMS messages to the Smart home number. And since now any mobile operator has a limited number of SMS messages, either in units per day, or in their cost, the funds or limit on the SIM card will quickly expire.

Possible consequences: you will constantly have to spend money in order to top up the balance of the smart house SIM card, and if the SMS limit is exhausted, data from the home will not be received.

The threat is related to the possibility of violating the availability of the system. To minimize the risks associated with the threat, it is enough to update the module's firmware by adding a list of «White numbers» to it.

**Scenario 3**: an attacker uses a powerful radio jammer located near the house will be able to disable all wireless communication modules.

Possible consequences: Loss of control of the system may cause jamming of doors, failure to turn on or off the light, etc.

The threat is related to the possibility of violating the availability of the system.

**Scenario 4**: a Cybercriminal uses a interceptor «HackRF» will be able to intercept a radio signal from a «Smart house» that extends over considerable distances, configure the" HackRF " to the frequencies that is used in the system, identify the carrier communication channel and compromise information, jamming the channel with interference or send false information.

Possible consequences: a Complete loss of control over the system will make it impossible to interact with it.

The threat is related to the entire face of the security cube: privacy, integrity, and availability, since the model of this threat is relevant.

## 7. Conclusion

To sum up, I would like to note the fact that the fight against cybercrime in the field of automated information systems using IoT Technologies should begin with the introduction of new information security measures for the «Internet of things» itself.

In IoT Technologies, all vulnerabilities are mainly related to the fact that IoT have access to the Internet. Here we should make a reservation – not "all", but "many", but there is also a share of vulnerabilities that are typical only for the «Internet of things», in particular for wireless communication modules.

Since IoT is a part of an automated system, their protection, from the point of view of information security, must be conducted properly.

The article presented primitive examples of real infrastructures. It is not possible to give an objective assessment of the security of the system based on them. However, real systems use devices that are as close to the devices in the stands as possible.

The development of such systems, the selection of components and their Assembly and configuration, allow us to give not a comprehensive, but individual

assessment of the security of each "Internet thing" that makes up the system, which is extremely necessary for the final assessment of the infrastructure audit.

## 8. Acknowledgment

This work was supported by the RFBR grant 18-07-00212 “Development of a method and decision protocol for detecting anomalous node behavior in group control systems of autonomous mobile robots”.

## References

[1] Basan A, Basan E, Makarevich O, Babenko L 2019 Investigation of the impact of active network attacks on a group of mobile robots. *Cybersecurity Issues* (1) ISSN 2311-3456 pp 35-44

[2] Makhdoom I, Lipman J, Ni W 2019 Anatomy of Threats to the Internet of Things *IEEE communications surveys & tutorials* **21(2)** pp 1636-1675

[3] Siboni S, Sachidananda V, Meidan Y, Bohadana M, Mathov Y, Bhairav S, Shabtai A , Elovici Y 2019 Security Testbed for Internet-of-Things Devices. *IEEE transactions on reliability* **68(1)** pp 23-44.

[4] Atamli A , Martin A 2014 Threat-based Security Analysis for the Internet of Things. *Proceedings of International Workshop on Secure Internet of Things.* pp 36-43.

[5] Zhou W, Yu B. 2018 A Cloud-Assisted Malware Detection and Suppression Framework for Wireless Multimedia System in IoT Based on Dynamic Differential Game. *China Communications* pp 209-223

[6] Carielli S, Eble M, Hirsch F, Rudina E, Zahavi R 2019 IoT Security Maturity Model: Practitioner’s Guide Version 1.0 p 129

[7] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity 2018 Version 1.1.April 16 p 55

[8] Alam S, Mohammad M, Chowdhury 2011 Interoperability of Security Enabled Internet of Things. *Wireless PersCommun* pp 567-586 DOI 10.1007/s11277-011-0384-6